Bundesministerium
des Innern

Migrationsleitfaden

Leitfaden für die Migration der Basissoftwarekomponenten auf Server- und Arbeitsplatz-Systemen

www.kbst.bund.de

2. überarbeitete Auflage

Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik
in der Bundesverwaltung

KBSt

Schriftenreihe der KBSt
ISSN 0179-7263
Band 72
August 2005

Schriftenreihe der KBSt

Band 72

ISSN 0179 - 7263

Dieser Band wurde erstellt von der KBSt im
Bundesministerium des Innern (BMI)
in Zusammenarbeit mit dem Bundesamt für
Sicherheit in der Informationstechnik (BSI),
dem Bundesverwaltungsamt (BVA)
und der EDS Business Solutions GmbH

Redaktion: EDS Business Solutions GmbH, Berlin

Nachdruck, auch auszugsweise, ist genehmigungspflichtig

Interessenten erhalten die derzeit lieferbaren Veröffentlichungen der KBSt

und weiterführende Informationen zu den Dokumenten beim

Bundesministerium des Innern

Referat IT 2 (KBSt)

11014 Berlin

Tel.: +49 (0) 1888 681 - 2312

Fax.: +49 (0) 1888 681 - 52312

Homepage der KBSt: www.kbst.bund.de

mailto: Monika.Pfeiffer@bmi.bund.de

Migrationsleitfaden

Leitfaden für die Migration der Basissoftwarekomponenten auf Server- und Arbeitsplatz-Systemen

2. überarbeitete Auflage

Berlin, August 2005

Herausgegeben vom
Bundesministerium des Innern

1 Einleitung 9
1.1 Motivation 9
1.2 Über diesen Leitfaden 10
1.3 Hinweise zur Benutzung des Leitfadens 12
1.4 Hinweise an die Entscheider 15
1.4.1 Grundsätzliche Empfehlungen 15
1.4.2 Fortführende und ablösende Migration 15
1.4.3 Vergleichbarkeit von Alternativen 16
1.4.4 Künftige Schwerpunkte 16
1.4.5 Rechtliche Aspekte 17
1.4.6 Wirtschaftlichkeit 17
1.5 Informationsbasis 18
1.6 Ausblick 19
2 Erläuterungen zum Verständnis alternativer Migrationspfade 20
2.1 Wichtige Definitionen 20
2.1.1 Open Source Software, Free Software, Freie Software 20
2.1.2 Proprietäre Software 20
2.1.3 Commercial Linux Software 21
2.1.4 Ablösende Migration 21
2.1.5 Fortführende Migration 21
2.2 Migrationspfade 21
2.2.1 Ausgangslage Microsoft Windows 22
2.2.2 Systemlandschaft bei ablösender Migration 25
2.2.3 Systemlandschaft bei fortführender Migration 26
2.2.4 Interne Abhängigkeiten in der Microsoft-Systemlandschaft 27
2.3 Linux-Distributionen 30
2.3.1 Einleitung 30
2.3.2 Debian GNU Linux 32
2.3.3 Suse Linux Distribution von Novell 34

2.3.4 Red Hat-Distribution 35
2.3.5 Standard Desktops 36
2.3.6 Zertifizierungen 45
2.3.7 Fazit 47
2.4 Open Source Lizenzmodelle 47
2.4.1 GPL 48
2.4.2 Lesser GPL 49
2.4.3 BSD Lizenz 49
3 Technische Betrachtung der Migrationspfade 51
3.1 Einleitung 51
3.2 Dateiablage 52
3.2.1 Überblick 52
3.2.2 Windows NT 4 53
3.2.3 Ablösende Migration 62
3.2.4 Fortführende Migration 73
3.3 Druckdienst 79
3.3.1 Überblick 79
3.3.2 Einleitung 79
3.3.3 Ausgangssituation – Drucken unter Windows NT 4 80
3.3.4 Ablösende Migration 88
3.3.5 Fortführende Migration 98
3.4 Authentisierungsdienste 99
3.4.1 Überblick 99
3.4.2 Ausgangslage – Windows NT 4 100
3.4.3 Ablösende Migration – Linux, Samba und OpenLDAP 108
3.4.4 Fortführende Migration 111
3.5 Netzwerkdienste 112
3.5.1 Überblick 112
3.5.2 Ausgangslage – Netzwerkdienste unter Windows NT 112
3.5.3 Ablösende Migration – Netzwerkdienste unter Linux 118
3.5.4 Fortführende Migration – Netzwerkdienste unter Windows 2000 120

3.6 System-Überwachungs- und –Management-Dienste 122
3.6.1 Überblick 122
3.6.2 Ausgangslage Windows 122
3.6.3 Ablösende Migration – Linux 124
3.6.4 Fortführende Migration 131
3.7 Verzeichnisdienst 134
3.7.1 Überblick 134
3.7.2 Grundlagen 134
3.7.3 Active Directory Service (ADS) 138
3.7.4 Ablösende Migration – Samba und OpenLDAP 155
3.7.5 Fortführende Migration – Einführung ADS 159
3.8 XML (Extensible Markup Language) 166
3.8.1 Allgemeines 166
3.8.2 Vorteile und Schwächen 173
3.9 Backend-Integration 175
3.9.1 Überblick 175
3.9.2 Einführung 176
3.9.3 Dokumente, Daten und XML 177
3.9.4 Web Services 186
3.9.5 „.NET“ 189
3.9.6 Java 2 Enterprise Edition (J2EE) 192
3.9.7 Component Object Model (COM) 194
3.9.8 Fazit 196
3.10 Webserver 196
3.10.1 Überblick 196
3.10.2 Einleitung 197
3.10.3 Internet Information Server 4.0 197
3.10.4 Ablösende Migration 200
3.10.5 Fortführende Migration 208

3.11 Datenbanken 210

3.11.1 Überblick 210

3.11.2 Einleitung 210

3.11.3 MS SQL Server 7.0 211

3.11.4 Ablösende Migration 216

3.11.5 Fortführende Migration 224

3.12 Groupware 225

3.12.1 Überblick 225

3.12.2 Einleitung 226

3.12.3 Ausgangslage – Microsoft Exchange 5.5 227

3.12.4 Ablösende Migration 232

3.12.5 Fortführende Migration 262

3.13 Office / Desktop 271

3.13.1 Überblick 271

3.13.2 Einleitung 272

3.13.3 XML und Interoperabilität zwischen Office-Anwendungen 273

3.13.4 Ausgangslage MS Office 279

3.13.5 Ablösende Migration 284

3.13.6 Fortführende Migration 305

3.13.7 Bewertung der Office-Migrationspfade 319

3.13.8 Weitere Desktopanwendungen 330

3.13.9 Integration von Windows-Anwendungen beim Einsatz von Linux-Client 339

3.14 Terminal-Dienste und Client-Konzepte 352

3.14.1 Überblick 352

3.14.2 Einleitung 352

3.14.3 Linux-Terminal-Server-Projekt 357

3.14.4 Terminalservices NX 358

3.14.5 Windows Terminal Services und Citrix 359

3.15 Hochverfügbarkeit 362

3.15.1 Ziele 362

3.15.2 Die „fünf Neunen“ und die Realität 363

3.15.3 Vorgehensweise 363

3.15.4 Kategorien von HA-Systemen 365
3.15.5 Proprietäre HA-Software 366
3.15.6 Open Source HA-Software 367

4 Rechtliche Aspekte 371
4.1 Einleitung 371
4.2 Methode 371
4.3 Notwendigkeit der Rechtsberatung im Einzelfall 372
4.4 Vertragsrecht 372
4.4.1 Ablösende Migration: Vertragsverhältnisse 372
4.4.2 Ablösende Migration: Vertrag mit Zwischenhändler 375
4.4.3 Ablösende Migration: Vertrag mit Rechtsinhabern 377
4.4.4 Vergleich fortführender und ablösender Migration 379
4.5 Urheberrecht 380
4.5.1 Ablösende Migration: Zulässigkeit von OSS-Lizenzen nach deutschem Urheberrecht 380
4.5.2 Ablösende Migration: Umfang der Rechtseinräumung bei OSS-Lizenzen 381
4.5.3 Ablösende Migration: Entgegenstehende Urheberrechte Dritter 382
4.5.4 Vergleich fortführender und ablösender Migration 384
4.6 Patentrecht 386
4.6.1 Allgemeines 386
4.6.2 Ablösende Migration: Entgegenstehende Patentrechte Dritter 386
4.6.3 Vergleich fortführender und ablösender Migration 387
4.7 Haftung und Gewährleistung 388
4.7.1 Allgemeines 388
4.7.2 Ablösende Migration: Vertragliche Haftung und Gewährleistung bei Überlassungsverträgen 388
4.7.3 Ablösende Migration: Vertragliche Haftung und Gewährleistung bei Open Source Lizenzverträgen 391
4.7.4 Ablösende Migration: Vertragliche Haftung und Gewährleistung bei Erstellung und Änderung von Freier Software 392
4.7.5 Ablösende Migration: Produkthaftung 393

4.7.6 Ablösende Migration: Verschuldensabhängige außervertragliche Haftung 393
4.7.7 Ablösende Migration: Mitverschulden 394
4.7.8 Vergleich fortführender und ablösender Migration 394
4.8 Vergaberecht 395
4.8.1 Allgemeines 395
4.8.2 Ablösende Migration: Neutrale Ausschreibung 396
4.8.3 Ablösende Migration: transparente Ausschreibung 397
4.8.4 Ablösende Migration: Vergabeentscheidung 398
4.8.5 Vergleich fortführender und ablösender Migration 399
4.9 Fazit 400
5 Wirtschaftlichkeitsbetrachtung 401
5.1 Vorwort 401
5.2 Einleitung 402
5.3 Methodische Grundsätze 404
5.3.1 Ziele und Rahmenbedingungen 405
5.3.2 Monetäre Analyse 407
5.3.3 Grundsätzliche Überlegungen zur Kostenerhebung 407
5.3.4 Nutzwert-Analyse 413
5.3.5 Vollkostenansatz 413
5.3.6 Vergleichbarkeit 414
5.3.7 Einsatzbereiche 415
5.4 Analyse der Ausgangssituation 416
5.4.1 Infrastruktur Server 417
5.4.2 Infrastruktur APC 417
5.4.3 Infrastruktur Netzwerk 418
5.4.4 Infrastruktur Druck 419
5.4.5 Serverdienste 419
5.4.6 Standardsoftware 420
5.4.7 Dokumentvorlagen und Makros 421
5.4.8 IT-Fachverfahren 422

5.5 Wirtschaftlichkeit nach WiBe 426
5.5.1 Überblick 426
5.5.2 Monetäre Wirtschaftlichkeit 426
5.5.3 Erweiterte Wirtschaftlichkeit nach WiBe 438
5.5.4 Strategische Dimension 439
5.6 Alternative Wirtschaftlichkeitsbetrachtung im monetären Bereich nach MiKoMa 440
5.6.1 Überblick 440
5.6.2 Grundstrukturen 441
5.6.3 Migrations- und Anbieterszenarien 447
5.6.4 Vergleichs- und Rentabilitätsrechnung 449
5.7 Neueinführung vs. Migration von Systemen 451
5.8 Gesamtergebnisse der Wirtschaftlichkeitsbetrachtung 452
6 Migrationsempfehlungen 454
6.1 Grundsätzliche Aussagen 454
6.1.1 Weg der Entscheidungsfindung 454
6.1.2 Grundsatzempfehlungen 455
6.2 Vollständig „Ablösende Migration“ 457
6.2.1 Architekturmodell 458
6.2.2 Mittlere und große Behörden 462
6.2.3 Spezialisierte Behörden mit IT-Dienstleistung 465
6.2.4 Kleine Behörden 467
6.3 Vollständig „Fortführende Migration“ 469
6.3.1 Minimierung des Grades an Integration, Bewahrung von Freiheitsgraden 472
6.3.2 Weitere Migrationspfade 473
6.4 Teilmigration 474
6.4.1 Punktuelle Migration 474
6.4.2 Serverseitige Teilmigration 476
6.5 Migrationswege 477
6.5.1 Schnelle Migration 477
6.5.2 Sanfte Migration 479
6.5.3 Kritische Erfolgsfaktoren 481

7 Anhang 495

7.1 Anhang -WiBe 495

7.1.1 Überleitungstabellen Kriterien WiBe 4.0 zu Kostenartengruppen MiKoMa 2.0 495

7.1.2 Matrix zur Soft- und Hardware-Kostenermittlung 497

7.2 Rechtsgrundlagen 501

8 Mitwirkende Autoren und Experten 506

8.1 Autoren 506

8.2 Experten 507

9 Abkürzungsverzeichnis 508

10 Glossar 519

11 Tabellenverzeichnis 525

12 Abbildungsverzeichnis 528

1 Einleitung

„Ein Produkt ersetzt ein anderes, wenn es den Abnehmern einen Umstellungsanreiz bietet, der stärker ist als die Umstellungskosten, oder der den Widerstand gegen die Umstellung überwindet. Ein Ersatzprodukt bietet einen Umstellungsanreiz, wenn es im Vergleich zu seinem Preis dem Abnehmer einen höheren Wert als das bislang benutzte Produkt bietet.“

M.E. Porter

1.1 Motivation

Die erste Auflage des Migrationsleitfadens hat großes Interesse und viel Zustimmung gefunden, stieß jedoch vereinzelt auch auf Kritik. Ein Teil dieser Kritik, so stellte sich heraus, basierte auf einem grundlegenden Missverständnis hinsichtlich der Motivation und Zielsetzung des Leitfadens. Um diesem Missverständnis entgegen zu wirken, haben sich der Herausgeber und die Autoren entschlossen, hier noch einmal deutlicher hervorzuheben, welches die Motivation für die Erstellung der ersten und der hier vorliegenden zweiten Auflage des Leitfadens ist und welche Ziele mit dem Leitfaden verfolgt werden.

Der Anlass für die Erstellung des Migrationsleitfaden liegt in dem durch den Wegfall des Supports für Windows NT und Exchange 5.5 entstandenen Handlungsdruck für die Verwaltung. Zu dem Zeitpunkt, als im Bundesministerium des Innern (BMI) der Entschluss für die Erstellung des Migrationsleitfadens gefasst wurde, basierte der überwiegende Teil der IT-Infrastrukturen in der öffentlichen Verwaltung auf Windows-NT-Systemen. Damit musste sich die öffentliche Verwaltung mittelfristig mit einer Umstellung wesentlicher Teile ihrer IT-Landschaft auseinandersetzen. Diese Situation verbunden mit langfristigen Zielen, die sich aus der politisch vorgegebenen IT-Strategie des Bundes ableiten,

- Softwarevielfalt,
- verbesserte Interoperabilität der Systeme,
- Unabhängigkeit von Plattformen und Herstellern sowie
- Offenheit und Flexibilität in den Systemen,

führten im BMI zu dem Entschluss, einen Leitfaden für die Migration der Basissoftwarekomponenten auf Server- und Arbeitsplatz-Systemen zu erstellen.

Vor diesem Hintergrund und in Umsetzung der strategischen Vorgaben ist neben einer Migration durch Fortführung der bestehenden Produktlinie der Firma Microsoft auch eine Migration durch Ablösung dieser Produkte mittels technologischer Alternativen in technischer und wirtschaftlicher Sicht zu betrachten. Als eine solche technologische Alternative sind – der Vorgehensweise des Deutschen Bundestages folgend – linuxbasierte Systeme, insbesondere Open Source Software

(OSS) und kommerzielle Software, die unter Linux betrieben werden kann, zu untersuchen. Das Wissen um diese Systeme ist in der öffentlichen Verwaltung noch wenig verbreitet, seine Beschaffung im Vergleich zu der Beschaffung von Informationen über Produkte der Firma Microsoft vergleichsweise schwierig. Dem will der Migrationsleitfaden abhelfen.

1.2 Über diesen Leitfaden

Aufgrund der in weiten Teilen doch erheblichen Veränderungen und Weiterentwicklungen bei den aktuellen Versionen der im Leitfaden behandelten Basissoftwarekomponenten auf Server- und Arbeitsplatz-Systemen hat sich der Herausgeber des Migrationsleitfadens dazu entschlossen, diesen eineinhalb Jahre nach der Erstveröffentlichung im Juli 2003 überarbeiten und fortschreiben zu lassen.

Dabei liegt der Grund für die nunmehr erfolgte Überarbeitung und Ergänzung des Migrationsleitfadens nicht etwa in einer veränderten Ausgangslage, sondern vielmehr in der Verfügbarkeit neuer Zielsysteme bei einem Großteil der betrachteten Komponenten. Der Leitfaden kann aber jeweils nur einzelne Komponenten betrachten und prüfen, basierend auf den Funktionalitäten der Ausgangslage, die als Minimalanforderungen für die Zielsysteme herangezogen werden, ob die verfügbaren Alternativen auch wirkliche Alternativen sind.

Genau wie in der ersten Auflage soll bereits mit dem Titel darauf aufmerksam gemacht werden, dass bereits durch den „natürlichen“ Lebenszyklus der Microsoft-Software eine Reihe von Migrationsentscheidungen zu treffen sind.

Da der Ausgangspunkt der Betrachtung die Ankündigung der Einstellung des Supports von Microsoft Windows NT ist, wird im Leitfaden zur Unterscheidung zwischen der Ablösung dieser Software durch OSS-Produkte und einer Umstellung auf nachfolgende Generationen von Microsoft-Produkten generell zwischen einer *ablösenden* und einer *fortführenden* Migration gesprochen. Im Fokus des Migrationsleitfadens steht auch weiterhin nicht die einseitige Ausrichtung auf Ablösung von bereits im Einsatz befindlichen Produkten, sondern die Unterstützung bei der Suche nach einer den Umständen entsprechenden optimalen Lösung.

Der Migrationsleitfaden richtet sich an die mit der Planung und Umsetzung der IT-Strategien und -Vorhaben in der Öffentlichen Verwaltung verantwortlichen Entscheider und IT-Verantwortlichen.

Der erste Teil (Kapitel 2) beschäftigt sich mit der Ausgangssituation der IT-Software, die zur Entstehung der Migrationsplanungen führte, und bietet einen Überblick über die Basis-Architektur der Microsoft-Software sowie der alternativen, auf Open Standards/Open Source-basierten Plattform. Die so genannte Karte der Systemlandschaft zeigt dabei die Abdeckung von Funktionen durch konkrete Produkte oder Lösungen und visualisiert die Zusammenhänge zwischen einzelnen Produkt- und Softwareschichten.

Der zweite Teil (Kapitel 3, 4 und 5) setzt sich mit einer potenziellen Migration oder einer Neueinführung der Systeme und Infrastrukturen auseinander. Die ein-

zelnen Einsatzbereiche der Software werden sowohl einer technischen als auch einer betriebswirtschaftlichen Betrachtung unterzogen. Neu im Leitfaden ist eine Betrachtung der rechtlichen Aspekte einer Migration (Kapitel 4).

Die technischen Betrachtungen (Kapitel 3) fokussieren sich auf die Identifikation und Beurteilung von Alternativlösungen für Microsoft-Produkte. Berücksichtigt wurden bei der Überarbeitung wesentliche Neuerungen und Entwicklungsfortschritte sowohl bei den möglichen Alternativlösungen als auch bei den Microsoft-Produkten. Insbesondere die Entwicklungen in den Office-Suiten und die auch und gerade dort wachsende der Bedeutung von XML bildeten einen Schwerpunkt in den Fortschreibungsthemen. Ein weiteres Augenmerk lag auf den Bewegungen der Angebote an Messaging- und Groupware-Lösungen. Marktveränderungen und technische Weiterentwicklungen waren Anlass diese Basissoftwarekomponenten noch mal etwas genauer in Augenschein zu nehmen. Weitere Teile, die genauer unter die Lupe genommen wurden, waren Middleware- und Integrationskomponenten, Datenbankmanagementsysteme, Verzeichnisdienste, Softwareverteilungslösungen als Teil des Systemmanagements und einiges mehr.

Im Abschnitt zur Wirtschaftlichkeitsbetrachtung (Kapitel 5) geht es weiterhin um die Frage nach dem betriebswirtschaftlich optimalen Weg mit dem Softwarewechsel umzugehen. Im Rahmen der Fortschreibung wurde die Vermittlung der Methoden zur Bestimmung des aus wirtschaftlicher Sicht optimalen Migrationspfades noch stärker akzentuiert und die Abgrenzung in der Verwendung der Methoden deutlicher herausgearbeitet.

Grund für die Aufnahme der Betrachtung von rechtlichen Aspekten (Kapitel 4) der Migration waren vor allem die kontroversen Diskussionen um das Thema Softwarepatente, welche aus Sicht der Autoren und des Herausgebers des Leitfadens zur einer nicht unerheblichen Verunsicherung bei den Entscheidern, insbesondere hinsichtlich des Einsatzes von Open Source Software, geführt hat. Mit den Betrachtungen in diesem Abschnitt soll diesen Verunsicherungen entgegen gewirkt werden. Sie befassen sich daher nicht nur mit den patent- und urheberrechtlichen Aspekten, sondern untersuchen auch die nicht minder interessanten Themen Vertragsrecht, Vergaberecht sowie Haftung und Gewährleistung.

Im dritten Teil (Kapitel 6) sind die Migrationsempfehlungen zu unterschiedlichen Behördenstrukturen als zusammenfassendes Ergebnis der technischen, rechtlichen und wirtschaftlichen Betrachtungen formuliert. Diese Empfehlungen beinhalten konkrete Vorschläge für kleine, mittlere, große und spezialisierte Behörden. Zusätzliche werden die Vor- und Nachteile verschiedener Migrationswege abgewogen. Abschließend sind im dritten Teil die kritischen Erfolgsfaktoren für Migrationsvorhaben dargestellt. Obwohl eine Softwareablösung nichts grundsätzlich Neues ist, bestätigen die Erfahrungen der in der Öffentlichen Verwaltung durchgeführten Migrationsprojekte, dass die Einführung von Software Produkten sorgfältig geplant werden muss und der Erfolg dieser Vorhaben wesentlich von der Vorbereitung der an der Migration beteiligten Mitarbeiter abhängt.

Den Behörden soll mit dem Migrationsleitfaden neben Informationen zu Produkten eine Unterstützung an die Hand gegeben werden, mit der sie eine für ihre individuelle Ausgangslage und ihre zukünftigen Anforderungen technisch und wirtschaftlich geeignete Lösung finden können. Der Migrationsleitfaden gibt dabei Hinweise, mit denen sicher gestellt werden kann, dass eine freie Wahl der Migrationsrichtung nicht allein durch finanzielle Argumente verhindert wird, wenn diese Entscheidung zu Produkt-, Hersteller- oder Plattformabhängigkeiten mit weit reichenden wirtschaftlichen Folgen führen kann.

Seit der ersten Veröffentlichung des Leitfadens hat sich in besonderer Weise bestätigt, was schon während der Arbeit an der ersten Ausgabe des Migrationsleitfadens erkennbar war, nämlich dass es sich um ein insgesamt sehr dynamisches und sich schnell veränderndes Themenfeld handelt. Die Anzahl der unter Linux verfügbaren Softwarepakete, sowohl unter GPL als auch kommerziellen Lizenzen, hat deutlich zugenommen. Ebenso stieg die Anzahl der Hersteller, die einem strategischen Commitment zur Linux-Strategie konkrete Produkte oder zumindest eine Release-Planung haben folgen lassen. Neben den großen Softwareanbietern wie SAP, Oracle, Sun oder IBM, stoßen kontinuierlich kleine und mittlere Softwareunternehmen mit einem wachsenden Angebot an Spezialanwendungen dazu. Dieser Entwicklung trägt die vorliegende Fortschreibung des Leitfadens ebenfalls Rechnung, um den Lesern weiterhin eine optimale Unterstützung bieten zu können.

Es bleibt aber letztendlich die Aufgabe der Leser, die eingangs erwähnten „Umstellungsanreize“ für sich zu finden. Die Autoren hoffen, dass der Migrationsleitfaden dabei eine gute und verlässliche Hilfe für technische, rechtliche sowie wirtschaftliche Überlegungen sein wird.

1.3 Hinweise zur Benutzung des Leitfadens

Den Lesern des Leitfadens werden im folgenden Abschnitt kurze Hinweise zum Umgang mit der internen Struktur des vorliegenden Dokumentes gegeben. Hiermit sollen die Leser eine Navigationshilfe bezüglich der für sie relevanten Inhalte innerhalb des recht umfangreichen Leitfadens erhalten. Dabei wird zwischen zwei Zielgruppen unterschieden, an die sich der Leitfaden richtet. Die eine Zielgruppe sind die mit der Planung und Umsetzung der IT-Strategien und -Vorhaben verantwortlichen Entscheider. Die zweite Gruppe ist die der IT-Verantwortlichen in den Behörden, für die detaillierte technische Betrachtungen von großem Interesse sein dürften. Beiden Zielgruppen wird die vollständig Lektüre der folgenden Hinweise empfohlen.

Unmittelbar im Anschluss an dieses Kapitel folgt ein Abschnitt, der sich speziell an die Entscheider wendet. Der Abschnitt „Hinweise für Entscheider“ enthält eine zusammenfassende Darstellung der wesentlichen Inhalte und Ergebnisse des Migrationsleitfadens in komprimierter Form.

Grundsätzlich sollte es kein Leser des Migrationsleitfadens versäumen, sich den ersten vier Abschnitten des Kapitels 2 zu widmen. Diese enthalten wichtige Be-

griffsbestimmungen, die für das Verständnis des Leitfadens von Bedeutung sind. Des Weiteren werden die Komponenten der einer Migration zugrunde liegenden IT-Landschaft beschrieben. Es werden die Komponenten nach einer ablösenden Migration wie auch nach einer fortführenden Migration dargestellt.

In Ergänzung dazu steht den Entscheidern, die sich einen Überblick über die Ergebnisse der technischen Betrachtungen zu den verschiedenen Migrationskomponenten verschaffen wollen, in Kapitel 3 jeweils zu Beginn eines Abschnitts eine zusammenfassende Darstellung der jeweiligen Zielsetzung und der Ergebnisse zur Verfügung.

Eine Zusammenfassung der Ergebnisse der wirtschaftlichen Betrachtungen liefert das Kapitel 5.8. Weiterhin enthält das Kapitel 6 entsprechende Empfehlungen zu ökonomischen Auswirkungen der unterschiedlichen Migrationsverfahren.

Die Wirtschaftlichkeitsbetrachtung (Kapitel 5) beleuchtet die finanziellen Aspekte von Migrationsprojekten und ist somit für Leser, die grundsätzliche strategische und wirtschaftliche Entscheidungen treffen müssen, von besonderer Relevanz. Das Hauptaugenmerk liegt nach der umfassenden Überarbeitung auf der Methodenvermittlung. Die beiden Methoden WiBe und MiKoMa werden auch nach ihrer Aktualisierung weiterhin als Alternativen betrachtet. Daneben gibt es Hinweise, unter welchen Bedingungen welche Methode am besten geeignet ist und wie sie angewendet werden sollte. Berechnungsbeispiele werden nur zu Verständniszwecken aufgeführt.

Neu im Leitfaden ist ein Abschnitt über die rechtlichen Aspekte (Kapitel 4), insbesondere im Zusammenhang mit dem Einsatz von Open Source Software. Damit wird der teilweisen Verunsicherung der Nutzer durch die Diskussionen um Urheberrecht und Patentschutz Rechnung getragen. In diesem Zusammenhang stehen ebenso rechtliche Fragen hinsichtlich der Vergabe, der Haftung und Gewährleistung sowie zur Vertragsgestaltung. Soweit dies im vorliegenden Rahmen möglich ist, werden entsprechende Antworten und Hinweise im Kapitel „Rechtliche Aspekte“ gegeben.

Für eine vertiefende Lektüre der für eine Behörde relevanten Empfehlungen empfiehlt es sich, einen Blick auf das Kapitel 6 zu werfen. Hier werden für unterschiedliche Migrationsszenarien[1] differenziert nach unterschiedlichen Behördenstrukturen[2] Empfehlungen für eine Kombination von geeigneten Systemkomponenten ausgesprochen.

Damit dürften den Entscheidern die wesentlichen und für sie relevanten Informationen zur Verfügung stehen. Es bleibt allerdings jedem Entscheider unbenommen, sich auch den weiteren Inhalten des Leitfadens zu widmen.

---

1 Vollständig ablösende Migration, vollständig fortführende Migration und Teilmigration.

2 Kleine, mittlere, große und spezialisierte Behörde.

Für die IT-Verantwortlichen dürften grundsätzlich alle Informationen des Leitfadens von Interesse sein. Der Leitfaden ist so aufgebaut, dass im Anschluss an die Einleitung das Kapitel 2 jene allgemeinen Informationen enthält, die als Grundlage für das Verständnis des gesamten Leitfadens von Interesse sind. Neben den bereits oben erwähnten ersten vier Abschnitten sind in den daran anschließenden Abschnitten Informationen über verschiedene Linux-Distributionen sowie Open Source Lizenzmodelle zu finden.

Die technischen Detailbetrachtungen in Kapitel 3 stellen für die IT-Verantwortlichen in Kenntnis ihrer jeweiligen hausspezifischen technischen Anforderungen wohl mit die wichtigste Informationsquelle dar, wenn es darum geht, Hinweise auf u.a. folgende Fragen zu bekommen:

- Was ist technisch machbar bzw. wo bestehen Probleme?
- Wie können bekannte Probleme ggf. gelöst bzw. umgangen werden?
- Worauf ist bei einer Migration einer Komponente aus technischer Sicht zu achten?
- Welche Funktionalitäten können auch nach einer Migration weitergenutzt werden bzw. wo gibt es Einschränkungen?

Innerhalb der Abschnitte werden die jeweiligen Systemkomponenten aus technischer Sicht betrachtet. Es werden die technische Ausgangsituation und daran anschließend die Aspekte der ablösenden und fortführenden Migration beschrieben. Der technisch versierte und interessierte Leser erhält einen Überblick über die unterschiedlichen Technologien. Er hat die Möglichkeit, sich detailliert über die Eignung der unterschiedlichen Lösungen und Produkte zu informieren. Speziell für Leser, die bisher nicht oder kaum Kontakt zu linuxbasierten Technologien hatten, bieten die Abschnitte zur ablösenden Migration vielfältige Informationen an.

Der Leitfaden verfolgt dabei nicht das Ziel, die immer notwendige präzise Definition der spezifischen fachlichen Anforderungen der einzelnen Behörden an einzelne Komponenten zu ersetzen. Auch hat er nicht den Anspruch, einen generischen Anforderungskatalog für IT-Infrastrukturen in der Verwaltung aufzustellen, um daran die Leistungsfähigkeit der Alternativen zu bewerten. Dafür sind die Anforderungen in den verschiedenen Behörden viel zu unterschiedlich. Daher kann es auch nicht Absicht des Leitfadens sein – weder in der ersten noch in der vorliegenden zweiten Version - integrierte Gesamtlösungen detailliert zu betrachten, da auch hier zunächst die besonderen Anforderungen zu berücksichtigen sind.

Innerhalb des Kapitels 6 münden die technischen und wirtschaftlichen Betrachtungen der vorangestellten Kapitel in konkrete Empfehlungen. Dargestellt werden unterschiedliche Szenarien, die differenziert in Abhängigkeit von der jeweiligen Größe und Spezialisierung der Behörde erläutert werden. Der Leser hat die Möglichkeit, sich entsprechend seiner Bedürfnisse und der konkreten Ausgangssituation gezielt zu informieren.

1.4 Hinweise an die Entscheider

1.4.1 Grundsätzliche Empfehlungen

Wie bereits im vorangegangenen Abschnitt angedeutet, werden im Migrationsleitfaden grundsätzlich beide Wege, sowohl der ablösenden als auch der fortführenden Migration, analysiert. Die Anzahl der Szenarien, in denen eine ablösende Migration unter Einsatz von Open Source Produkten für die Behörden vorteilhaft ist, hat zugenommen.

Die Ergebnisse des Leitfadens beziehen sich in erster Linie auf eine Ausgangslage, wie sie in den meisten Behörden noch vorzufinden ist: Für diese sind Windows NT 4 als Betriebssystem sowie die darauf aufsetzenden Microsoft-Softwareprodukte, wie z.B. MS Exchange 5.5, Internet Information Server 4 und MS SQL Server 7 charakteristisch.

1.4.2 Fortführende und ablösende Migration

Diese Konfiguration bildet die Ausgangssituation für die fortführende Migration innerhalb der Microsoft-Produktfamilie. Hier wird insbesondere die Umstellung der o.g. Produkte auf Windows 2003, zum Teil noch Windows 2000 und die entsprechenden Produktserien betrachtet. Für die Clients steht Windows XP im Fokus der Betrachtung. Die Ausrichtung auf Windows 2000/2003 bedeutet nicht, dass alle, die schon eine Umstellung nach Windows 2000/2003 vollzogen haben, den Leitfaden nun beiseite legen sollten. Auch für diese Behörden liefert der Leitfaden – sowohl in den technischen Betrachtungen als auch in den Empfehlungen – wichtige Erkenntnisse. Die Beachtung dieser und der daran anknüpfenden Maßnahmen zur Reduktion der internen Abhängigkeitsgrade sorgt dafür, dass alle Optionen bezüglich zukünftiger Migrationen offen gehalten werden können. Diese Empfehlungen richten sich primär an jene Behörden, die zum einen gerade erst eine Migration nach Windows 2000/2003 durchgeführt haben, und zum anderen an die Behörden, welche die Microsoft-Produktlinie vorläufig weiterführen möchten oder (aus unterschiedlichen Gründen) weiterführen müssen.

Der Blick auf die ablösende Migration zeigt, dass durch die Vielzahl und Vielfalt der Lösungen eine Differenzierung der Ergebnisse und Empfehlungen sinnvoll ist. Insbesondere die Größe, die Intensität der IT-Nutzung und der „Spezialisierungsgrad“ bei Behörden, die selbst IT-Dienstleistungen für andere Behörden erbringen, sind die wesentlichen Kriterien für die Auswahl der richtigen Lösung. Neben der Auswahl der passenden Produkte und Konfigurationen müssen die richtigen Migrationsszenarien gefunden werden. Der Leitfaden unterscheidet an dieser Stelle zwischen punktueller, breiter und vollständiger Migrationen – abhängig von dem „Flächendeckungsgrad“ innerhalb der IT. „Punktuell“ meint die Ablösung einzelner Komponenten der IT-Landschaft, wie z.B. die MS Office Suite oder MS Exchange. „Partiell“ meint die Ablösung der gesamten Serverinfrastruktur und unter Beibehaltung bzw. Fortführung der Windows Clients. Vollständig meint schließlich die Ablösung der gesamten Windows-Systeme durch eine linuxbasierte Systemlandschaft.

Die Empfehlungen des Migrationsleitfadens zeigen hier, welche Lösungsausprägungen für welche Anforderungen und welche Behördenstruktur aus heutiger Sicht zu bevorzugen sind.

1.4.3 Vergleichbarkeit von Alternativen

Fest steht, dass sich nicht alle Funktionen von Windows und anderen Microsoft-Produkten spiegelartig unter Linux mit Open Source Software bzw. kommerzieller Software für Linux abbilden lassen. Es lässt sich jedoch sowohl aus Erfahrungen der Nutzer beider Plattformen als auch aus den durchgeführten Migrationsprojekten die Erkenntnis bestätigen, dass beide Software-Alternativen grundsätzlich vergleichbar sind.

Da es im Einzelfall durchaus auf Spezialfunktionen und konkrete Eigenschaften ankommen kann, empfiehlt es sich für jede Behörde, die Kritikalität abweichender Funktionalitäten für sich zu bewerten. Solche Abweichungen finden sich in erster Linie im Bereich der Officeanwendungen, insbesondere in der Integration von Fach- und Officeanwendungen, sowie in der Kompatibilität bezüglich des Dokumentenaustausches zwischen Microsoft Office und OpenOffice.org bzw. StarOffice. Die Kompatibilitätsprobleme führen dazu, dass die gemeinsame Bearbeitung von Dokumenten mit OpenOffice.org bzw. StarOffice und MS Office nur sehr eingeschränkt möglich ist. Im Prinzip ist eine gemeinsame Bearbeitung nur auf Inhaltsebene möglich. Dies ändert sich auch nicht grundsätzlich durch die Erweiterung der XML-Unterstützung in Office 2003 auf Word und Excel.

Aus den technischen Betrachtungen ergibt sich, dass es - insbesondere im Behördenumfeld - für die bestehenden Windows-Systemkomponenten und -Infrastrukturdienste sowie für den Windows-Desktop insgesamt adäquate Open Source Lösungen und/oder kommerzielle Lösungen für linuxbasierte Systeme gibt.

1.4.4 Künftige Schwerpunkte

Um die technische Betrachtung mit einem notwendigen Zukunftsausblick zu versehen, wird über die beschriebene Ausgangssituation hinaus die Bedeutung der Komponenten betrachtet, die in der neuen Softwarearchitektur von Microsoft eine zentrale Rolle spielen. Hierzu zählen vor allem das .NET Framework mit seinen wesentlichen Bestandteilen Web-Services und mit besonderem Augenmerk XML.

Zusammenfassend lassen sich folgende Erkenntnisse formulieren:

- Sowohl das .NET-Framework als auch die Alternative Java/J2EE bieten grundsätzlich zwei Möglichkeiten, die Wiederverwendbarkeit von Komponenten und die Interoperabilität zwischen Plattformen und Anwendungen zu realisieren.
- Die über die Verwendung des gleichen Komponentenmodells (COM+ bei Microsoft und JavaBeans in Java) erreichbare Wiederverwendbarkeit wird hier aufgrund ihrer Bindung an die Laufzeitumgebung und/oder Programmiersprachen als *tiefe Integration* bezeichnet. Die mit einem Komponen-

tenmodell erstellten Anwendungen sind nur innerhalb einer Plattform verwendbar.

- XML gehört generell und nicht nur als Grundlage für den Einsatz von Web-Services als Dokument- und Datenaustauschformat die Zukunft.
- Web-Services können aufgrund ihrer Unabhängigkeit von einer konkreten Laufzeitumgebung und Nutzung von Protokollschnittstellen für eine *flache Integration* von Diensten verwendet werden. Die auf Web-Services basierten Dienste können über die Plattformgrenzen hinweg eingesetzt werden.
- Eine generelle Empfehlung für das Komponentenmodell beim *tiefen Integrationsmodell* wurde bereits in der Standardisierungsempfehlung SAGA formuliert und legt JSE/J2EE aufgrund der grundsätzlichen Plattformunabhängigkeit als obligatorisches Komponentenmodell fest. Nur in begründeten Fällen (z.B. bei erheblichen Wirtschaftlichkeitsvorteilen) soll von dieser zu bevorzugenden Technologie abgewichen werden (z.B. zugunsten des .NET-Frameworks).

1.4.5 Rechtliche Aspekte

Die intensiven Diskussionen um die Relevanz patent- und urheberrechtlicher Bestimmungen im Jahre 2004 haben bei einigen Entscheidern die Unsicherheit geweckt, ob die Einführung von Open Source Software und Linux aufgrund rechtlicher Belange nicht ein zu großes Risiko darstellt. Dies hat dazu geführt, dass die Betrachtung rechtlicher Aspekte einer Migration, insbesondere im Hinblick auf den Einsatz von Open Source Software in den Migrationsleitfaden aufgenommen wurde. Betrachtet wurden Aspekte

- des Vetragsrechts,
- des Urheber- und Patentrechts,
- des Vergaberechts sowie
- von Haftung und Gewährleistung.

Im Gesamtergebnis lässt sich keine eindeutige rechtliche Überlegenheit für eine der beiden betrachteten Migrationsrichtungen erkennen. Der Einsatz welcher Software nun im Einzelfall rechtlich vorteilhafter ist, hängt insbesondere von der vorgesehenen Art der Nutzung der Software, den möglichen Vertragspartnern und den hierbei ausgehandelten Konditionen ab. Daher ist es notwendig, dies jeweils im Einzelfall zu prüfen, eine pauschale Empfehlung zugunsten der einen oder anderen Richtung kann im Rahmen des Leitfadens nicht gegeben werden. Allerdings liefert Kapitel 4 umfassende Hinweise zu Einzelkriterien, die im Rahmen einer Einzelbewertung berücksichtigt werden sollten.

1.4.6 Wirtschaftlichkeit

Im Fokus der Wirtschaftlichkeitsbetrachtung des Migrationleitfadens liegen zwei wesentliche Schwerpunkte:

- Formulierung von Methoden und Hilfen zur Ermittlung von behördenspezifischen Wirtschaftlichkeitsbetrachtungen und projektbezogenen Berechnungen von Migrationskosten sowie
- Ermittlung von grundsätzlichen Aussagen zur Wirtschaftlichkeit von Open Source Produkten.

Im Rahmen der im Migrationsleitfaden beschriebenen Methoden für Wirtschaftlichkeitsbetrachtungen können die besonderen (z.T. sehr behördenspezifischen) Integrationsaspekte nicht tiefergehend betrachtet werden können. Eine Berücksichtigung dieser Aspekte kann aufgrund der Zielsetzungen des Migrationsleitfadens nur im Rahmen der behörden- und damit anforderungsspezifischen Wirtschaftlichkeitsbetrachtungen hinreichend qualifiziert erfolgen.

Da der Leitfaden am Ende aber offen lässt bzw. auch offen lassen muss, welcher Migrationspfad im Einzelfall der wirtschaftlichere ist, dürfte dies für die Leser des Leitfadens keine Beeinträchtigung darstellen.

Mit der WiBe 4.0[1] und einer auf die Gegebenheiten der Migrationsprojekte abgestimmten Migrationskostenmatrix werden zwei methodische Ansätze zur Rentabilitätsberechnung der Umstellungsvorhaben beschrieben. Das Hauptaugenmerk liegt in der vorliegenden Fassung des Migrationsleitfadens auf der Methodenvermittlung. Berechnungsbeispiele werden nur und ausschließlich zu Verständniszwecken eingefügt.

1.5 Informationsbasis

Die Ergebnisse dieses Leitfadens beruhen im Wesentlichen auf:

- Erfahrungen aus durchgeführten Migrationsprojekten
- Erfahrungen aus der Entwicklung von OSS- und COLS-Produkten
- Einbindung von Experten-Know-how
- Machbarkeitsstudien zu geplanten Migrationen
- Migrationsfeinkonzepten
- Migrationsdokumentationen
- Fach- und Produktliteratur

Die für den Leitfaden wichtigen, fachlich relevanten Informationen wurden über

- intensive Dokumentenanalyse
- Interviews und deren Auswertung

[1] IT-WiBe 21 – Empfehlungen zur Durchführung von Wirtschaftlichkeitsbetrachtungen in der Bundesverwaltung, insbesondere beim Einsatz der IT, Version 3.0 – 2001, Schriftenreihe der KBSt, Band 52, Mai 2001.

- Workshops zu speziellen Themenkomplexen sowie
- die direkte Beteiligung zahlreicher Experten und Softwarehersteller

erlangt.

Die aus den o.g. Informations- und Wissensquellen gewonnenen Inhalte und Erkenntnisse wurden für die einzelnen Problemstellungen, die im Leitfaden behandelt werden, aufgenommen, themenspezifisch zusammengeführt, analysiert und bewertet.

1.6 Ausblick

Die dieser Version des Migrationsleitfadens zu Grunde gelegte weitgehend einheitliche Ausgangssituation wird in der öffentlichen Verwaltung schon in naher Zukunft nicht mehr gegeben sein, eine klare Trennung zwischen fortführender Migration (Windows nach Windows) und ablösender Migration (Windows nach Linux) mithin nicht mehr möglich. Zukünftig gibt es viele unterschiedliche Ausgangslagen für Windows (NT, 2000, 2003, XP) und für Linux (Debian, Suse, Red Hat, …). Deshalb wird der MLF zu einem Leitfaden weiter entwickelt werden, der den Behörden Hilfestellungen an die Hand gibt, ihre IT-Infrastrukturen so aufzubauen und zu betreiben, dass sie jederzeit ohne übermäßige Aufwände in der Lage sind, sowohl einzelne Elemente der IT-Infrastruktur als auch diese insgesamt zu migrieren.

Konkret wird es notwendig sein, den Migrationsleitfaden in einen Leitfaden für den Aufbau und Betrieb von flexiblen, offenen und wirtschaftlichen IT-Infrastrukturen zu überführen. Der MLF soll seiner Zielgruppe, IT-Entscheider und IT-Verantwortliche in der Verwaltung,:

- Kriterien für die Auswahl geeigneter Softwarekomponenten an die Hand geben,
- Hilfestellung für den Betrieb von Softwarekomponenten liefern, welche die Flexibilität, Offenheit und Wirtschaftlichkeit sichern helfen,
- Probleme und Möglichkeiten für die Migration einzelner Komponenten sowie ganzer Infrastrukturen aufzeigen und
- die neuesten technischen Entwicklung sowohl bei den führenden kommerziellen SW-Herstellern gleichermaßen wie bei den Open Source-Lösungen aufnehmen.

Darüber hinaus ist es erforderlich, neben den im MLF schon betrachteten Basissoftwarekomponenten auch weitere wichtige Elemente von IT-Infrastrukturen, wie z.B. Fachanwendungen, Dokumentenmanagementsysteme, Contentmanagementsysteme, erweiterte Groupwareumgebungen usw. aufzunehmen.

2 Erläuterungen zum Verständnis alternativer Migrationspfade

2.1 Wichtige Definitionen

Im Alltag werden Begriffe gebraucht, ohne dass über ihre inhaltliche Bedeutung ein einheitliches Verständnis herrscht. Dies gilt unter anderem für Begriffe wie Open Source Software, Freie Software oder Free Software, Proprietäre Software, kommerzielle Software u.a. Darüber hinaus führt der Leitfaden eigene Begriffe ein.

Damit beim Studium des Leitfadens keine Missverständnisse entstehen, werden nachfolgend die wichtigsten Begriffe kurz definiert.

2.1.1 Open Source Software, Free Software, Freie Software

Die Begriffe „Open Source Software“ und „Free Software“ oder „Freie Software“ werden innerhalb dieses Migrationsleitfadens synonym angewendet. Im Rahmen des Leitfadens wird hierfür die Abkürzung OSS eingesetzt.

OSS erlaubt es jedem, den frei verfügbaren Quellcode zu lesen und zu modifizieren. Diese Offenheit gibt den Nutzern die Möglichkeit, aus dem Quellcode selbst zu lernen bzw. ihn an die persönlichen Bedürfnisse anzupassen. Die Software steht frei zu Verfügung und es fallen für die Benutzer keine Lizenzkosten an. Sie darf in der modifizierten Form kopiert und weitergegeben werden. Die Freiheit der Software wird durch die entsprechenden Lizenzen geregelt bzw. gewahrt. Die wichtigsten dieser Lizenzmodelle sind in Kapitel 2.4 beschrieben.

OSS darf nicht mit jener Software verwechselt werden, die zwar kostenfrei verfügbar ist, aber nicht durch eigene Anpassungen und Ergänzungen modifiziert werden darf bzw. deren Lizenz es verbietet, sie zu kommerziellen Zwecken einzusetzen.

2.1.2 Proprietäre Software

Proprietäre[1] Software ist keine OSS, sie steht im Eigentum einer Person oder einer Organisation. In der Regel handelt es sich dabei um den Hersteller der Software (Urheberrecht). Die Nutzung der Software unterliegt den Lizenzbestimmungen, die der Eigentümer der Software festgelegt hat. Dabei ist ihre Vervielfältigung, Weiterverbreitung und Modifizierung meist untersagt.

Unter der Voraussetzung, dass die entsprechenden Lizenzbedingungen akzeptiert werden, wird sie in einigen Fällen auch kostenlos angeboten.

[1] lateinisch: Eigentümer

2.1.3 Commercial Linux Software

Commercial Linux Software (COLS) fasst die Gruppe proprietärer Software zusammen, die unter dem Betriebssystem Linux eingesetzt werden kann. In der Regel zeichnet sie sich durch Nutzung von Standards und die dadurch bedingte Interoperabilität sowie durch wohldefinierte Schnittstellen aus.

2.1.4 Ablösende Migration

Im vorliegenden Leitfaden wird zwischen ablösender und fortführender Migration differenziert. Worin unterscheiden sich diese beiden Migrationsarten?

Mit ablösender Migration wird der Wechsel von Windows-Anwendungen, -Diensten sowie ganzen windowsbasierten Systemumgebungen hin zu OSS- oder COLS-Plattformen verstanden. Beispiele sind:

- von Windows NT hin zu Linux
- von MS Office hin zu OpenOffice.org
- von MS SQL Server hin zu Oracle

2.1.5 Fortführende Migration

Unter fortführender Migration ist die Fortführung der Microsoft-Produktlinien zu verstehen, also die Migration von z.B. NT 4 nach Windows 2000, Windows XP oder Windows 2003. Beispiele sind:

- von Windows NT 4 hin zu Windows 2000/2003
- von MS Office 97 hin zu MS Office 2003

2.2 Migrationspfade

Viele Behörden und Organisationen stehen gegenwärtig vor der Entscheidung, wie sich ihre zukünftigen IT-Systemlandschaften in den kommenden Jahren entwickeln sollen. Die Gründe dafür sind vielfältig:

- Auslaufender Hersteller-Support für wesentliche Produkte
- Erweiterte technische Anforderungen
- Konsolidierung der bestehenden Systemlandschaften
- Strategische Ziele, wie beispielsweise verstärkte Herstellerunabhängigkeit und erhöhte Interoperabilität.

Ihnen stellt sich somit aktuell die Frage, welche Systeme und Komponenten zukünftig die Basis ihrer IT-Struktur bilden sollen. Der Migrationsleitfaden analysiert und untersucht die folgenden grundlegenden Migrationspfade:

- Ablösende Migration unter Einsatz von Linux und Open Source Software (OSS)
- Ablösende Migration unter Einsatz von Linux/Open Source Software und Nutzung von kommerziell verfügbaren Linux-Produkten (COLS)
- Fortführende Migration durch MS Windows 2000 / 2003 sowie Folgegenerationen und die darauf basierenden Microsoft-Anwendungen und -Systeme.

Zudem müssen Möglichkeiten für gemischte Migrationspfade betrachtet werden, da nicht davon auszugehen ist, dass für alle Komponenten der jeweiligen Ausgangslage OSS-/COLS-Alternativlösungen empfohlen werden können; sei es aus technischen und/oder wirtschaftlichen Gründen.

Im Rahmen dieses Leitfadens können keine diesbezüglich allseits umfassenden Betrachtungen durchgeführt werden. Dies ist sowohl aufgrund des Umfanges der zu betrachtenden IT-Landschaften als auch aufgrund der jeweils sehr spezifischen Anforderungen einzelner Behörden nicht leistbar. Der Migrationsleitfaden soll vielmehr in den wesentlichen Kernfragen, die von der Mehrheit aller Behörden gleichermaßen gestellt werden, Antworten und Hilfestellungen zur Entscheidungsfindung liefern.

2.2.1 Ausgangslage Microsoft Windows

Die Abbildung Bild 1 stellt die Microsoft Systemlandschaft dar, die in vielen Behörden und Organisationen so oder in vergleichbarer Form anzutreffen ist. Das Bild gibt einen Überblick über die Dienste und Softwaremodule, welche Bestandteil der angenommenen Ausgangssituation für die jeweiligen Migrationsbetrachtungen sind. Innerhalb des Kapitels 3 erfolgt zu jeder dieser Komponenten zunächst eine technische Betrachtung der Ist-Situation hinsichtlich der verfügbaren Funktionalitäten und Besonderheiten mit Blick auf eine durchzuführende Migration. Im Anschluss daran werden jeweils eine oder ggf. auch mehrere adäquate Lösungen bezüglich einer ablösenden Migration aus technischer Sicht untersucht. Im dritten Schritt geht es um die technische Betrachtung der fortführenden Migration. Und als vierter und letzter Schritt der technischen Betrachtungen erfolgen schließlich eine Bewertung und eine Empfehlung für den einen oder den anderen Migrationspfad.

Bild 1: Systemlandschaft – Ausgangssituation

Bei der Erstellung dieses Leitfadens war es notwendig, an verschiedenen Stellen Annahmen bezüglich der Ausprägung einer IT-Infrastruktur zu treffen. Soweit im Rahmen der technischen und wirtschaftlichen Betrachtungen keine anderen Annahmen getroffen werden, gelten die folgenden.

2.2.1.1 Serverplattform

Es wird davon ausgegangen, dass die bestehende Ausgangssituation in den Behörden auf einem der beiden gängigen NT-Domänenmodelle beruht:

- Umgebung mit einer NT-Domäne, in der Benutzer- und Computerkonten verwaltet werden.
- Umgebung mit einer NT-Account-Domäne, welche die Benutzerkonten beinhaltet und mehreren Ressource-Domänen, welche die Computerkonten verwalten und der Account-Domäne vertrauen.

Innerhalb dieser Umgebung werden unterschiedliche Infrastruktur-Dienste, Anwendungen und Integrationskomponenten auf Basis von Windows NT 4 Server bereitgestellt.

Die zentralen Infrastruktur-Dienste, die innerhalb des Leitfadens betrachtet werden, sind:

- Anmeldedienst – Authentifizierung
- Dateidienste
- Druckdienste
- Netzwerkdienste
- Systemmanagementdienste.

Bezüglich der Serveranwendungen stehen aufgrund ihrer großen Verbreitung in den öffentlichen Verwaltungen die folgenden Lösungen im Fokus des Leitfadens:

- Internet Information Server (IIS) in der Version 4 als Webserver für Intranet- und Internetauftritte
- Exchange 5.5 als Groupware- und Messaging-Lösung
- SQL-Server 7 als Datenbankenmanagementsystem für die meisten Datenbankanwendungen.

Die Verknüpfung und Integration der verschiedenen Dienste und Anwendungen erfolgt unter Windows bisher in der Regel auf Basis

- des Component Object Models (COM) und
- des dazugehörigen Dienstes Distributed COM (DCOM).

Die Bereitstellung von Windows NT 4 Services kann mittels zwei unterschiedlicher Betriebssystemvarianten erfolgen:

- Windows NT 4 Server
- Windows NT4 Server Enterprise Edition.

Die zweite Variante (Enterprise Edition) ermöglicht die Realisierung der Dienste durch zwei Knoten (Server) in einem Cluster.

2.2.1.2 Clientplattform und Anwendungen

Auf der Anwenderseite ist davon auszugehen, dass in erster Linie Windows NT 4 Workstation als dominierendes Betriebssystem zum Einsatz kommt. Ältere Betriebssystemvarianten wie Windows 95 oder 98 werden bei der Betrachtung vernachlässigt. Auf Basis des Betriebssystems wird als wichtigste Anwendungssoftware die Microsoft Office Suite verwendet. Dabei sind sowohl die Version 97 als auch die Version 2000 als die derzeit gängigen Varianten zu betrachten. Die Anwender setzen sie für ihre tägliche Aufgabenbewältigung ein. Dafür stehen ihnen in der Regel Programme zur Textverarbeitung, Tabellenkalkulation, Präsentationsunterstützung und die Nutzung der Messaging- bzw. Groupware-Funktionen zur Verfügung.

Neben diesen Standardprodukten werden vielfältige Fachanwendungen zur Erfüllung behördenspezifischer Aufgaben auf den Systemen betrieben, die häufig stark in den Windows-Desktop integriert sind. Sie müssen hinsichtlich einer Mig-

ration im Detail betrachtet werden. Da diese Anwendungen von der Migration der grundlegenden IT-Infrastruktur essentiell betroffen sind, müssen abhängig von der Anzahl und Komplexität Strategien für Übergangslösungen erarbeitet werden. Einige Vorschläge und Empfehlungen zur Vorgehensweise werden im Leitfaden dargestellt.

Abschließend gibt es noch eine Reihe weiterer Standardanwendungen und Werkzeuge (z.B. Dateimanager, Packer), die den Benutzern bei der Erledigung ihrer täglichen Arbeiten zur Verfügung stehen. Sie werden auch in der neuen Systemlandschaft von den Anwendern benötigt.

2.2.2 Systemlandschaft bei ablösender Migration

Abbildung Bild 2 gibt einen Überblick über eine alternative linuxbasierte Systemlandschaft. Gezeigt werden die wichtigsten Systeme und Anwendungen, die für eine ablösende Migration in Frage kommen können.

In der letzten Dekade haben viele Softwarehersteller ihre Produkte und Lösungen für Linux entwickelt oder auf Linux portiert. Neben großen Anbietern wie IBM, SUN oder Oracle, kann an dieser Stelle auch auf zahlreiche kleinere Unternehmen mit Speziallösungen verwiesen werden. Aufgrund der in Bereich der kommerziellen Software vorhandenen Informations- und Vertriebsbasis müssen diese Produkte in Bezug auf die Machbarkeit nicht näher betrachtet werden. Der Migrationsleitfaden konzentriert sich in erster Linie auf die zum Teil weniger bekannten Open Source Softwarelösungen und auf die Lösungen, die in kritischen Bereichen erst seit kurzem ablösende Migrationen möglich machen.

Abbildung Bild 2 macht deutlich, dass für bestimmte Aufgabengebiete mehr als eine alternative Lösung zur Verfügung steht. Bei den technischen Betrachtungen rücken daher die klassischen Open Source Softwarelösungen zunächst in den Vordergrund. Dort, wo es keine adäquaten Open Source Anwendungen gibt, werden Softwarelösungen betrachtet, die eine proprietäre Alternative unter Linux darstellen und gleichzeitig auf offenen Standards beruhen.

Bild 2: Systemlandschaft – Ablösende Migration

2.2.3 Systemlandschaft bei fortführender Migration

Bei der fortführenden Migration steht die Ablösung der vorhandenen Windows NT4-Umgebung durch neuere Versionen im Vordergrund. Wie das Bild 3 verdeutlicht, sollen dabei die Produkte der 2000er/2003er Versionen im Vordergrund stehen. Ausgehend vom Windows-Server mit seinen Infrastrukturdiensten werden im Kapitel 3 die technischen Besonderheiten und die für eine Migration notwendigen technischen und konzeptionellen Maßnahmen für die einzelnen Dienste und die Serverprodukte betrachtet. Des Weiteren sollen die Auswirkungen der technischen Änderungen und Neuerungen analysiert und bewertet werden.

Neben der Serverseite erfolgt genau wie bei der ablösenden Migration eine Betrachtung des Desktops. Hierbei steht jedoch Office 2003 im Focus der Untersuchung.

Bild 3: Systemlandschaft – Fortführende Migration

2.2.4 Interne Abhängigkeiten in der Microsoft-Systemlandschaft

Systemarchitekturen, die vorwiegend auf den Microsoft-Produkten basieren, weisen unterschiedlich starke interne Abhängigkeiten auf. Im folgenden Abschnitt werden einige der internen Abhängigkeiten innerhalb einer von Microsoft geprägten Infrastruktur dargestellt.

Eine recht offensichtliche Abhängigkeit besteht darin, dass Anwendungssoftware von Microsoft sich nur auf Microsoft-Betriebssystemen installieren und betreiben lässt. Dies gilt für die Serveranwendungen der Back-Office-Produktpalette (also MS SQL Server, MS Exchange usw.) und mit wenigen Ausnahmen (Office 98 für MacOS, Internet Explorer 4 für Unix) auch für die Desktopanwendungen (z.B. Office) und systemnahe Clientsoftware (z.B. MS SQL Clientkomponenten).

Serveranwendungen im Allgemeinen benötigen in der Regel eine Benutzerverwaltung, um die Anwender zu authentifizieren und den Zugriff auf Ressourcen zu autorisieren. Microsoft bietet verschiedene Varianten hinsichtlich der zu verwendenden Benutzerdatenbank an. Am Beispiel des MS SQL Servers seien hier die Varianten aufgezählt.

- Variante A:
  Es wird eine SQL-spezifische Benutzerverwaltung verwendet.
- Variante B:
  Es wird die lokale Benutzerdatenbank des Serverbetriebssystems verwendet.
- Variante C:
  Es wird die Benutzerdatenbank einer Windows-Domänenstruktur verwendet, sofern der Server Mitglied dieser Struktur ist. Diese Variante wird seit dem Erscheinen von Windows NT für nahezu alle Serveranwendungen von Microsoft angeboten und ermöglicht in einer reinen Microsoftumgebung ein Single Sign On für den Anwender.
- Variante D:
  Eine Variante, in der Authentifizierungs- und Autorisierungsinstanzen anderer Hersteller verwendet werden können, wird nicht angeboten.

Mit Windows 2000 und Folgesystemen verlagert Microsoft die Benutzerverwaltung und Authentifizierung hin zu Verzeichnisdiensten (s.u.) und offenen Standards wie Kerberos und LDAP, ohne jedoch fremde Instanzen zuzulassen.

Bezüglich der Windows-NT-4.0-Welt sind noch weitere Abhängigkeiten hinsichtlich der Benutzerverwaltung zu erwähnen. Microsoft Exchange-Umgebungen (Version 4 bis 5.5) z.B. sind ohne Windows NT Domänenstruktur nicht realisierbar. Ein anderes Beispiel für die zwingend notwendige NT Domäne ist die Funktionalität der Cluster Services. Gleiches gilt für die von Microsoft geschaffene, verteilte Komponentenarchitektur DCOM (Distributed Component Object Model), deren Sicherheitsarchitektur voraussetzt, dass der Client und der Server einer gemeinsamen Domänenstruktur angehören. Eine Vielzahl von Client/ Server-Anwendungen (von Microsoft und anderen Herstellern) verwendet DCOM.

Mit Windows 2000 hat Microsoft das NT-Domänenmodell zum Verzeichnisdienst Active Directory weiterentwickelt. Innerhalb des Active Directory sind das NT-Domänenmodell und dessen Eigenschaften weiterhin spürbar und im Sinne der Abwärtskompatibilität notwendig. So bedeutet z.B. die Einführung von Kerberos als Authentifizierungsmechanismus nicht die Abschaffung des NTLM (NT LAN Manager) Mechanismus, zumal auch reine Windows 2000 Umgebungen an bestimmten Stellen (z.B. Cluster) weiterhin NTLM verwenden. Gleichzeitig sind dem Active Directory Funktionalitäten hinzugefügt worden, die entweder in der bisherigen Microsoft Welt eher separat gehandhabt wurden oder gar nicht vorhanden waren. Bezüglich der Funktionalität der Gruppenrichtlinien sind Teile bereits als Systemrichtlinien, Internet Explorer Administration Kit (IEAK) oder Security Configuration Editor (SCM) unter Windows NT bekannt gewesen. Neu hingegen sind in den Gruppenrichtlinien Funktionalitäten wie Softwareverteilung, die Bindung an Organisationseinheiten, Domänen und Standorte oder An- und Abmeldeskripte.

Völlig neuartig bei Windows Active Directory ist die Integration von Verschlüsselungstechnologien wie IPsec oder EFS (Encrypted File System). Sollen diese

eingesetzt werden, muss eine PKI (Public Key Infrastructure) aufgebaut werden, die sich in das Active Directory integriert. In diesem Zuge hat Microsoft auch das Kerberos Protokoll erweitert, um Authentifizierung via SmartCard zu ermöglichen. Des Weiteren benötigt Windows Active Directory zwingend eine DNS (Domain Name System) Infrastruktur zur Namensauflösung. Das DNS muss mindestens der BIND Version 8.2.2 entsprechen. Windows 2000/2003 beinhaltet einen eigenen DNS.

Exchange 2000 ist das erste Produkt von Microsoft, das zwingend ein Windows Active Directory voraussetzt. Im Gegensatz zu Exchange 5.5 besitzt Exchange 2000/2003 keinen eigenen Verzeichnisdienst mehr. Sämtliche Informationen der E-Mail-Benutzer und der Verteilerlisten des Exchange 2000/2003 befinden sich im Active Directory, das durch eine Schemaerweiterung für die Integration von Exchange vorbereitet werden muss. Eine zentrale Rolle für Exchange 2000/2003 spielt der Global Catalog Dienst des Active Directory, den Exchange nutzt, um Informationen über Domänengrenzen hinweg zu erfragen. Den Global Catalog verwendet z.B. auch Outlook 2000. Darüber hinaus verwendet Exchange 2000/2003 das Active Directory nicht nur lesend, sondern auch schreibend: so schreibt der Empfängeraktualisierungsdienst (Recipient Update Service) von Exchange seine Ergebnisse ins Active Directory. Die Werkzeuge zur E-Mail-Benutzerverwaltung sind komplett in der Management Konsole „Active Directory – Benutzer und Computer“ integriert.

Diese Zusammenhänge und Abhängigkeiten zwischen Microsofts Betriebs- und Anwendungssystemen charakterisieren eine wachsende Integrationstiefe innerhalb dieser Plattform und werfen hinsichtlich des potenziellen Einsatzes von Produktalternativen eine Reihe von strategischen Fragestellungen auf:

- Wie lässt sich die Unterbrechung einer bestimmten Produktlinie und der damit verbundenen Updatezyklen umsetzen?
- Wie kann die Abhängigkeit von einer Produktlinie und der entsprechenden technischen Ausrichtung minimiert werden?
- Welche Maßnahmen führen zu einer Reduzierung der Herstellerabhängigkeit und der Diversifikation der Softwarelandschaft?
- Gibt es ausreichend Ersatz für bestimmte Softwarekomponenten durch kostengünstigere Alternativen?

Aufgrund des in der Zwischenzeit produktintern erreichten Abhängigkeitsgrades können diese Fragestellungen in der Regel nur mit einem strategischen Ansatz beantwortet werden, der in den IT-Konzepten der Verwaltungen entsprechend Eingang finden muss.

2.3 Linux-Distributionen

2.3.1 Einleitung

Für die Realisierung der Server- und Clientsysteme kann auf eine Vielzahl von unterschiedlichen Linux-Distributionen zurückgegriffen werden. Sie enthalten neben dem reinen Betriebssystem zusätzlich zahlreiche andere Software-Pakete. Dabei handelt es sich nicht nur um die Desktopanwendungen, die in der Regel in vielfältiger Ausprägung mitgeliefert werden, sondern auch um Software für Webserver, Datenbankmanagementsysteme, Mailserver, Firewall, Proxyserver, Verzeichnisdienst und weiteres mehr. Zentrale Aufgabe von Distributionen ist darüber hinaus die Bereitstellung eines Installationsprogramms, sowie von Konfigurationswerkzeugen. In einem vom Hersteller und Distributionsprodukt abhängigem Maß liefern Distributoren außerdem über einen bestimmten Zeitraum Softwareaktualisierungen und –Patches für die jeweilige Distribution.

Im Folgenden wird auf einige ausgewählte Distributionen kurz eingegangen und auf Besonderheiten hingewiesen. Im Folgenden wird auf einige ausgewählte Distributionen kurz eingegangen und auf Besonderheiten hingewiesen. Ein Besonderheit sind die im Abschnitt 2.3.5 dargestellten „Standard Desktop“, diese werden von unterschiedlichen Herstellern angeboten und zielen in erster Linie auf den Enterprisemarkt. Ergänzung zu der Kurzvorstellung der „Standard Desktops“ werden die jeweiligen Systemmanagementmöglichkeiten skizziert.

Distributionen bieten die unterschiedlichsten Hersteller an. In der Regel sind sie ursprünglich für die Vereinfachung der Installationsvorgänge des Betriebssystemkerns (Kernel) und der jeweiligen Programme entwickelt und gepackt worden. Die Distributionsfirmen haben für die Installation eine Reihe von unterschiedlichen Administrationswerkzeugen für den freien Betriebssystemkern und die umgebenden Software-Einheiten entwickelt, die teilweise wiederum als freie Software lizenziert wurden. Der Kunde kauft mit einer Distribution nicht Linux selbst. Bezahlt wird vielmehr die vom Distributor geschaffene Zusammenstellung von Betriebssystem, Zusatzprogrammen, Installationsprogrammen und Dokumentation. Das Ziel der Distributionen ist die Verringerung des administrativen und organisatorischen Aufwandes für den Nutzer, denn der Kern des Betriebssystems bringt keine eigenen Konzepte bzgl. dieser Anforderungen mit. Somit ist das Betriebssystem offen für unterschiedliche Management- und Organisationskonzepte.

Mit dem Erwerb einer Distribution erhält der Kunde in der Regel neben den Datenträgern (in der Zwischenzeit eine Vielzahl von CDs) und eine ausführliche Dokumentation. Die Dokumentation unterscheidet sich in ihrem Umfang und in ihrer Qualität in der jeweiligen Distribution, beinhaltet jedoch normalerweise eine Installationsanleitung und weiterführende Informationen für den Betrieb. Auf den Datenträgern befinden sich die entsprechenden Versionen der Betriebssystemsoftware und eine Vielzahl von weiteren Softwareeinheiten. Aufgrund der GNU General Public License (GPL), die für viele unter Linux eingesetzte Programme und den Betriebssystemkern (Kernel) gilt, wird von Distributoren auch der Quell-

code der entsprechenden Programme mitgeliefert. Dadurch ist der Anwender in der Lage, bei Problemen die Software neu zu kompilieren und seinen Bedürfnissen entsprechend anzupassen.

Die unterschiedlichen Distributionen lassen sich sowohl als fertiges Gesamtpaket (CD, Dokumentation) im Handel käuflich erwerben und in vielen Fällen auch kostenlos aus dem Internet beziehen. Bei dem Erwerb des Gesamtpaketes kann der Kunde in der Regel auf einen Support des Anbieters zurückgreifen; dieser steht ihm bei den im Internet verfügbaren Versionen nicht zur Verfügung. Bei den Distributionen, die im Folgenden betrachtet werden, kann noch zwischen Versionen von kommerziellen Distributionsanbietern und einer Distribution, die durch eine Gemeinschaftsarbeit einer Projektgruppe entwickelt wurde, unterschieden werden, wobei es hiervon abgeleitete Distributionen gibt, die ebenfalls kommerziell zur Verfügung gestellt werden.

Der Kompatibilität der Linux-Versionen und Vereinheitlichung der unterschiedlichen Distributionen kommt in der Zukunft eine wichtige Rolle zu. Um zu große Unterschiede zwischen den einzelnen Distributionen zu vermeiden, wurde beispielsweise zur Festlegung der Linux-Verzeichnisstruktur der Filesystem-Hierarchy-Standard[1] definiert. Anbieter von Distributionen setzen diesen Standard in der Regel innerhalb ihrer Distributionen um. Als wichtiger Bestandteil der Interoperabilitätsbemühungen ist der Filesystem-Hierarchy-Standard ebenfalls in die Linux Standard Base[2] (LSB) integriert. Die Linux Standard Base hat sich zum Ziel gesetzt, Standards zu definieren, mit denen eine möglichst weite Kompatibilität aller Distributionen erreicht und die Divergenz zwischen den Linux-Systemen verhindert werden soll. Die Standardisierung soll gleichermaßen den Softwareentwicklern und Distributoren die Arbeit erleichtern. Bei einer weiteren Verbreitung von LSB-konformen Distributionen wird zukünftig eine Softwareverteilung unabhängig von der jeweiligen Distribution möglich sein.

Neben LSB ist im Kontext der Standardisierungsaktivitäten die Free Standard Group[3] zu nennen. Es handelt sich dabei um einen Zusammenschluss der LSB, der OpenI18N[4] (ehemals die Linux Internationalization Initiative Li18nux) und der LANANA (The Linux. Assigned Names and Numbers Authority). Die LANANA befasst sich mit der Verwaltung des Linux-Namensraums zur Vermeidung von Namenskonflikten bei Applikationen und Treibern. Mitglieder der FSG sind unter anderem Caldera, Compaq, Conectiva, Debian, Dell, Hewlett Packard, Hitachi, IBM, Intel, Miracle Linux, The Open Group, Oracle, Red Hat, Sun, Suse, Turbolinux, VA Software und die Mitglieder der Open Source Entwicklergemeinschaft.

1 http://www.pathname.com/fhs/

2 http://www.linuxbase.org

3 http://www.freestandards.org

4 http://www.openi18n.org

Die Liste der LSB-zertifizierten Distributionen kann im Internet[1] eingesehen werden.

Bei der Auswahl einer Distribution spielen einerseits die Anforderungen zum Support und Administrationskonzept sowie zur Hardware-Unterstützung, andererseits die wirtschaftlich-organisatorischen Rahmenbedingungen eine Rolle. Die Existenz von Rahmenverträgen oder Angebot von speziell auf Behördenbedarf abgestimmten Anwendungen sind Beispiele solcher Entscheidungskriterien.

Die im Folgenden vorgestellten Distributionen wurden aufgrund ihrer starken Verbreitung ausgewählt.

2.3.2 Debian GNU Linux

Innerhalb des Debian-Projektes wird von einer Vielzahl von Entwicklern in Gemeinschaftsarbeit eine freie Distribution entwickelt. Analog zur Entwicklung des Linux-Kerns sind die ungefähr 1000 Mitglieder des Debian-Projekts, die weltweit verteilt sind, in der Regel Profis, die sich im Auftrag von Unternehmen und anderen Organisationen oder als Freiberufler an der Entwicklung der Distribution beteiligen. Ein stark formalisierter Vorgang gewährleistet dabei, dass nur solche Personen Mitglieder des Debian-Projekts werden können, die über das entsprechende Fachwissen verfügen. Obwohl im Umfeld der Erstellung der Distribution auch Personen mitwirken, die nicht den IT-Profis zuzuordnen sind, beispielsweise bei den Übersetzungen von Handbüchern, wird Debian doch als die Distribution von Profis für Profis bezeichnet.

Kennzeichnend für Debian ist, dass die eigentliche Distribution freie Software im Sinne der „Debian Free Software Guidlines“ (aus denen später die offizielle Open-Source-Definition entwickelt wurde) ist und deswegen beliebig oft – auch kommerziell – kopiert, geändert und eingesetzt werden kann. Die Distribution ist extrem umfangreich, gut gewartet und zeichnet sich durch einen sehr leistungsfähigen Mechanismus zur Softwareverwaltung und –Aktualisierung aus, der deswegen auch von anderen Distributionen übernommen wurde

Debian GNU/Linux kann sowohl im Internet bezogen als auch bei einem Händler käuflich erworben werden. Die Debian-Distribution gilt als nicht kommerziell, und so werden beim Kauf der CDs primär die Produktions- und Vertriebskosten der Datenträger bezahlt. Das Debian-Projekt selbst bietet keine Packungen mit CDs an, was diese Distribution von den anderen unterscheidet.

Charakteristisch für Debian ist die Fehlerbehandlung innerhalb der Entwicklergemeinschaft. Mittels des Bug-Tracking wird eine Liste veröffentlicht, die alle offenen Fehlermeldungen enthält und die von den Entwicklern abgearbeitet werden. Durch diesen Mechanismus der Qualitätssicherung zählt Debian zu den stabilsten und fehlerfreiesten Distributionen. Debian zeichnet sich durch lange Versionszyklen aus, welche die hohe Qualität der Distribution bedingen. So werden keine „überhasteten“ Versionen auf den Markt gebracht.

[1] http://www.opengroup.org/lsb/cert/cert_prodlist.tpl?CALLER=cert_prodlist.tpl

Eine kennzeichnende Eigenschaft von Debian ist das eigene Paketformat und die dazugehörigen Systemwerkzeuge. Ein wesentlicher Vorteil liegt in der Möglichkeit, die Systeme bzw. einzelne Programme problemlos aktualisieren zu können, ohne die Software komplett neu zu installieren. Das Paketmanagement dient auch zur regelmäßigen Aktualisierung der Systeme mittels Sicherheits- und Stabilitäts-Updates.

Rund um den Support für den Betrieb und die Entwicklung stehen eine Reihe von Mailinglisten[1] zur Verfügung Sollte diese Informationsquelle nicht ausreichend sein, kann auf die Supportdienstleistungen zahlreicher kommerzieller Anbieter zurückgegriffen werden.

2.3.2.1 Auf Debian GNU/Linux basierende Distributionen

Die hohe Qualität, der große Umfang, das extrem leistungsfähige Softwaremanagement sowie die Zusicherung, dass der Hauptteil der Distribution immer freie Software sein wird, macht Debian GNU/Linux nicht nur für Anwender sondern auch für kommerzielle Distributoren interessant. So gibt es heute einige kommerzielle, auf Debian GNU/Linux basierende Distributionen mit unterschiedlichem Fokus, welche die Distribution um verschiedene Eigenschaften, wie beispielsweise zusätzliches Qualitätsmanagement, komfortablere Installations- und Rollout-Routinen oder spezielle Anpassungen und Ergänzungen erweitern. Diese Distributoren können außerdem Maintenance (Pflege der Distribution, wie beispielsweise die Integration sicherheitsrelevanter Patches) und Support in vergleichbarer Form wie kommerzielle Distributoren, die komplett selbst entwickelte Distributionen erstellen, anbieten.

Linspire

Linspire ist eine für den Desktop-Einsatz bestimmte, auf Debian GNU/Linux basierende Distribution, die sich insbesondere an Privatanwender richtet. Da diese Distribution deswegen nicht im Fokus dieses Werks liegt, wird sie hier nur erwähnt.

Univention Corporate Server (UCS)

Die Distribution Univention Corporate Server (UCS) ist eine kommerzielle Distribution und besteht im Wesentlichen aus zwei Komponenten, dem UCS-Basissystem und dem UCS-Managementsystem.

Das UCS-Basissystem ist eine auf Debian GNU/Linux basierende Distribution, mit eigenem Installations-, Rollout- und Konfigurationsmanagementsystemen. Im Vergleich zur offiziellen Debian Distribution ist sie weniger umfangreich.

Das UCS-Managementsystem ist ein auf dem Verzeichnisdienst OpenLDAP und anderen Open Source Komponenten bestehendes Managementsystem, mit dem in Analogie zu Active Directory auch heterogene und verteilte Infrastrukturen

[1] http://www.debian.org/support

zentral über einheitliche Schnittstellen verwaltet werden können. Das UCS-Managementsystem ist separat vom UCS-Basissystem installierbar.

UCS unterstütz den Einsatz als Server und Clientbetriebssystem wobei zum Teil auf den jeweiligen Einsatzzweck angepasste Pakete und Konfigurationen zum Einsatz kommen. Auch im Desktopbereich steht die zentrale Verwaltung über das UCS-Managementsystem im Mittelpunkt.

2.3.3 Suse Linux Distribution von Novell

Der amerikanische Softwarehersteller Novell hat den ehemals Deutschen Linux-Distributor Suse Ende 2003 übernommen und ist damit selbst zum Linux-Distributor geworden. Die Novell-Distribution wird zurzeit weiterhin unter dem Namen Suse vertrieben.

Traditionell ist die Suse Distribution sehr stark auf dem deutschen Markt vertreten. Suse hat ursprünglich damit begonnen, die internationale Slackware-Distribution[1] für den deutschen Markt anzupassen. Nach einer gewissen Zeit wurde eine eigene Distribution entworfen. Im Laufe der Zeit entwickelte Suse Produkte für unterschiedliche Einsatzgebiete. Die folgende Tabelle beschreibt die wichtigsten Eigenschaften unterschiedlicher Distributionen.

Tab. 1: Suse Linux

Produkte	Schwerpunkt
Professional	Wird in erster Linie vom Hersteller für den Desktop-Einsatz im Heim- und Workstationbereich empfohlen. Die Distributionen enthalten umfangreiche Softwarepakete, die durch mitgelieferte Installationsroutinen auf den Rechnern installiert werden können.
Enterprise	Die Suse Linux Server sind Server-Betriebssysteme für den Einsatz in IT-Umgebungen aller Größen und Ausrichtungen. Verfügbar für alle relevanten Hardware-Plattformen: Für die 32- und 64- Bit-Prozessoren von AMD und Intel, wie auch für die gesamte eServer-Reihe von IBM, inklusive Mainframe.
Desktop (siehe auch Kapitel 2.3.5.3)	Ist für den Desktop-Einsatz im Unternehmens- und Behördenumfeld bestimmt.

Die Suse-Distribution basiert auf dem von Red Hat entwickelten RPM-Paketsystem. Mit Hilfe des Paketsystems kann Software – auch von Drittanbietern – in der Regel problemlos installiert und wieder entfernt werden. Einige distributionsspezifische Softwarepakete sollten jedoch erfahrungsgemäß in der vom jeweiligen Produzenten präferierten Methode installiert werden. Die Suse-Distributionen enthalten das integrierte Installations- und Administrationssystem

[1] http://www.slackware.org

YaST. Den Anwendern wird sowohl ein textbasiertes als auch ein grafisches Frontend zur Systemverwaltung angeboten.

Die oben genannten Distributionsvarianten unterscheiden sich in erster Linie in ihrem empfohlenen Einsatzbereich und den damit verbundenen Unterschieden im angebotenen Support, der verfügbaren Lizenzierungen und letztendlich auch im Anschaffungspreis.

Für den Einsatz in unternehmenskritischen Bereichen werden im Hinblick auf die Verfügbarkeit und Skalierbarkeit mit den Enterprise-Lösungen optimierte Lösungen angeboten. Es wurde beispielsweise die Clusterfähigkeit, Multiprozessorfähigkeit und Asynchrones I/O integriert.

Darüber hinaus unterscheiden sich die Distributionen durch das jeweilige Supportprogramm. In Abhängigkeit von den individuellen Kundenbedürfnissen werden beispielsweise 24x7 Support, individuelle Service Level Agreements und Zertifizierungen angeboten.

2.3.4 Red Hat-Distribution

Eine weitere kommerzielle Distribution ist die von Red Hat. Auch Red Hat bietet seinen Kunden mehrere Distributionsvarianten für unterschiedliche Einsatzgebiete (s.a. Tab. 2). Red Hat verwendet eine Eigenentwicklung zur Programmverwaltung. Die Programmpakete (.RPM) werden mittels des Red Hat Package Managements verwaltet, das eine einheitliche und komfortable Softwareverwaltung ermöglicht.

Tab. 2: Red Hat

Produkt	Bemerkungen
Red Hat Enterprise Linux WS	Die Distributionen sind in erster Line für den Workstation-Bereich gedacht. Sie ist der Desktop-/Client-Partner für Enterprise Linux-Lösungen.
Enterprise Linux	Die Enterprise-Lösungen werden in erster Linie als Lösungen für den Unternehmensbereich angeboten. Die Systeme sind für eine Reihe von Plattformen unterschiedlicher Hardwarehersteller zertifiziert und beinhalten beispielsweise Hochverfügbarkeits-Clustering Technologien.
Red Hat Desktop (siehe auch Kapitel 2.3.5.2)	Für den Desktop-Einsatz in Unternehmen und Behörden bestimmt.

Die unterschiedlichen Produkte unterscheiden sich in erster Linie in dem empfohlenen Einsatzbereich und den damit verbundenen Unterschieden im angebotenen Support, der verfügbaren Lizenzierungen und im Anschaffungspreis.

2.3.5 Standard Desktops

Neben dem Angebot der unterschiedlichen Distributionen (s.o), mit ihren umfangreichen Softwarepaketen, werden spezielle Lösungen für komplette Desktopsysteme angeboten. Diese Lösungen, sind in erster Line für den Bereich der Enterpriseumgebungen, die sich durch eine große Anzahl von Desktopsystemen auszeichnen, geschaffen worden. Die einzelnen Produkte, der unterschiedlichen Lösungsanbieter, beinhalten alle ein Linux-Betriebssystem und eine Zusammenstellung der wichtigsten Softwareprogramme für den Desktopbereich. Die Desktopsysteme wurden speziell für den Arbeitsplatzbereich angepasst und in Hinblick auf die Benutzerfreundlichkeit und visuelle Erscheinung optimiert. Die Anbieter der Desktopsysteme bieten unfassende Supportleistungen (Updates, Support und Schulungen) für diese Systeme an. Neben der kurzen Beschreibung der unterschiedlichen Standard Desktopsysteme, werden in den folgenden Abschnitten auch die Möglichkeiten der zentralen Administration der Desktopsysteme aufgezeigt. Insbesondere für Verwaltungen, mit einer großen Anzahl Computerarbeitsplätzen, ist der Aspekt der zentralen Desktopverwaltung und des Systemmanagements von entscheidender Bedeutung.

2.3.5.1 Sun Java Desktop

Mit dem Sun Java Desktop System (JDS) hat Sun Microsystems eine umfassende Desktoplösung auf den Markt gebracht. Die Distribution beinhaltet neben dem Betriebssystem die wichtigsten Softwareprogramme für die Kommunikation, die Internetnutzung sowie weitere nützliche Desktopanwendungen. Als Bürolösung stellt Sun den Nutzern des Sun Java Desktop die StarOffice-Suite zur Verfügung.

Tab. 3: Sun Java Desktop

Komponente	Einsatz
GNOME	Der GNOME-Desktop stellt die grafische Benutzerschnittstelle des JDS dar.
StarOffice	Stellt die zentrale Softwarekomponente des JDS dar. Das Bürosoftwarepaket beinhaltet alle Komponenten für die tägliche Büroarbeit.
Evolution	Mail- und Groupwareclient.
Mozilla	Webbrowser
GIMP	Umfangreiches Photo- und Bildbearbeitungsprogramm
YaST /Auto YaST	Desktop Admin Tool und Installationssupport
Real Player, Flash Player, CD-Player, Java Media-Player, Bildbetrachter	Die Programme dienen zum Darstellen und Abspielen von Multimediainhalten.

JDS Verwaltungswerkzeuge

Neben den Desktop Applikationen liefert Sun Microsystems noch kostenlose Software für die Administration von Multi User Umgebungen aus. Im Folgenden wird ein kurzer Überblick über die Funktionalitäten und Möglichkeiten gegeben:

Java System Update Service (SUS)

Der Java System Update Service dient der Bereitstellung von Updates und Patches des Java Desktop Systems. Die Aktualisierung der installierten Pakete erfolgt über den automatisierten Dienst via Internet, der sich mit dem Update-Server von Sun verbindet und die Aktualität der installierten Pakete überprüft. Bei der Verfügbarkeit von aktuelleren Dateien schlägt der Update Service die Installation vor, die man jeweils akzeptieren oder ablehnen kann.

Java Desktop System Configuration Manager (APOC)

Der Java Desktop System Configuration Manager ist eine zentrale Serveranwendung und Bestandteil des JDS. Er steuert die Definition von Nutzergruppen und die entsprechende Zuweisung von Nutzerrechten und Desktopeinstellungen. Das Verwaltungswerkzeug erlaubt die zentrale Festlegung und Administration der Benutzereinstellungen der wichtigsten Java Desktop Applikationen, GNOME, StarOffice, Evolution und Mozilla. Der Zugriff auf den Configuration Manager erfolgt mittels eines Webbrowsers. Für Systemadministratoren bietet sich die Möglichkeit, nutzerbezogene Einstellungen der oben genannten Arbeitsplatzapplikationen vorzunehmen und Richtlinien für diese Applikationen festzulegen. Grundsätzlich können Benutzer und Rechnergruppen verwaltet werden. Neben der Gruppierung wird auch die Vererbung von Konfigurationsrichtlinien zur Vermeidung von redundanten Arbeitschritten unterstützt. Die Konfigurationsdaten werden in einem zentralen Verzeichnisdienst hinterlegt, die Anbindung kann an unterschiedliche LDAP-Server erfolgen. Unter anderen wird auch der OpenLDAP-Verzeichnisdienst unterstützt. Auf den Java Desktop Systemen laufen spezifische Konfigurations-Agenten, die die Konfigurationsdaten für den jeweiligen Nutzer aus dem Verzeichnisdienst beziehen und diese auf den Desktopsystemen den Konfigurationssystem-Adaptern bereitstellten. In der JDS Version 2 werden folgende Konfigurationssysteme unterstützt:

- GConf-Adapter für den Gnome-Desktop
- Gnome-Applikation (Evolution)
- Mozilla-Adapter
- StarOffice-Adapter

Sun Control Station (SCS)

Die Sun Control Station ist ein Softwarepaket, deren verschiedene Module die Administratoren bei der Systemverwaltung unterstützen. Der Zugriff auf die Control Station erfolgt ebenfalls browserbasiert. Die Control Station besteht in ihrer Architektur aus den Bereichen Kernanwendung und den implementierten

Modulen für die Systemverwaltung. In der Grundausstattung verfügt die Control Station über fünf vorinstallierte Module:

- **AllStart–Modul** – Das AllStart-Modul unterstützt sowohl die Kickstart- als auch die AutoYaST-Technologie zur Installation und Anpassung linuxbasierter Systeme. Neben dem Sun Java Desktop System werden auch Red Hat Systeme unterstützt. Das Modul ermöglicht die initiale Verteilung der Desktopsysteme, die Erstellung von Profilen und die Überwachung der Systeminstallationen und Updates.
- **Health Monitoring-Modul** – Das Modul erlaubt die Überwachung der Arbeitsplatzrechner in Bezug auf Systeminformationen, Verfügbarkeit und Status.
- **Inventory-Modul** – Es können Hardware-Informationen über die gemanagten Systeme bereitgestellt werden.
- **Performance-Modul** – überwacht die Performance der verwalteten Systeme. Die Überwachung kann für unterschiedliche Kriterien erfolgen, unter anderem nach der CPU-Auslastung und dem Speicherverbrauch.
- **Software-Management-Modul** – Das Modul unterstützt die zentrale Softwareverteilung für die verwalteten Systeme. Es erlaubt die Installation, Deinstallation und Verwaltung von Softwareeinheiten.

Mit Hilfe der Remote Desktop Takeover-Funktionalität können Administratoren oder Support- Mitarbeiter im Unternehmen Anwendern des JDS 2 Systems Unterstützung bieten, ohne den Anwender vor Ort aufsuchen zu müssen. Diese Funktionalität der Fernwartung und Ferndiagnose über das Netzwerk erlaubt der administrativen Kraft, den entfernten Desktop des Benutzers auf seinem Computer darzustellen und zu verändern, jedoch nur mit aktiver Zustimmung des Anwenders.

2.3.5.2 Red Hat Desktop

Der Red Hat Desktop (RHD) ist ein Bestandteil der Red Hat Enterprise Linie und wurde speziell für den Enterprisemarkt entwickelt. Es ist vollständig kompatibel mit den weiteren Red Hat Enterprise Produkten. Der RHD bietet ein voll funktionstüchtiges Desktopsystem mit allen Kernapplikationen, die für die tägliche Arbeit benötigt werden. In der folgenden Tabelle werden die wichtigsten Applikationen des RHD kurz vorgestellt.

Tab. 4: Red Hat Desktop

Komponente	Funktion
GNOME	Der GNOME-Desktop stellt die grafische Benutzerschnittstelle des RHD dar.
OpenOffice	Das Bürosoftwarepaket beinhaltet alle Komponenten für die tägliche Büroarbeit.
Evolution	Mail- und Groupwareclient.
Mozilla	Webbrowser

Komponente	Funktion
Adobe Acrobat	Zum Betrachteten von PDF-Dateien.
Citrix Client	Ermöglicht den Zugriff auf einen Citrix-Terminalserver
Real Player, Macromedia	Die Programme dienen zum Darstellen und Abspielen von Multimediainhalten
Red Hat Update Agent	Stellt die Verbindung zum Red Hat Network dar und erlaubt die Aktualisierung und Verwaltung des Desktopsystems.

RHD Systemmanagement

Mit dem Red Hat Desktop können auch Desktop Management Module erworben werden. Für den Bereich von Enterpriseumgebungen werden zwei unterschiedliche Lösungsarchitekturen angeboten. Neben dem Red Hat Network Proxy ist auch der Satellite Server verfügbar. Die folgende Abbildung zeigt die grundsätzliche Architektur der beiden Lösungen.

Bild 4: Red Hat Network

Beim Proxy-Modell greifen die Desktopsysteme auf einen im lokalen Netzwerk befindlichen Proxyserver zu, dieser stellt Daten und einige Funktionalitäten lokal zur Verfügung. Der Proxyserver ist wiederum mit den zentralen RHN-Servern im Internet verbunden.

Für Verwaltungen, die in der Regel über die vollständige und alleinige Kontrolle ihrer Systeme verfügen wollen und müssen, bietet sich die Variante des Red Hat Network Satellite Servers an. Der Satellite Server, basierend auf einem RH Enterprise Advanced Server und einer Datenbankinstanz, ermöglicht das Desktop Management der RHD-Systeme. Der Satellite Server kann zur Aktualisierung der

durch Red Hat bereitgestellten Updates und Patches über das Internet mit dem Red Hat Network verbunden werden, aus Sicherheitsgründen können die Updates aber auch mit alternativen Methoden (CD-ROMs, usw.) eingespielt werden.

Die folgende Tabelle gibt einen Überblick über die wichtigsten Komponenten der Desktopmanagementarchitektur.

Tab. 5: Managementkomponenten

Komponente	Funktionen
Satellite Server (Red Hat Network)	
Webbasierte Oberfläche	Webbasierte Nutzeroberfläche zum Systemmanagement. Ermöglicht den Zugriff auf den Sattelite Server zur Verwaltung und Konfiguration der Desktopsysteme.
Lokales Datenbank Repository	Zur Speicherung der Informationen über die Systeme, Richtlinien und Profilen.
Custom Channels	Die so genannten “Custom Channels” dienen zur Verteilung von RPM-basierten Paketen, sowohl von Betriebssystemkomponenten als auch anderer Applikationen. Zur Einrichtung, Duplikation oder Anpassung eines Channels stehen Channel Management Werkzeuge zur Verfügung.
Desktop	
RH Update Agent und RH Network Deamon	Der Update Agent dient zur initialen Verbindungsaufnahme mit dem Satellite Server. Er ermöglicht den Zugriff auf die Channels, Paketinstallation und das Systemprofilmanagement. Der RH Network Deamon läuft im Hintergrund auf dem Desktopsystem und überprüft den Sattelite Server auf Nachrichten und Updates.

Die Architektur des Satellite Servers besteht aus einer zentralen Serveranwendung, die direkt auf die Inhalte einer unterliegenden Datenbank zugreift. Innerhalb des Datenbanksystems werden alle relevanten Informationen über die zu verwaltenden Systeme (Rechner, Gruppen, Pakete, Channels, usw.) vorgehalten und gespeichert. Der Zugriff auf die Systemmanagementanwendung erfolgt über eine webbasierte Benutzerschnittstelle.

Die einzelnen Architekturkomponenten in Verbindungen mit den unterschiedlichen Servicemodulen von Red Hat bieten das Framework zur Verwaltung der Red Hat Desktop Systeme. Es werden drei unterschiedliche Servicelevels angeboten:

- **Update**: Nur für Einzelsysteme bzw. wenige Desktopsysteme sinnvoll.
- **Management**: Beinhaltet die Leistungen des Updatelevels und erweiterte Managementfunktionalitäten (siehe Tabelle Management und Update Modul).
- **Provisioning**: Beinhaltet die Leistungen des Updates- und Managementlevels und zusätzliche Funktionen für ein „Life-Cycle-Management“ (siehe Tabelle Provisioning Modul).

Die wichtigsten im Rahmen der Systemverwaltung und der jeweiligen Servicelevels zur Verfügung stehenden Funktionalitäten werden in der folgenden Tabelle kurz dargestellt.

Tab. 6: Systemmanagementfunktionalitäten des Red Hat Networks

Komponente	Funktionen
Management und Update Modul	
Webschnittstelle	Webbasierte Nutzeroberfläche zum Systemmanagement. Ermöglicht den Zugriff auf den Sattelite Server und das Red Hat Network zur Verwaltung und Konfiguration der Desktopsysteme.
Updates und Patches	Es werden von RH entsprechende Updates, Sicherheitsupdates und Patches bereitgestellt, diese müssen zur Verteilung im lokalen Netzwerk auf dem Satellite Server bereitgestellt werden.
Systemgruppen	Erlauben die Bildung von Rechnergruppen und somit die vereinfachte Verwaltung der Systeme. Den Systemgruppen können wiederum unterschiedliche Aktionen (Installation, Updates, Zuordnung zu einzelnen Channeln, usw.) zugeordnet werden. In der Regel werden die Systemgruppen für längerfristige Gruppierungen verwendet.
Systemsets	Werden nach Bedarf zusammengestellt; diese eher temporären Rechnergruppierungen können auf Basis von Systemgruppen, einzelnen Systemen oder Systemeigenschaften zusammengestellt werden.
Gruppenbasierte Administration	Erlaubt die Zuordnung von System- bzw. Rechnergruppen zu einzelnen Administratoren.
Zeitgesteuerte Aktualisierung	Legt den Updatezeitpunkt für eine bestimmte Systemgruppe fest.
Systemsuche	Administratoren können nach unterschiedlichen Suchkriterien (Software-, Hardware-, Netzwerkinformationen) Rechnertypen suchen.
Profilpaketvergleich	Erlaubt den Vergleich unterschiedlicher Systeme in Hinblick auf die installierten Pakete.
RPM-Abhängigkeitstest	Erlaubt die Überprüfung der Paketabhängigkeiten und somit eine Paketzusammenstellung für ein stabiles System.
Provisioning Modul	
Kickstart	Mittels so genannter „Kickstartprofile“ ist die Installation ganzer Desktopsysteme möglich. Mittels der Profile können zahlreiche Systemparameter (Bootloader, Zeitzone, Softwarepakete, usw.) automatisiert übergeben werden. Mittels des Kickstart-Konfigurationseditors können entsprechende Scripte erstellt werden.
Bare Metal Provisioning	Automatische Systembereitstellung unter Verwendung von Kickstart zur Verteilung von Betriebssystemen, Softwarepaketen und unter Verwendung weiterer Techniken (Systemgruppen, Channels, Richtlinien, Berechtigungen).
Rollback und Recovery.	Durch die Speicherung der Systeminformationen aller Systeme und aller durchgeführten Änderungen können Systeme in einen älteren Zustand zurückgeführt werden.
Konfigurations-Management	Ein Konfigurationsmanagement erfolgt auf Basis von reinen Textdateien, in denen die Systemeinstellungen festgelegt

Komponente	Funktionen
	werden. Daneben kann die Konfiguration auch in Verbindung mit der Kickstartfunktionalität bei der Installation festgelegt werden.
RPM – basierte Softwareverteilung	Neben der Verteilung der Betriebssystempakete können weitere Softwarepakete automatisiert verteilt werden, sofern sie RPM-basiert sind.

Der Satellite Server dient zur automatisierten und zentralisierten Verwaltung von Linux-Installationen in Verbindung mit der Softwareverteilungsinfrastruktur des Red Hat Networks. Der Satellite-Dienst in Verbindung mit dem RHN Provisioning Modul ermöglicht die vollständige zentrale Verwaltung von Enterprise Linux-Installationen beliebiger Größe. Im Rahmen des Managements werden von Inventory-Funktionen über automatisierte Installation, das Konfigurationsmanagement bis hin zur Softwareverteilung die zentralen Punkte des Lebenszyklus einer IT-Umgebung abgedeckt. Dabei können auch kundenspezifische Softwarepakete verwaltet und verteilt werden.

2.3.5.3 Novell Linux Desktop

Mit dem Novell Linux Desktop (NLD) hat Novell (nach der Übernahme von Suse) eine komplette Desktoplösung auf den Markt gebracht. Das Desktopsystem besteht aus dem linuxbasierten Betriebssystem und einer Reihe von Desktopanwendungen. Der Novell Linux Desktop basiert auf dem Linux-Kernel 2.6 und auf der Codebasis des Suse LINUX Enterprise Servers 9. In der folgenden Tabelle werden die wichtigsten Anwendungen des NLD kurz vorgestellt.

Tab. 7: Novell Linux Desktop

Komponente	Funktion
KDE und GNOME	Die Desktopoberflächen realisieren die grafischen Benutzerschnittstellen des NLD.
OpenOffice	Das Bürosoftwarepaket beinhaltet alle Komponenten für die tägliche Büroarbeit. In der Version des NLD wird eine so genannte Novell Version[1] dargeboten. Insbesondere wurden die Menüs und Symbolleisten an die Erscheinung des NLD angepasst.
Evolution	Mail- und Groupwareclient.
Mozilla Firefox	Webbrowser.
Adobe Acrobat	Zum Betrachteten von PDF-Dateien.
Citrix Client	Für den Zugriff auf einen Citrix-Terminalserver.
Real Player, Macromedia	Die Programme dienen zum Darstellen und Abspielen von Multimediainhalten.

[1] Novell-Version von OpenOffice: http://www.novell.com/de-de/products/desktop/features/ooo.html

Komponente	Funktion
YaST, AutoYaST	Für die Installation, Konfiguration und Verwaltung des Desktopsystems.
ZENworks Linux Management	Tritt gegenüber ZENworks Linux Management als Client auf und ermöglicht somit die Fernanwendung von Updates und die Steuerung des Systemverhaltens von einem zentralen Standort aus.

ZENworks Linux Management

Mit der ZENworks Linux Management-Lösung stellt Novell eine Systemmanagementlösung für linuxbasierte Systeme zur Verfügung. Mit der Version 6.5 hat Novell begonnen, die Managementlösung von Ximinan, die Red Carpet Enterprise Application, in ZENworks zu integrieren.

Die Architektur entspricht im Wesentlichen noch der ursprünglichen Red Carpet Lösung, eine tiefere Integration in das weitere ZENworks-Framework ist erst mit den zukünftigen Version zu erwarten. Prinzipiell kann zwischen einer Client- und einer Serverkomponente unterschieden werden. Die Clientkomponente, der Update Manager, setzt sich aus einem Dienst, einem Kommandozeilentool und einer grafischen Komponente zusammen. Der Systemmanagementserver, bestehend aus einer Anwendung, einem Datenbanksystem und einem Softwarepaketrepository, bildet die zentrale Komponente des Managements. Die Kommunikation zwischen dem Server und dem Clientsystemen erfolgt mittels einer XML-RPC-Schnittstelle auf Basis des HTTP/HTTPS-Protokolls. Innerhalb des Datenbanksystems, zur Zeit werden PostgreSQL und Oracle unterstützt, werden alle relevanten Informationen über die zur verwaltenden Systeme (Rechner, Gruppen, Pakete, Channels, usw.) vorgehalten und gespeichert. Der Zugriff auf die Systemmanagementanwendung erfolgt über eine webbasierte Benutzerschnittstelle.

ZENworks Linux Management unterstützt neben den Novell/Suse-Distributionen alle Distributionen (z.B. Red Hat, Mandrake, usw.) die mit der oben genannten Clientsoftware ausgestattet werden können.

Die wichtigsten Funktionalitäten, die im Rahmen der Systemverwaltung und der jeweiligen Servicelevels zur Verfügung stehen, werden in der folgenden Tabelle kurz dargestellt.

Tab. 8: Systemmanagementfunktionalitäten des ZENworks Linux Managements

Komponente	Funktionen
Webschnittstelle	Webbasierte Nutzeroberfläche zum Systemmanagement. Ermöglicht den Zugriff auf den Sattelite Server und dem Red Hat Network zur Verwaltung und Konfiguration der Desktopsysteme.
Bereitstellung von Updates und Patches	Innerhalb der Softwarepaketrepositorys können Softwarepakete unterschiedlichster Anbieter und Distributionen bereit-

Komponente	Funktionen
	gestellt werden. Die Verteilung kann dann über dezidierte Channels erfolgen.
Arbeiten mit Gruppen	Erlaubt die Bildung von Clientgruppen und somit die vereinfachte Verwaltung der Systeme. Den Gruppen können wiederum unterschiedliche Aktionen (Installation, Updates, Zuordnung zu einzelnen Channeln, usw.) zugeordnet werden. In der Regel werden die Gruppen für längerfristige Gruppierungen verwendet.
Zusammenstellung von Rechnersets	Rechnersets werden nach Bedarf zusammengestellt, diese eher temporären Rechnergruppierungen können auf Basis von Gruppen, einzelner Systeme oder Systemeigenschaften zusammengestellt werden.
Feingranulare Rechteverwaltung	Es besteht eine umfassende Vergabemöglichkeit von Nutzungsrechten. Die Nutzungsrechte teilen sich in die Optionen „Grant“, „Modify“ und „View“ auf. Die Nutzungsrechte können auf die unterschiedlichen Objekte innerhalb des Systemmanagements vergeben werden, beispielsweise auf Gruppen, Maschinen, Pakete und weitere Objekte. Die Rechteverwaltung erlaubt somit die Übertragung von Nutzungsrechten auf unterschiedliche Administratoren.
Gruppierung von Softwarepaketen	Mit den so genannten Channels ist die individuelle Erstellung von Softwaregruppierungen möglich, Diese werden in der Regel für unterschiedliche Betriebssystemgruppen, Clientausprägungen oder andere Kriterien zusammengestellt.
Management von Novell/Suse 9.x Patches	Ermöglicht die Verwaltung und Verteilung von Novell/Suse-Patches.
Transaktionen	
Durchführung von Updates (Transaktionen)	Transaktionen entsprechen in der Regel Updates, Installationen neuer Software und anderen Maßnahmen, die in Bezug auf Gruppen, einzelne Rechner oder Rechnersets durchgeführt werden können.
Zeitgesteuerte Aktualisierung	Transaktionen können für einen ausgewählten Zeitpunkt festgelegt und durchgeführt werden.
Rollback Transaktionen	Ermöglichen die Herstellung eines ursprünglichen Systemzustandes der Clientsysteme
Pre-Position Transaktionen	Ermöglichen die Festlegung der Downloadzeit der Softwarepakete für die Clientsysteme, die eigentliche Installation kann zu einem festgelegten späteren Zeitpunkt erfolgen.
Systemsuche	Administratoren können nach unterschiedlichen Suchkriterien Rechnertypen suchen.
Erstellung von Reports	Mittels des Linux Management Report Tools können wichtige Informationen über die Verwaltung der Systeme generiert werden. Neben vorgefertigten Reports können auch individuelle Reports auf Basis von unterschiedlichen Filterkriterien erstellt werden.
RPM-Abhängigkeitstest	Erlaubt die Überprüfung der Pakete und somit die Auflösung von Konflikten und Abhängigkeiten. Die entsprechenden Pakete und deren Metadaten müssen Bestandteil des ZENworks Linux Management Servers sein.

Neben den Möglichkeiten des ZENworks Linux Managements können auch weitere administrative Aufgaben mittels der YaST und AutoYaST-Tools vorgenom-

men werden. YaST steht für Yet another Setup Tool und ist das zentrale Instrument für Installation, Konfiguration und Administration eines Novell/Suse-Linux-Systems.

Es umfasst:

- automatische Hardwareerkennung
- Festplatten- und Dateisystemverwaltung
- Softwareauswahl und -installation
- Installation und Konfiguration von Geräten (Hardware) und Systemdiensten
- Systemkonfiguration
- Steuerung der Systemsicherheit

Mittels AutoYaST können automatisierte Client-Installationen durchgeführt werden. Das Prinzip, das der automatischen Installation mittels AutoYaST zugrunde liegt, besteht in der Abbildung aller Informationen und Aktionen bei der Installation eines Systems mit XML-Daten. Diese Kontrolldatei enthält zudem Angaben zu speziellen Installationsarten oder besonderen Prozessen, die während der Installation ablaufen sollen. Mit dieser Kontrolldatei kann ein Novell/Suse-Linux-System ohne weiteren Eingriff automatisch installiert werden.

AutoYaST beruht auf einem Klassen-Konzept, mit dem Rechner in verschiedene Kategorien wie Regionen, Hardwareklassen oder Rollen (Server, Client) eingeteilt werden können. Es verfügt über eine graphische Benutzeroberfläche zur Erzeugung der Kontrolldateien und Klassen.

Die folgende Auflistung zeigt einen beispielhaften Ablauf einer AutoYaST-gesteuerten Installation:

- Booten über Diskette, CD, DVD oder PXE (Netzwerk)
- Einlesen der XML-Kontrolldatei vom Bootmedium oder über das Netzwerk – diese kann anhand des Klassenmodells erzeugt und in Abhängigkeit von IP- oder MAC-Adresse unter Zuhilfenahme eines Verzeichnisdienstes zur Verfügung gestellt werden
- Automatische Installation gemäß den XML-Daten

2.3.6 Zertifizierungen

Bei den Zertifizierungen muss zwischen der Hardware-, der Software- und der Mitarbeiter-Zertifizierung unterschieden werden.

Zu beachten ist bei allen Zertifizierungen, dass diese in der Regel nur dann gelten, wenn eine Distribution in unveränderter Form und mit allen Sicherheitsaktualisierungen eingesetzt wird. Erweist es sich in einem Projekt als erforderlich, ein bestimmtes Softwarepaket durch ein aktuelleres auszutauschen, entfällt die Zertifizierung.

2.3.6.1 Hardware

Im Rahmen der Hardware-Zertifizierung erfolgt ein Testprozedere und abschließend eine Zertifizierung der Produkte auf bestimmte Linux-Plattformen und Versionen. Überprüft wird die Performance und Funktionstüchtigkeit der Hardware im Zusammenspiel mit bestimmten Linux-Distributionen. Hardware-Hersteller haben die Möglichkeit, mit dem Produzenten der jeweiligen Distributionen ihre Produkte zertifizieren zu lassen. Für Hardware-Hersteller leistet eine solche Zertifizierung neben der Qualitätssicherung ein wirksames Marketingargument.

Die Zertifizierungen bieten den Kunden, speziell im Umfeld unternehmenskritischer Anwendungen und Lösungen, wie beispielsweise Einsatz von ERP-Systemen mit RAID- oder SAN-Hardware, eine erhöhte Sicherheit bezüglich der Kompatibilität der verwendeten Hardware und des Betriebssystems. Für die späteren Kunden bzw. Anwender kann die Zertifizierung ein entscheidender Aspekt für die Kaufentscheidung sein.

2.3.6.2 Software

Die Software-Zertifizierungen werden von den jeweiligen Software-Herstellern (Independent Service Vendor) durchgeführt. Die einzelnen Hersteller validieren und zertifizieren die Distributionen als Betriebssystem-Plattform für ihre Anwendungssoftware. Beispielsweise haben die Unternehmen SAP und Oracle den Suse Linux Enterprise Server als Plattform für bestimmte Anwendungen zertifiziert. Zertifizierungen liegen auch für Systeme des Distributions-Herstellers Red Hat vor. In der Regel werden nur die Enterprise-Versionen der jeweiligen Distributions-Hersteller dem Zertifizierungs-Prozess unterworfen.

Die Software-Zertifizierung ist für viele Kunden eine Grundvoraussetzung für den Einsatz einer Betriebssystemplattform, denn oftmals erhalten sie für die Installation und den Betrieb der Anwendungssoftware nur den notwendigen Support durch die jeweiligen Anwendungshersteller, wenn eine Zertifizierung erfolgt ist.

2.3.6.3 Mitarbeiter-Zertifizierungen

Neben der Hard- und Software-Zertifizierung werden Zertifizierungen zu den Fachkenntnissen und den Fähigkeiten der Mitarbeiter verlangt.

Zurzeit sind die beiden maßgeblichen Zertifizierungsprogramme

- von Red Hat, der Red Hat Certified Engineer (RHCE)[1]
- und dem Linux Professionell Institute (LPI)[2]

marktführend. Die Ziele beider Zertifizierungsmaßnahmen sind u. a. die Schaffung von Standards für die Mitarbeiterqualifizierung. Der Arbeitgeberseite bieten sich durch die Qualifizierungsmöglichkeiten folgende Vorteile:

---

1 http://www.redhat.com/training/rhce/courses/index.html

2 http://www.de.lpi.org/

- Unterstützung bei Einstellungsverfahren
- Standardisierte Qualifizierung von Mitarbeitern

Den Mitarbeitern oder bzw. den zukünftigen potenziellen Mitarbeitern bieten die Zertifizierungen:

- Qualifizierung für den Aufgabenbereich
- Nachweis der Qualifizierung
- verbesserte Chancen auf dem Arbeitsmarkt

Beide Zertifizierungsprogramme können grundsätzlich als vergleichbar angesehen werden, wobei das RHCE mehr auf die eigene Distribution abgestimmt ist. Das Unternehmen Red Hat begann das Red Hat Certified Engineer (RHCE) Programm zu entwickeln, als es noch keine anderen Linux-Zertifikationsprogramme gab. Erst danach hat sich aus der Linux-Gemeinschaft das LPI entwickelt. Es ist anbieterneutral, distributionsneutral und zugleich eine gemeinnützige Organisation.

2.3.7 Fazit

Insgesamt stehen den Anwendern zahlreiche Distributionen und Distributionsversionen zur Auswahl. Wichtig für die Entscheidung ist die Identifikation und Festlegung von notwendigen Anforderungen wie z.B. Managebarkeit oder Support oder Zertifizierungen. Die Entscheidung für eine bestimmte Distribution kann nur in Abhängigkeit von den jeweiligen Erwartungen an die Distribution bzw. deren Hersteller und den Rahmenbedingungen erfolgen. Wird beispielsweise mangels interner Ressourcen umfangreicher Herstellersupport verlangt, sind in erster Linie die Distributionen der kommerziellen Anbieter zu bevorzugen. Ist eine Hardware- oder Softwarezertifizierung für ein bestimmtes Anwendungsszenario notwendig, können diese in der Regel nur die Enterprise-Versionen der kommerziellen Anbieter bieten. Welche Hard- und Software für welche Distribution und Version tatsächlich zertifiziert ist, gilt es im Einzelfall zu prüfen.

Für Anwender, die nicht auf eine kommerzielle Variante angewiesen sind, steht mit der Debian-Distribution eine stabile, gut getestete und bewährte Distribution zur Verfügung. Werden umfangreiche Support-Dienstleistungen benötigt, kann auch in diesem Fall auf zahlreiche Dienstleitungsunternehmen auf dem Markt zurückgegriffen werden.

2.4 Open Source Lizenzmodelle

Innerhalb der Linux-Welt existiert eine ganze Reihe von unterschiedlichen Lizenzmodellen, die wichtigsten werden im Folgenden aufgeführt und kurz charakterisiert.

2.4.1 GPL

Das wohl bekannteste Lizenzmodell ist die General Public License (GPL)[1], das in der Free Software Foundation erarbeitet worden ist. Der Linux Kernel sowie ein Großteil aller Linuxanwendungen unterliegen der "GPL", einer Lizenz, die unter anderem die freie Verfügbarkeit und die Offenlegung des Quellcodes dieser Programme garantiert. Zur Absicherung, dass die Software auch in Zukunft frei bleibt, werden durch die GPL die Freiheiten und Bedingungen der Nutzung genau festgelegt.

Die Freiheiten und Bedingungen umfassen im Einzelnen:

- Paragraph 0:
  Die Freiheit, das Programm für jeden Zweck auszuführen.
- Paragraph 1:
  Erlaubt das Erstellen und die Verbreitung von wörtlichen Quellcodekopien des Programms, sofern der Copyright-Vermerk und die Lizenz mit kopiert und verbreitet wird. Ausdrücklich erlaubt ist auch die Erhebung einer Gebühr für die physikalische Erstellung einer Kopie und anderer Dienstleistungen, wie zum Beispiel Gewährleistungen.
- Paragraph 2:
  Erlaubt Veränderungen an dem Programm und die veränderte Version zu kopieren und zu verbreiten, sofern die veränderte Version Angaben über die Änderungen enthält und gebührenfrei und unter denselben Lizenzbedingungen veröffentlicht wird. Ausgenommen sind Teile des veränderten Programms, die unabhängige Abschnitte darstellen und separat verbreitet werden.
- Paragraph 3:
  Erlaubt das Kopieren des Programms oder einer abgeleiteten Version in Objektcode oder ausführbarer Form, sofern der dazugehörige maschinenlesbare Quellcode oder ein schriftliches Angebot (min. 3 Jahre gültig), diesen Quellcode auf Anfrage bereitzustellen, beigefügt sind.

Die weiteren Paragraphen betreffen den Verfall von Lizenzrechten, den Haftungs- und Gewährleistungsausschluss, Konfliktsituationen mit anderen Ansprüchen und eine Reihe von weiteren Themen, die im Bedarfsfall nachzulesen sind.

Die GPL verhindert durch ihre Bedingungen die Privatisierung von kollektiv erstellter Software und fördert somit ausdrücklich die Erweiterung des Bestandes von freier Software.

[1] Das englische Original finden sie unter: http://www.gnu.org/copyleft/gpl.html. Eine deutsche Übersetzung finden sie unter: http://www.novell.com/de-de/licensing/gpl.html, verbindlich ist jedoch nur das Original.

2.4.2 Lesser GPL

Eine alternative Lizenzform stellt die GNU Lesser General Public License (LGPL)[1] dar. Die Lizenz wurde ursprünglich unter dem Namen Library GPL entworfen.

Die LGPL deckt sich in weiten Teilen mit den inhaltlichen Absichten der GPL. Das heißt, die Software bzw. Bibliotheken müssen frei kopierbar, verbreitbar und modifizierbar sein. Zudem muss der Quelltext, auch der von den modifizierten Versionen, verfügbar sein.

Der Unterschied zur GPL besteht in erster Linie in der Tatsache, dass Programme, die nicht unter GPL oder Ähnlichem stehen, freie Bibliotheken unter LGPL verwenden und eine ausführbare Einheit bilden dürfen. Würden die Bibliotheken unter GPL stehen, dürften nur unter GPL stehende Programme diese auch einbinden. Die LGPL erlaubt den Entwicklern hingegen Programme zu entwerfen, die nicht unter dem stringenten Schutz der GPL stehen, und dabei trotzdem freie Bibliotheken zu verwenden. Programme, die unter LGPL stehende Bibliotheken verwenden, dürfen unter frei wählbaren Lizenzbedingungen verbreitet werden. Für den Kunden muss aber der Quellcode, für die unter LGPL stehenden Bibliotheken verfügbar sein, so dass er den Code ändern und neu einbinden kann.

2.4.3 BSD Lizenz

Die BSD Lizenz[2] ist eines der ältesten freien Lizenzmodelle. Für die Verbreitung von modifizierten Unix-Versionen[3] entwickelte die Berkeley Universität das Lizenz-Modell.

Die BSD Lizenz erlaubt das freie Kopieren der Software mit oder ohne eigene Modifikationen als Quellcode und/oder Binaries unter den folgenden Bedingungen:

- Bei der Verbreitung der Software müssen in den entsprechenden Dateien der Copyright Vermerk und die BSD Lizenz selbst enthalten sein.
- Bei der Verbreitung der Software in Binärform, müssen der Copyright Vermerk und die Bestimmungen der BSD Lizenz in der Programmdokumentation oder anderweitig enthalten sein.
- Weder der Name der Universität noch die Namen der Autoren dürfen ohne schriftliche Genehmigung zu Werbezwecken verwendet werden.

In der ursprünglichen Version der Lizenz gab es noch einen weiteren Aspekt. Demnach mussten alle Werbematerialien, die ein unter Lizenz stehendes Feature bewerben, den Hinweis "Dieses Produkt beinhaltet Software, die von der Universität von Kalifornien in Berkeley und ihren Kontributoren entwickelt wurde"

---

1 http://www.gnu.org/copyleft/lesser.html

2 http://www.opensource.org/licenses/bsd-license.html

3 Die Lizenz bezog sich ausschließlich auf den von der Universität Berkeley erstellten Quellcode

tragen. Diese Klausel wurde aus der alten Lizenz entfernt und das letzte Berkeley Release wurde unter der neuen Variante lizenziert. Deshalb wird auch von der alten und der neuen BSD-Lizenz gesprochen.

Die BSD-Lizenz beinhaltet keinerlei Einschränkungen für den Gebrauch und die Weiterverbreitung von Quellcode und Programmen. Einzig Copyright-Hinweis, dass die BSD-Lizenzbedingungen selbst und ein Garantieausschluss dem Werk beizulegen sind. Die Lizenz schreibt nicht explizit vor, dass modifizierte Software im Quellcode weitergegeben werden muss. So kann jede beliebige Software-Firma Source Code, der unter BSD-Lizenz steht, in eines ihrer Produkte integrieren und dafür dann den Source Code unter Verschluss halten.

Die BSD-Lizenz ist im Vergleich zu den zuvor beschriebenen Lizenzen mit Restriktionen verbunden, die jedoch als geringfügig eingestuft werden können.

3 Technische Betrachtung der Migrationspfade

3.1 Einleitung

In den technischen Betrachtungen werden die einzelnen Produkte, Lösungen, Dienste, wie sie im Kapitel 2 in den abgebildeten IT-Landschaften dargestellt werden, aus technischer Sicht näher unter die Lupe genommen. Betrachtet werden:

- die Infrastrukturdienste
  - Dateiablagedienste
  - Druckdienste
  - Authentifizierungsdienste
  - Netzwerkdienste
- die Middleware- und Integrationskomponenten
  - Verzeichnisdienst
  - Objektkomponentenmodelle
  - Plattformen für verteilte Systeme und Web-Services
  - XML
- die Serverdienste
  - Groupware und Messaging
  - Datenbankserver
  - Webserver
  - Sonderdienste
- die Desktopanwendungen inkl. Officepaket

Im Focus der Betrachtungen steht die technische Machbarkeit einer Migration einzelner Microsoft-Produkte hin zu adäquaten OSS- oder COLS-Lösungen. Ausgehend von der in Kapitel 2.1 dargestellten Windows-geprägten IT-Landschaft wird für die einzelnen Komponenten dieser Landschaft genau geprüft:

- Wie sieht die Ausgangslage aus?
  - Welche wichtigen Funktionen stehen zur Verfügung?
  - Welche Schnittstellen werden bzw. müssen bedient werden?
  - Was sind die Besonderheiten im Wirkbetrieb?
- Welche Alternativen stehen als OSS- oder ggf. auch als COLS-Lösung zur Verfügung?
  - Wo liegen die funktionalen Unterschiede?

- Werden die kritischen Anforderungen abgedeckt?
- Welche Schnittstellen werden bzw. müssen bedient werden?
- Was ist bei der Migration zu beachten, wo liegen die Probleme, wie sind diese zu lösen?
- Gibt es mehrere Alternativen, für wen bzw. für welchen Zweck ist welche der Alternativen zu verwenden?
- Wie lassen sich die Alternativen in heterogene Welten integrieren, wenn notwendig, wie funktioniert das Zusammenspiel insbesondere mit Microsoft (Kompatibilität, Interoperabilität)?
- Wie wirkt sich die mögliche Integration auf zukünftige Microsoft-Produktlinien aus?

❍ Was sind die Potenziale bei der Fortführung der Microsoft Produktlinie?

- Welche zusätzlichen Funktionalitäten stehen zur Verfügung?
- Wo liegen die wesentlichen Änderungen?
- Erfüllen die Neuerungen und mögliche Modifikationen offene kritische Anforderungen?
- Was ist hinsichtlich der Unabhängigkeit der Systeme zu beachten?

Alle Betrachtungen schließen in der Regel mit einer Kurzbewertung ab. Bei mehreren Alternativen werden, sofern sich dies als sinnvoll erweist, auch diese vergleichbaren Lösungen kommentiert.

3.2 Dateiablage

3.2.1 Überblick

Im Ergebnis der folgenden detaillierten, technischen Betrachtungen der Dateiablagedienste lässt sich zusammenfassend festhalten:

Bei der direkten Ablösung eines Windows NT Servers als Dateiablage unter Beibehaltung der Windows Clients bietet sich im Open Source Bereich Samba als erste Wahl an. Für einen Windows-Client stellt sich Samba ziemlich genau wie ein NT-Server dar. Samba wird kontinuierlich weiterentwickelt und neben der Community auch von einer wachsenden Zahl IT-Dienstleistern unterstützt.

Je nach Umfang einer clientseitigen Linux-Migration rücken auch NFS und AFS in den Fokus der Alternativbetrachtungen. NFS und AFS sind in UNIX-Netzen verbreitet, für die Einbindung von Windows-Clients ist aber die Installation von spezieller Software auf allen Clients erforderlich. Ein NFS-Client ist unter anderem in Microsoft Windows Services for UNIX (SFU 3.0) enthalten. Ein AFS-Client ist kostenlos und als Open Source von OpenAFS.org erhältlich. Für den Einsatz von NFS oder AFS in einer Umgebung mit Windows-Clients sind in jedem Fall tief greifende konzeptuelle Änderungen im Vergleich zur Dateiablage mit Windows NT erforderlich.

Wenn das Kerberos-Sicherheitskonzept, das auch dem Active Directory von Windows 2000 zu Grunde liegt, bei der Modernisierung der IT-Infrastruktur im Rahmen eines Migrationsprojektes eine wichtige Rolle spielt, sollte auch bei einer Fortführung der Windows-Produktlinie auf der Clientseite das OpenAFS als Alternative zu Win2000 als Dateiserver weiter evaluiert werden.

Für die physikalische Speicherung der Daten auf den Plattensystemen der eigentlichen Server eignen sich u.a. die Dateisysteme XFS und EXT3. Beide Systeme unterstützen Journaling-Funktionalitäten, Quotas und die Vergabe von Zugriffberechtigungen auf Datei- und Verzeichnisebene. Sowohl XFS als auch EXT3 unterstützen erweiterte Dateiattribute und POSIX-ACLs für die Gewährung von Rechten. Bei der Abbildung der Windows-ACL auf die POSIX-ACL ist zu berücksichtigen, dass die feine Granularität, in der die Rechte unter Windows definiert werden können, verloren geht. Es bleibt letztendlich zu prüfen, welche Auswirkungen die Einschränkungen im Einzelfall haben und ob diese akzeptiert werden können.

3.2.2 Windows NT 4

3.2.2.1 Funktionale Anforderungen

Der generelle Funktionsumfang einer netzwerkgestützten Dateiablage besteht in der:

- Entgegennahme (Schreiben) und Lieferung(Lesen) von Dateien
- Erzeugung und Darstellung einer Verzeichnisstruktur
- Verwaltung und Darstellung von Metadaten für Verzeichnisse und Dateien
- Umsetzung von Zugriffsrechten und -beschränkungen für Verzeichnisse und Dateien
- Verwaltung von Dateisperren bei konkurrierendem Zugriff

Die Nutzung von Windows NT File Services dient in den meisten Umgebungen den folgenden Zwecken:

- Ablage der benutzerspezifischen Dateien (Home-Verzeichnisse)
- Ablage der servergestützten Profile, sofern zwischen Client-Computern wandernde Benutzer (Roaming User) optimiert unterstützt werden sollen
- Ablage von gruppenspezifischen Dateien (Gruppen-Ordnern), die nur von einigen Benutzern (z.B. die einer Abteilung) genutzt werden sollen
- Ablage von dateibasierenden Datenbanken, die von mehreren Benutzern gleichzeitig benutzt werden sollen (z.B. MS Access Datenbanken mit getrenntem Frontend)

- Ablage von Programmdateien (exe-Dateien, dll-Dateien etc. einer Anwendung), um eine Ablage auf dem Client-Computer zu vermeiden
- Ablage von Datenbankensystemen, die die Möglichkeit bieten, die Nutzdaten auf einem anderen Server unter einem UNC-Pfad abzulegen.

Die hier beschriebenen Nutzungszwecke bewirken in der Praxis oftmals sehr unterschiedliche technische Detail-Anforderungen, die in den folgenden Absätzen an geeigneter Stelle hervorgehoben werden.

3.2.2.2 Das Dateisystem NTFS4

Das Dateisystem NTFS4 bildet die Grundlage für die Dateiablage und -Verwaltung unter Windows NT4.

Eigenschaften

NTFS4 besitzt unter anderen folgenden Eigenschaften:

Jeder Ordner und jede Datei verfügt über eine so genannte Access Control List (ACL), die an der Datei oder dem Ordner gespeichert wird. In der ACL stehen so genannte Access Control Entries (ACE), in dem die SID des Gruppen- oder des Benutzerkontos und die Berechtigung stehen. Über die ACL erfolgt somit die Zugriffssteuerung, die insgesamt granular aufgebaut werden kann. Die ACL ist in die Bereiche SACL (System Access Control List) und DACL (Discretionary Access Control List) zu unterscheiden: In der DACL sind die SIDs der Gruppen und Benutzer abgelegt, die auf das Objekt zuzugreifen dürfen bzw. daran gehindert werden. In der SACL ist festlegt, wie das Sicherheitssubsystem die Zugriffe auf das Objekt überwacht.

NTFS4 unterstützt im Prinzip keine Vererbung: Lediglich beim Neuerstellen einer Datei werden die Rechte des Ordners in die ACL der Datei kopiert. Ändern sich die Rechte des Ordners, muss explizit das Durchschreiben in die ACLs der beinhalteten Dateien angeordnet werden. Eine Besonderheit ist zu beachten: Eine Datei, die sich im UNC-Pfad \\server\freigabe\ordner\subordner befindet, kann von einem Anwender gelesen werden, obwohl der Ordner „ordner“ das Lesen verbietet, der Ordner „subordner“ es aber zulässt.

Bezüglich der Länge der Pfadnamen gibt es kein Limit. Unterstützt werden Dateinamen mit bis zu 256 Zeichen. Die verwendeten Zeichen dürfen theoretisch dem Unicode-Zeichensatz (16bit) bis auf wenige Ausnahmen (z.B. *, \) entnommen werden. Zu jedem Ordner und jeder Datei wird ein Kurzname gespeichert, welcher der 8.3-Konvention entspricht und automatisch vom Betriebsystem generiert wird. Während bei der Speicherung dabei zwischen Groß- und Kleinschreibung unterschieden wird, ist dies beim Zugriff auf die Datei in der Regel nicht der Fall.

Jeder Ordner und jede Datei verfügt über Attribute in Form von Flags (schreibgeschützt, Archiv, System, versteckt und komprimiert) und über die Zeiten der ersten Erstellung, der letzten Änderung und des letzten Zugriffs. Der Komprimierungsgrad ist stark abhängig vom Inhalt.

NTFS unterstützt die Technologie von Multiple Streams. Die Einsatzhäufigkeit ist relativ gering. Alternative Daten Streams werden zum Teil auch von Schadprogrammen genutzt, da viele Virenscanner diese Streams nicht untersuchen und die Schadprogramme daher unentdeckt bleiben. Multiple Streams müssen von der jeweiligen Anwendung unterstützt werden bzw. in dieser programmiert sein. Multiple Streams ermöglichen unter anderem die Speicherung der Ressource Folk von Macintosh-Dateien.

Seit dem Service Pack 4 werden innerhalb von NTFS Quotas unterstützt. Die Vergabe und Kontrolle der Quoten basiert auf der Besitzer-Eigenschaft und umfasst das gesamte Volumen (logisches Laufwerk des File Servers). Durch diese technischen Beschränkungen ist der Einsatz eher als ein Sonderfall und weniger als die Regel in bestehenden Umgebungen einzustufen.

Die maximale Dateigröße ist unter NTFS4 auf 2 TB (Terabyte) und die Größe des logischen Laufwerkes beschränkt. Das logische Laufwerk kann maximal 2 TB (theoretisch 16 Exabyte) umfassen. Die tatsächliche Netto-Datenmenge hängt von der Clustergröße ab, die bei der Formatierung verwendet wurde. Die Anzahl der Dateien ist auf 2^{32}-1 beschränkt.

NTFS ermöglicht ein Auditing (Überwachen) der erfolgten Zugriffe bzw. der Zugriffsversuche. Auf diese Weise können z.B. wiederholte, ungewünschte Löschungen von Dateien diagnostiziert werden.

NTFS formatierte Datenträger werden im laufenden Betrieb defragmentiert. Eine automatische Korrektur (Selbstheilung) unter Windows NT 4 erfolgt nicht. Zu diesem Zweck müssen Produkte von Drittherstellern eingesetzt werden.

Rechtesystem des NTFS

Windows kennt insgesamt 13 Berechtigungen, die einem Objekt im Dateisystem (Datei oder Verzeichnis) pro Benutzer oder Gruppe zugeordnet bzw. entzogen werden können:

- Ordner durchsuchen / Datei ausführen
- Ordner auflisten / Datei lesen
- Attribute lesen
- Erweiterte Attribute lesen
- Dateien erstellen / Daten schreiben
- Ordner erstellen / Daten anhängen
- Attribute schreiben
- Erweiterte Attribute schreiben
- Unterordner und Dateien löschen
- Löschen
- Berechtigungen lesen

- Berechtigungen ändern
- Besitzrechte übernehmen.

Änderungen an Zugriffsrechten werden über den Dialog *Eigenschaften* und dort auf der Karteikarte *Sicherheitseinstellungen* vorgenommen. In der Absicht, die Komplexität des Systems aus 13 eng verwandten Einzelberechtigungen vor dem Durchschnittsbenutzer zu verbergen, werden in dieser Karteikarte vordefinierte Aggregate, so genannte *Sammelberechtigungen*, aus sinnvollen Kombinationen der Einzelberechtigungen zur Auswahl angeboten. Für Dateien gibt es fünf, für Verzeichnisse sechs solcher Sammelberechtigungen, die jeweils zugelassen oder verweigert werden können. Erst im Dialog *Berechtigungseintrag* der über die Buttons *Erweitert/Anzeigen/Bearbeiten* in den *Sicherheitseinstellungen* erreichbar ist, werden die 13 einzelnen Berechtigungen komplett dargestellt.

Dabei ist die bei den Sicherheitseinstellungen gebotene Sicht auf die Sammelberechtigungen äußerst problematisch, weil die Darstellung sehr schnell das Fehlen von Rechten suggerieren kann, obwohl sie in Wirklichkeit vorhanden sind. So entsteht beispielsweise aus einem Vollzugriff, bei dem allein die Berechtigung zum Schreiben der erweiterten Attribute nicht zugelassen ist, in der einfachen Darstellung bei den Sicherheitseinstellungen das Bild eines Rechteprofils, das nur das Lesen und Ausführen erlaubt. Die folgende Tabelle zeigt, welche Kombinationen von Berechtigungen zu welcher Darstellung als Sammelberechtigung führt. Wohlgemerkt, wenn nur ein einziges Recht in diesen Aggregationen nicht gesetzt ist, enthält die entsprechende Checkbox für die Sammelberechtigung kein Häkchen mehr.

Tab. 9: Eigenschaften der Windows Sammelberechtigungen

	Windows Sammelberechtigungen					
	Voll-zugriff	**Ändern**	**Lesen & Ausführen**	**Ordner-inhalt auflisten**	**Lesen**	**Schreiben**
Ordner durchsuchen / Datei ausführen	X	X	X	X		
Ordner auflisten / Daten lesen	X	X	X	X	X	
Attribute lesen	X	X	X	X	X	
Erweiterte Attribute lesen	X	X	X	X	X	
Dateien erstellen / Daten schreiben	X	X				X
Ordner erstellen / Daten anhängen	X	X				X
Attribute schreiben	X	X				X
Erweiterte Attribute schreiben	X	X				X
Unterordner/Dateien löschen	X					
Löschen	X	X				

	Windows Sammelberechtigungen					
	Voll-zugriff	Ändern	Lesen & Ausfüh-ren	Ordner-inhalt auflisten	Lesen	Schrei-ben
Berechtigungen lesen	X	X	X	X	X	X
Berechtigungen ändern	X					

Wegen der beschriebenen Inkonsistenzen wird im Folgenden ausschließlich die erweiterte Ansicht im Dialog *Berechtigungseintrag* betrachtet.

Attributsystem

Zusätzlich zu den Berechtigungen wird für Datei- und Verzeichnisobjekte noch eine Anzahl von so genannten *Attributen* und *erweiterten Attributen* verwaltet.

Tab. 10: Windows Attribute

Name	Bit	Bedeutung
Archiv	A	Datei wurde seit dem letzten Zurücksetzen des Attributes verändert
Schreibgeschützt	R	Datei ist schreibgeschützt
Versteckt	H	Datei wird nicht angezeigt
System	S	Datei ist für das System reserviert
Komprimiert	C	Datei/ Ordner wird auf dem Medium komprimiert gespeichert
Verschlüsselt	E	Datei/ Ordner wird auf dem Medium verschlüsselt gespeichert

Überwachung

Windows verfügt über weit reichende Überwachungsmöglichkeiten auf der Datei- und Verzeichnisebene. So können alle Berechtigungen einzeln pro Benutzer oder Gruppe überwacht werden. Die daraus resultierenden Informationen werden im Sicherheitsprotokoll des Domänen-Controllers bzw. des jeweiligen Windows 2000 Rechners gespeichert, sofern in der Systemrichtlinie die Überwachungsrichtlinie freigegeben wird.

3.2.2.3 Zugriffssteuerung

Die Zugriffssteuerung über das Netzwerk auf Dateien oder Ordner erfolgt in Windows NT Umgebungen über zwei Mechanismen:

- Ordnerfreigabe (Share)
- und NTFS-Rechte.

Um über das Netzwerk auf eine Datei zugreifen zu können, muss einer der darüberliegenden Ordner freigegeben werden. Diese Freigabe wird ebenfalls mit ei-

ner ACL versehen, die in der Registry gespeichert wird. Die Rechte auf diese Freigabe beschränken sich auf die Stufen

- Lesen
- Ändern
- und Vollzugriff.

Diese Rechte gelten absolut. D.h., dass darunterliegende NTFS-Rechte effektiv durch die Freigaberechte beschnitten werden. Beispiel: Leserecht auf Freigabeebene verhindert das Schreiben auch dann, wenn die NTFS-Rechte dies zulassen würden.

Besonderes Augenmerk in Windows NT Umgebungen ist den Privilegien (Richtlinien für Benutzerrechte) zu schenken, denn sie können hinsichtlich der File Services z.B. durch „Besitz übernehmen von Dateien und Objekten“ und „Sichern von Dateien und Ordnern“ von Bedeutung sein.

3.2.2.4 Benutzer und Gruppenkonzept

Jeder Ordner und jede Datei ist einem Besitzer zugeordnet, der sowohl eine Gruppe als auch ein Benutzerkonto sein kann. Im Normalfall wird der erzeugende Benutzer der Besitzer. Ist der Benutzer Mitglied der Administratorengruppe, wird diese Gruppe der Besitzer.

Eine systematische Zugriffssteuerung in der Windows NT Umgebung bevorzugt die Vergabe von Rechten an Gruppen. Die Vergabe von Rechten an einzelne Benutzerkonten sollte den benutzerspezifischen Dateiablagen vorbehalten bleiben.

Innerhalb einer Windows NT Umgebung sind folgende Gruppentypen zu unterscheiden:

- globale Gruppen
- lokale Gruppen auf Member Servern
- lokale Gruppen auf Domain Controllern

Lokale Gruppen auf Domain Controllern unterscheiden sich insofern von denen auf Member Servern, als sie auf allen Domain Controllern der Domäne mit der gleichen SID vorhanden sind.

Lokale Gruppen auf Member Servern dürfen mit den folgenden Gruppen (Group Nesting) verschachtelt sein:

- den globalen Gruppen der eigenen Domäne
- oder den globalen Gruppen der Domänen, denen die eigene vertraut.

Globale Gruppen haben nur Benutzerkonten als Mitglieder.

In einer Windows NT Domänenlandschaft sind zwei verschiedene „klassische“ Zugriffsteuerungen bekannt:

- B-G-L-R Methode:
  Der Benutzer ist Mitglied einer globalen Gruppe. Die ist wiederum Mitglied einer lokalen Gruppe eines File Server. Nur für diese lokale Gruppe sind NTFS Berechtigungen an einer Datei-Ressource gesetzt (siehe Bild 5).
- B-G-R Methode:
  Der Benutzer ist Mitglied einer globalen Gruppe. Nur für diese globale Gruppe sind NTFS Berechtigungen einer Datei-Ressource vergeben (siehe Bild 6).

Bild 5: B-G-L-R Methode

Bild 6: B-G-R Methode

Beide Methoden funktionieren nur dann ohne Sicherheitsrisiken, wenn die Zuordnung von Ressource und lokaler Gruppe (bzw. globaler Gruppe) eindeutig ist. Das heißt, dass die Gruppe ausschließlich für diese Ressource verwendet wird.

Werden die File Services durch einen Cluster realisiert, hat die Methode B-G-L-R den Nachteil, dass die lokalen Gruppen auf den Knotenservern nicht die identischen SIDs besitzen können. Abhilfe schafft hier nur die Konfiguration der Knoten als Domain Controller oder die Verwendung der Methode B-G-R.

3.2.2.5 Werkzeuge

Zur Bearbeitung von Dateien und Ordnern und deren Rechte bietet Windows NT eine recht eingeschränkte Auswahl an Werkzeugen.

Mit graphischer Oberfläche:

- NT Explorer (explorer.exe)
- Datei Manager (winfile.exe).

Nur auf Kommandozeile:

- calcs
- Resource Kit Tools: xcacls, scopy etc.

Die mitgelieferten Werkzeuge bieten in der Regel nicht den vollen, sondern nur einen dedizierten Funktionsumfang. Bestes Beispiel hierfür ist der NT Explorer: er ermöglicht es nicht, den Besitzer zu setzen (nur zu übernehmen) oder ACLs mit zu kopieren. Es ist daher davon auszugehen, dass die Administration einer NT Umgebung über Werkzeuge von Drittherstellern oder selbst entwickelte Skripte (z.B. Perl) verfügt, die die Verwaltung vereinfachen oder sehr spezielle Aufgaben erledigen. Die Folge kann sein, dass die durch einen NT Explorer angezeigte Rechtestruktur von den tatsächlich vergebenen Zugängen abweicht.

3.2.2.6 Netzwerkprotokolle

Die Kommunikation über das Netzwerk mit Windows NT File Servern kann auf verschiedenen Transportprotokollen basieren:

- TCP/ IP
- NetBEUI
- SPX/ IPX
- Appletalk.

In einer existierenden NT Umgebung sind TCP/ IP, NetBEUI und SPX/ IPX nicht unwahrscheinlich. Es wird grundsätzlich angenommen, dass TCP/ IP als das zukünftige und einzig relevante Protokoll angestrebt wird. Aus diesem Grund werden auch die Dienste „Gateway Services for Netware“ und „File and Print Services for Macintosh“ nicht weiter betrachtet.

Hinsichtlich der File Services kann somit

- SMB (Server Message Block) via NetBT (NetBIOS over TCP/ IP)

als Standard mit den Ports 137/UDP/TCP (nbname), 138/UDP (nbdatagram) und 139/TCP (nbsession) angesehen werden.

3.2.2.7 Verbindungsherstellung

Dem Anwender werden in der Regel die Freigaben auf den File Servern in Form von Laufwerksbuchstaben bereitgestellt. Dies erfolgt oftmals per Logon-Script. Darüber hinaus besteht für den Anwender die Möglichkeit, im Windows Netzwerk zu „browsen“. D.h. er kann File Server anklicken und sich mit den sichtbaren Freigaben über ein Netzlaufwerk verbinden oder sie direkt öffnen.

3.2.2.8 Besonderheiten im produktiven Betrieb, die bei der Migration zu beachten sind

Im Folgenden werden exemplarisch einige Besonderheiten beschrieben, die sich im Rahmen einer Migration als kritische Punkte erweisen könnten.

- Zuweilen wird hinsichtlich der Ablage von benutzerspezifischen Dateien (Home-Verzeichnisse) verlangt, dass dort abgelegte Daten nur vom Benutzer selbst und dem Betriebssystem (z.B. zwecks Virenschutz) gelesen werden können. Unter Windows NT besteht die Möglichkeit, hierfür das Konto System zu verwenden.
- Die Ablage der servergestützten Profile unterliegt beim Zurückschreiben einem komplizierten Prozess seitens des Clients. Insbesondere in Terminal Server Umgebungen, die servergestützte Profile zwingend erfordern, ist die fehlerfreie Kommunikation und Rechtestruktur zu gewährleisten.
- Gruppenspezifische Dateien können von mehreren Benutzern gleichzeitig bearbeitet werden. Förderlich ist hierbei, dass die Anwender über die gemeinsame Verwendung informiert werden. Beispiel: der Anwender, der als zweiter eine Word-Datei öffnet, erhält die Meldung, dass Anwender 1 diese Datei bereits geöffnet hat und er sie nur schreibgeschützt öffnen kann.
- Bei der Ablage von dateibasierenden Datenbanken, unter die auch z.B. pst-Dateien (Persönliche Ordner in Outlook) fallen, muss ein fehlerfreies Locking funktionieren.
- Oftmals kann die Ablage von Programmdateien nicht komplett schreibgeschützt erfolgen. Es sind dann sehr granulare Berechtigungsstufen erforderlich (z.B. Schreiben aber nicht Löschen einer speziellen Datei).
- Nur wenige Anwendungen mit Datenbankensystemen (z.B. MS SQL) bieten die Möglichkeit, die Nutzdaten auf einem anderen Server unter einem UNC-Pfad abzulegen. Die fehlerfreie Kommunikation und Dateiablage ist hier aber besonders kritisch und unterliegt der Freigabe des Anwendungsherstellers.

3.2.2.9 Verwandte Themen

File Services unter Windows NT müssen neben der reinen Dateiablage noch andere wichtige Anforderungen erfüllen, um in existierenden Umgebungen durch Produkte von Drittherstellern befriedigt eingesetzt werden zu können.

- **Virenschutz**:
  Der Virenschutz erfolgt zumeist durch die lokale Installation eines Virenscanners auf dem File Server selbst. Durch einen lokal installierten Dienst wird das Scannen einer Datei beim Zugriff erst möglich. Viele Hersteller von Virenschutz-Software adressieren dieses Problem auf diese Weise. Alternativ besteht die Möglichkeit, die Laufwerke des File Servers über das Netzwerk von einem anderen Computer aus zu scannen. Die Nachteile sind offensichtlich; sie ergeben sich durch die entstehende Last und die zeitliche Verzögerung.
- **Quotierung**: Die eingebaute Quotierung von Windows NT wird in der Regel nicht verwendet. Der Einsatz von Drittherstellerprodukten ist notwendig, um benutzer- und gruppenspezifische Ablagen zu quotieren.
- **Datensicherung**: Der Einsatz des Bordmittels NTBACKUP ist als eher selten einzustufen. In der Regel werden File Server unter Windows NT durch die Installation einer entsprechenden Komponente (agent) in ein Datensicherungskonzept eingebunden, die andere Zielsysteme (Datenbanken, Mail) zentral und einheitlich sichert. Ein wichtiges Kriterium in diesem Zusammenhang ist die Wiederherstellungszeit im Desaster Recovery Fall. Als Besonderheit sei hier erwähnt, dass durch das Bordmittel NTBACKUP auch Dateien gesichert werden können, die ansonsten durch den Ausführenden nicht gelesen werden können.
- **Archivierung**: Oftmals wird im Zuge des Datensicherungskonzeptes eine revisionssichere Archivierung betrieben. Darüber hinaus bieten einige Produkte von Drittherstellern die Möglichkeit, selten benutzte Dateien auf kostengünstigere Systeme/ Medien zu verdrängen.

3.2.3 Ablösende Migration

3.2.3.1 Einleitung

In Hinblick auf die Dateiablage wird in diesem Leitfaden davon ausgegangen, dass eine zentrale Dateiablage auf wenigstens einem NT-Server vorhanden ist und zurzeit mit Windows-Clients darauf zugegriffen wird. Bei der Suche nach alternativen Migrationszielen außerhalb der Microsoft Produktlinie muss unterschieden werden zwischen Migrationsszenarien, bei denen eine Alternative nur für die Serverseite gesucht wird und solchen Szenarien, bei denen auch die Clients auf eine andere Betriebssystemplattform gebracht werden sollen.

Bei der Servermigration sind bezüglich der Dateiablage grundsätzlich zwei Ebenen zu betrachten. Zum einen besitzt jeder Server ein lokales Dateisystem, in dem er alle Dateien verwaltet. Zum anderen wird wenigstens eine Untermenge

dieser Dateien über einen Serverdienst mit einem geeigneten Netzwerkprotokoll an die Clients exportiert.

Die Ablösung von Windows NT als Dateiserver beinhaltet auf der ersten Ebene in jedem Fall die Übernahme bestehender Daten und Programme aus dem alten System in das neue. Damit einher geht auch eine Abbildung des Rechtesystems zur Autorisierung des Zugriffs auf Dateien und Verzeichnisse und eine Anpassung der Betriebskonzepte z.B. für die Datensicherung.

Auf der zweiten Ebene geht es um eine Nachbildung der bisherigen Funktionalität, sei es mit den bestehenden Clients oder mit einer neuen Clientarchitektur. Diese zweite Ebene bildet den eigentlichen Kern der Infrastrukturkomponente Dateiablage. Im Focus der Betrachtungen stehen im Besonderen die Themenkomplexe „Zugriffsrechte auf Datei- und Verzeichnisebene“ sowie die „grundsätzlichen Funktionalitäten der Dateiablage“.

Für die Ablösung eines NT 4.0 Servers für die Dateiablage kommen in erster Linie folgende Alternativen in Frage:

- UNIX/Linux mit Samba – Die Nachbildung der Dateiablage des NT-Server
- UNIX/Linux mit NFS – Die traditionelle netzwerkgestützte Dateiablage in UNIX-Netzwerken
- UNIX/Linux mit OpenAFS – Das von IBM freigegebene Netzwerkdateisystem mit Kerberos-Authentifizierung

Alternative Netzwerkdateisysteme, die über ein universitäres Forschungsstadium noch nicht hinausgewachsen sind oder die ganz oder teilweise auf proprietärer Software basieren, werden nicht betrachtet.

3.2.3.2 Genereller Vergleich des Funktionsumfangs für Dateiserver

Bei der funktionalen Übersicht der alternativen Netzdateisysteme kommen indirekt auch Eigenschaften des darunterliegenden Serverdateisystems zum Tragen. Für die linuxbasierten Server wird für diesen Vergleich das XFS oder das EXT3 Dateisystem zu Grunde gelegt.

Tab. 11: Vergleich der Dateiserver

Funktion	WinNT	Win2k	Samba	NFS	AFS
Windows-Client ohne Zusatzsoftware	X	X	X		
Länge der Dateinamen (Zeichen)	256	256	256	256	256
Zeichensatz für Dateinamen	Unicode	Unicode	Unicode	ISO-Latin	ISO-Latin
Darstellung von Groß/ Kleinschreibung	X	X	X	X	X
Unterscheidung von Groß/ Kleinschreibung				X	X
Disk Quotas		X	X	X	X

Funktion	WinNT	Win2k	Samba	NFS	AFS
Verschlüsselung		EFS	dateiweise client-seitig		
Kompression	X	X	[1]	[2]	
Maximale Dateigröße[3]	2 TB	2 TB	2 TB	9 EB[4]	2 GB
Maximale Pfadlänge	Unbegr.	Unbegr.	Unbegr.	Unbegr.	Unbegr.
Änderungsjournal		X			
Propagierung der Freigaben im ActiveDir.		X			
Verteiltes Dateisystem		DFS	DFS	Standard	Standard
Dateireplikationsdienst		FRS	rsync	rsync	rsync
Journaling		X	X (durch Dateisystem)	X (durch Dateisystem)	X (durch Dateisystem)
DACL		NTFS	POSIX	POSIX	AFS
SACL		NTFS	Samba Modul		
Typische Autorisierung über	NT/ LM PDC	AD / Kerberos	NT/LM LDAP, wenn AD-Mitglied dann Kerberos	NIS/ LDAP	Kerberos Version 4

Bei der direkten Ablösung eines Windows NT Servers als Dateiablage unter Beibehaltung der Windows Clients bietet sich im Open Source Bereich Samba als erste Wahl an. Für einen Windows-Client stellt sich Samba ziemlich genau wie ein NT-Server dar. Samba wird kontinuierlich weiterentwickelt und neben der Community auch von einer wachsenden Zahl von IT-Dienstleistern unterstützt.

Je nach Umfang einer clientseitigen Linux-Migration rücken auch NFS und AFS in den Fokus der Alternativbetrachtungen. NFS und AFS sind in UNIX-Netzen verbreitet, für die Einbindung von Windows-Clients ist aber die Installation von spezieller Software auf allen Clients erforderlich. Ein NFS-Client ist unter anderem in Microsoft Windows Services for UNIX (SFU 3.0) enthalten. Ein AFS-Client ist kostenlos und als Open Source von OpenAFS.org erhältlich. Für den Einsatz von NFS oder AFS in einer Umgebung mit Windows-Clients sind in jedem Fall tief greifende konzeptuelle Änderungen im Vergleich zur Dateiablage mit Windows NT erforderlich.

Wenn das Kerberos-Sicherheitskonzept, das auch dem Active Directory von Windows 2000 zu Grunde liegt, bei der Modernisierung der IT-Infrastruktur im

[1] Als Erweiterung (Patch) z.B. für Ext2/3 Dateisysteme erhältlich

[2] Als Erweiterung (Patch) z.B. für Ext2/3 Dateisysteme erhältlich

[3] TB Terabyte 1012, PB Petabyte 1015, EB Exabyte 1018

[4] NFSv3 mit XFS Dateisystem

Rahmen eines Migrationsprojektes eine wichtige Rolle spielt, sollte auch bei einer Fortführung der Windows-Produktlinie auf der Clientseite das OpenAFS als Alternative zu Win2000 als Dateiserver weiter evaluiert werden.

3.2.3.3 Samba

Die grundsätzlich verschiedenen Optionen, nämlich eine zentrale Dateiablage für Windows-Clients oder für eine heterogene Clientumgebung zu realisieren, stehen zunächst gleichwertig nebeneinander. Es gibt keinen Grund, die eine oder andere Lösung grundsätzlich auszuschließen. Bezüglich der Konzepte für Anwendung und Administration sind alle Optionen mit mehr oder weniger umfangreichen Änderungen in Administration und Anwendung verbunden. Im Sinne einer konservativ fortführenden Migration bringen die auf SMB/CIFS basierenden Server Samba und W2K die besten Voraussetzungen für eine weitestgehende Beibehaltung der bestehenden Konzepte.

Samba ist in vieler Hinsicht ein Nachbau des Windows NT Dienstes für Dateiablage, Druckdienste und Authentifizierung. Für die Anwender stellt sich Samba in größter Näherung genau wie ein NT-Server dar. Für die Administratoren ist Samba andererseits ein UNIX-Server. Die Bedienung muss der Philosophie und den Möglichkeiten des neuen Betriebssystems angepasst werden.

W2K als Produktnachfolger von NT bringt für die Anwender kaum mehr Änderungen bezüglich des NT-Servers als ein Samba-Server. Für die Administratoren ergeben sich allerdings unter anderem mit der Einführung von Active Directory mit den Komponenten DNS, LDAP und Kerberos umfangreiche Änderungen.

Inwieweit die Änderung oder Entwicklung in der einen oder anderen Richtung als einfacher oder vorteilhafter bewertet oder empfunden wird, hängt nicht zuletzt von den beteiligten Personen selbst ab. Eine Migration zu Samba, Linux und Open Source eröffnet neue Freiheitsgrade. Ein solcher Schritt zur Emanzipation von den Vorgaben und Best Practices eines Herstellers bringt dem einzelnen Administrator neben mehr Freiheit und mehr Eigenverantwortung aber auch neue Fehlerpotenziale.

Der Samba-Server erfüllt wie ein NT-Server die Anforderungen an eine Dateiablage. Die Benutzer von Windows-Clients können ihre Benutzerprofile und Logon-Scripts ebenso von einem Samba-Server beziehen, wie ihre Heimat- oder Gruppenverzeichnisse. Die ausführbaren Programme (.exe) können auch auf einem Samba-Server abgelegt (und von dort gestartet) werden, wie Access Datenbankdateien oder andere durch Lock-Mechanismen für den Mehrbenutzerbetrieb vorgesehene Dateien.

Im Unterschied zu einem NT-Server verwendet Samba als Netzwerkprotokoll ausschließlich TCP/ IP. Für die auf den Protokollen SPX/ IPX (Novell) und Appletalk (Apple) basierenden Dienste existieren andere Open Source Server (Mars und Netatalk), die in einer heterogenen Netzwerkumgebung das Arbeiten auf einem gemeinsamen Datenbestand möglich machen. Eine auf dem alten Net-

BEUI basierende Implementierung von SMB wird von Samba nicht angeboten. Auch NetBIOS über IPX wird nicht unterstützt.

Die clientseitig üblichen Werkzeuge zur Bearbeitung/ Verwaltung der Dateien auf der Dateiablage stehen weiterhin zur Verfügung. Insbesondere können der Explorer und der Datei Manager sowie cacls, xcacls etc. weiter verwendet werden. Auch der Benutzermanager kann mit Samba 3.0 weiter genutzt werden. Der Einsatz des Servermanagers ist im Prinzip möglich, eignet sich aber wegen der damit verbundenen Abkehr von der transparenten Serverkonfiguration (smb.conf) wenig.

Die Herstellung der Verbindungen zu den Freigaben lässt sich ohne Änderung weiterhin durch Logon-Scripts automatisiert oder durch Browsen der Netzwerkumgebung interaktiv durchführen.

Das Rechtesystem von Samba und Linux ermöglicht es, privilegierten Prozessen wie zum Beispiel einem Virenscanner auf dem Server lokal Zugang zu allen Dateien in den Heimatverzeichnissen der Benutzer zu gewähren, und gleichzeitig den Zugriff über das entsprechende Netzlaufwerk ausschließlich dem Benutzer selbst zu gestatten.

Auch in Umgebungen mit Windows Terminalservern lässt sich der Samba-Server zur Dateiablage und zur Authentifizierung verwenden. Allerdings werden die für Terminalserver spezifischen SAM-Objekterweiterungen von Samba nicht unterstützt.

Die Behandlung von Dateisperren (Locking sowohl auf Dateiebene als auch im Byte-Range) wird von Samba exakt wie vom NT-Server geleistet. Das heißt, sowohl die kooperative Bearbeitung von Dateien als auch die Benutzung von dateibasierenden Datenbanken ist mit Samba ebenso wie mit einem NT-Server möglich.

Die Quotierung von Plattenplatz (wie von anderen Systemressourcen) wird durch das Linux-Betriebssystem angeboten und steht damit auch für die vom Samba-Server angebotene Dateiablage zur Verfügung.

Für Datensicherung und Versionierung/ Archivierung stehen unter Linux verschiene Open Source Tools zur Verfügung. Zusätzlich lassen sich Linux-Server problemlos in die Sicherungskonzepte der meisten marktüblichen Produkte einbinden[1].

Eine Hochverfügbarkeit, wie s*i*e unter NT durch Clustering mit der Enterprise Edition erreicht wird, lässt sich mit Samba ebenfalls auf Basis von shared SCSI oder SAN mit IP Failover realisieren.

[1] Im Vorfeld ist jedoch eine genaue Evaluierung der Produkte vorzunehmen, da es auch Produkte gibt die Probleme mit der Sicherung von ACLs aufweisen. Dieses Problem gilt z.B. beim Einsatz von NetBackup (Veritas) beim Sichern XFS ACLs. Ext3 ACLs werden in diesem Produkt allerdings unterstützt.

Im Vergleich zu einigen Machbarkeitsstudien[1] aus den letzten Jahren haben sich die funktionalen Einschränkungen bezüglich des Samba-Einsatzes stark reduziert. Mit der Samba Version 3.0 ist es möglich, zwischen Master- und Ressourcendomänen Vertrauensstellungen aufzubauen und das Windows NT Domänenkonzept zu realisieren. Die Version 3.0 eröffnet auch die Möglichkeit, den Windows Benutzermanager zur Benutzer-Administration einzusetzen, beispielsweise können so neue Benutzer angelegt werden. Eine Möglichkeit zur Replikation zwischen Windows-Domänen-Controler und Samba-Domänen-Controller besteht weiterhin nicht, innerhalb einer Domäne können somit nur reine Windows bzw. Samba-Domänen-Controller eingesetzt werden. Falls die Integration von Windows-Serverdiensten in einer Samba-Domäne notwendig ist, können diese als Mitgliedserver integriert werden. Die SAM-Replikation in einer reinen Samba-Domänen-Controller Umgebung ist problemlos durch die Kombination von Samba und OpenLDAP möglich. Für die Funktionalität der SAM-Replikation ist die Kombination von Samba und OpenLDAP unverzichtbar. OpenLDAP dient Samba zur Verwaltung der Gruppen und Benutzern und bietet auch die notwendigen Replikationsmechanismen.

Vergleich der Dateisysteme

Tab. 12: Vergleich der Dateisysteme

	NTFS	XFS	EXT3	ReiserFS
Länge der Dateinamen	256	256	256	256
Zeichensatz für Dateinamen	Unicode	ISO-Latin	ISO-Latin	ISO-Latin
Darstellung von Groß-/ Kleinschreibung	X	X	X	X
Unterscheidung von Groß-/ Kleinschreibung		X	X	X
Disk Quotas	X	X	X	X[2]
Verschlüsselung	EFS	X[3]	X[4]	X[5]
Kompression	X	(X)[6]	(X)[7]	(X)[8]

1 Insbesondere eine Machbarkeitsstudie für ein Bundesministerium, aus dem Jahre 2001

2 In einigen Versionen nicht zuverlässig einsetzbar

3 Über Betriebssystemmittel (crypto-api/loopback und cfs/rpc) für ganze Dateisysteme oder Teilbäume realisierbar

4 S. Verschlüsselung in XFS

5 S. Verschlüsselung in XFS

6 Mittels loopback ist eine Kompression auf Dateisystem-Ebene möglich.

7 In der Inode eines ext2/ext3-Dateisystems ist ein Attribut für Kompression vorgesehen. Bis Kernel 2.2 waren Patches für ein Projekt e2compr verfügbar, die darauf basierend eine transparente Dateikompression mit unterschiedlichen Algorithmen erlaubten. Seit Kernel 2.4 wird dieses Projekt nicht mehr fortgeführt, da der Bedarf an Kompression faktisch nicht mehr gegeben ist. Mittels loopback ist jedoch eine Kompression auf Dateisystem-Ebene möglich.

8 S. Kompression in XFS

	NTFS	XFS	EXT3	ReiserFS
Maximale Dateigröße	2 Terra	16/ 64 Terra[1]	4 Terra[2]	16/ 64 Terra[3]
Maximale Pfadlänge	Unbe-grenzt.	Unbe-grenzt	Unbe-grenzt	Unbe-grenzt
Änderungsjournal	X			
Journaling	X	X	X	X
ACL	DACLs	POSIX ACLs über extended attributes	POSIX ACLs über extended attributes ab der kommen-den Ker-nelversion	
Auditing	SACLs	(X)[4]	(X)[5]	(X)[6]

Lokale Dateiablage bei Client-Migration

Im Rahmen der Betrachtungen zur Dateiablage wird davon ausgegangen, dass auf den Clients keine Nutzdaten lokal gespeichert werden. Bei einer eventuellen Migration wird ein neues System mit identischer Funktionalität aufgesetzt, ohne dass Daten vom alten Client übernommen werden.

Wenn eine große Zahl identisch ausgestatteter Clients zu migrieren ist, kommt ein festplattenloser Betrieb auf einem reinen Netzdateisystem in Frage. Dieser Spezialfall von netzwerkzentraler Dateiablage bietet insbesondere bei der Administration große Vorteile: Änderungen an der Client-Konfiguration werden nur ein einziges Mal auf dem Server ausgeführt und sind automatisch auf allen damit arbeitenden Clients wirksam. Für die Auswahl des Serverdienstes auf dem ein „diskless Client“ aufsetzt, müssen prinzipiell die gleichen Überlegungen angestellt werden, wie bei der Auswahl des Serversystems für die zentrale Dateiablage allgemein.

---

1 Je nachdem, ob 32 oder 64 bittig; theoretisches Maximum bei 9 Exabyte; in Linux Kernel 2.4 auf 2 Terra beschränkt durch maximale Dateisystem Größe

2 Je nachdem, ob 32 oder 64 bittig; in Linux Kernel 2.4 auf 2 Terra beschränkt durch maximale Dateisystem Größe

3 Je nachdem, ob 32 oder 64 bittig; theoretisches Maximum bei 1 Exabyte; in Linux Kernel 2.4 auf 2 Terra beschränkt durch maximale Dateisystem Größe

4 Auditing wurde unter Linux mehrmals entwickelt. Ein frühes Projekt-Audit wurde seit Anfang 2000 nicht mehr weitergepflegt. Das Projekt grsecurity implementiert ein prozessbasiertes ACL-System im Kernel (http://www.grsecurity.net/). Darüber ist ein komplettes Auditing von Dateien und anderen Systemaktivitäten möglich.

5 S. Auditing in XFS

6 S. Auditing in XFS

Zugriffssteuerung: Abbildung der Rechteprofile von Windows auf POSIX ACL

Die Regelung der Zugriffsrechte auf Verzeichnisse und Dateien durch einen Samba-Server entspricht im Wesentlichen den von NT bekannten Prinzipien. Auch unter Samba werden einzelne Verzeichnisse aus dem Dateisystem des Servers als Shares im Netzwerk zur Verfügung gestellt. Die Details der Zugriffsregelung werden auf Grundlage der im serverseitig verwendeten Dateisystem festgelegten Rechte für einen jeweils individuell beim Samba-Server authentifizierten Benutzer ermittelt. Die Autorisierung ist also ein Zusammenspiel zwischen dem Samba-Server und dem Betriebs- bzw. dem Dateisystem.

Shares (Freigaben) und ihre serverseitigen Eigenschaften wie Verzeichnispfad, Gewährung von anonymem Zugriff und allgemeiner Schreibschutz sind unter Samba typischerweise in einer für jede Serverinstanz eindeutigen Konfigurationsdatei geregelt und ausgewiesen. Die Bearbeitung dieser Konfigurationsdatei kann auch (nach entsprechender Authentifizierung/ Autorisierung mit verschlüsseltem Protokoll HTTPS) über ein Web-Fontend durchgeführt werden.

Zugriffsrechte auf Verzeichnisse und Dateien werden bei allen Betriebssystemen in der funktionalen Betriebssystemkomponente des Dateisystems abgehandelt. Während es beim FAT Dateisystem von DOS und älteren Windows-Versionen noch kein Eigentümerkonzept für Dateien gab, werden unter UNIX seit jeher und unter Windows mit dem NT Dateisystem (NTFS) Eigentümer und Benutzergruppen für Dateien unterschieden. Welche Benutzer mit welchen Verzeichnissen und Dateien auf welche Art umgehen dürfen, wird vom Dateisystem über eine Liste von Zugriffsrechten, so genannte Access Control Lists gesteuert.

Unter UNIX sind für alle Dateien mindestens die Zugriffsrechte zum Lesen, Schreiben und Ausführen für den Eigentümer, eine Eigentümergruppe und alle übrigen Systembenutzer definiert. Zusätzliche Einschränkungen oder die Gewährung von Rechten für andere Benutzer oder Benutzergruppen können bei einigen UNIX/ Linux Dateisystemen über erweiterte Attribute und POSIX Access Control Lists realisiert werden.

Samba als Fileserver hält seine Daten in einem UNIX Dateisystem und greift mit den effektiven Rechten des jeweils für einen Zugriff authentifizierten Benutzers auf die Daten zu. Der Samba-Server kann theoretisch zusätzliche Beschränkungen für den Zugriff auflegen, über die im Dateisystem festgelegten Beschränkungen kann sich der Server aber in keinem Fall hinwegsetzen. Sowohl bei der Übermittlung der bestehenden Zugriffsrechte vom Server an den Client als auch bei der Manifestierung von clientseitig initiierten Änderungen verwendet der Samba-Server den Rechtekanon des Dateisystems, in dem er die Benutzerdaten ablegt und verwaltet. Deshalb muss bei einer Migration das Rechtemodell von Windows in die UNIX-Welt abgebildet werden. Im Folgenden wird beschrieben, wie diese Abbildung vor sich geht und welche Besonderheiten und Einschränkungen dabei zu beachten sind. Die Autoren des Leitfadens gehen dabei davon aus, dass unter Linux ein Dateisystem mit Unterstützung für POSIX-ACL ver-

wendet wird. Zurzeit sind das die Dateisysteme XFS, JFS und mit Patch EXT2 und EXT3.

Abbildung der NTFS-ACL in das Rechtesystem von Linux

Bei der Abbildung der Windows ACL auf die POSIX ACL von Linux wird das Rechtesystem so weit reduziert, dass das Bild im Wesentlichen der einfachen Darstellung in den Sicherheitseinstellungen entspricht.

POSIX ACL kennen nur Rechte zum *Lesen*, *Schreiben* und *Ausführen*. Verschiedene Arten zu unterscheiden wie *Daten schreiben*, *Daten anhängen*, *Attribute schreiben* und *Erweiterte Attribute schreiben* gibt es bei den POSIX ACL nicht. Bei der Abbildung des Rechtesystems von Windows über Samba nach UNIX können deshalb immer nur komplette Aggregationen der Windows Rechte im UNIX Dateisystem abgebildet werden. Umgekehrt kann der Samba-Server auch nur solche Rechte-Aggregationen an den Windows-Client melden.

Tab. 13: POSIX-Berechtigungen und Windows-Aggregationen

		POSIX Berechtigungen		
		Lesen	**Schreiben**	**Ausführen**
WINDOWS	Ordner durchsuchen / Datei ausführen			
	Ordner auflisten / Daten lesen	X		
	Attribute lesen	X		(X)[1]
	Erweiterte Attribute lesen	X		
	Dateien erstellen / Daten schreiben		X	
	Ordner erstellen / Daten anhängen		X	
	Attribute schreiben		X	
	Erweiterte Attribute schreiben		X	
	Unterordner/ Dateien löschen			
	Löschen			
	Berechtigungen lesen	X	X	X
	Berechtigungen ändern			
	Besitz übernehmen			

Auf der Anwenderseite können mit den Windows-Dialogen durch Kombination der passenden NTFS-Berechtigungen die entsprechenden Kombinationen der POSIX-Berechtigungen erzeugt werden. Dabei ist zu beachten, dass das Setzen *einer* zusätzlichen NTFS-Berechtigung aus der Windows-Liste zum Setzen *aller*

[1] Wird angezeigt, darf aber nicht gesetzt werden, sonst wird das gesamte Aggregat Lesen aktiviert

Berechtigungen des POSIX-Aggregats führt, zu dem das so gesetzte NTFS-Recht gehört. Wenn beispielsweise für eine Datei, auf die bisher nur lesender Zugriff möglich war, in dem Dialog *Berechtigungseintrag* die Berechtigung *Attribute schreiben* gesetzt wird, so erweitert der Samba-Server automatisch die Rechte für *Erweiterte Attribute schreiben*, *Daten schreiben* und *Daten anhängen*. Nachdem also der Dialog mit *OK* beendet wurde, erscheint sofort beim nächsten Öffnen des Dialogfensters die neue wesentlich erweiterte Rechteausstattung. Das Vorteilhafte daran ist, dass dieses Verhalten des Samba-Servers Fehlinterpretationen der einfachen Rechtedarstellung nicht zulässt.

In der vereinfachten Darstellung der Sicherheitseinstellungen ist das Bild konsistent. Hier können die Berechtigungen *Lesen* und *Schreiben* einzeln und gemeinsam gesetzt werden sowie jeweils in Kombination mit *Lesen/Ausführen*. Letztere Sammelberechtigung kann nicht alleine gesetzt werden.

Die NTFS-Berechtigungen *Unterordner/Dateien löschen*, *Löschen*, *Berechtigungen ändern* und *Besitzrechte übernehmen* sind unter POSIX ACLs nicht abbildbar und führen beim Setzen daher zu keinerlei Resultat auf dem Samba-Server (in der Tabelle abgegraut dargestellt). Bei *Vollzugriff*, also den kompletten Lese-, Schreib- und Ausführberechtigungen sind sie allerdings auch als gesetzt markiert.

Tab. 14: POSIX- und Windowsberechtigungen

		POSIX Berechtigungen				
		Lesen	**Schreiben**	**Lesen und Ausführen**	**Lesen und Schreiben**	**Lesen, Schreiben und Ausführen**
WINDOWS	Vollzugriff					X
	Ändern					X
	Lesen/ Ausführen			X		X
	Ordnerinhalt auflisten (nur für Ordner)			X (nur für Ordner)		X (nur für Ordner)
	Lesen	X		X	X	X
	Schreiben		X			

Abbildung der Vererbungsfunktion

Die POSIX-ACL Implementation verfügt lediglich über passive Vererbung. Eine aktive Vererbung wie im NTFS ist nicht abbildbar. Samba bietet jedoch die Möglichkeit auf einzelnen Shares die Vererbung von ACLs zu aktivieren. Hierbei werden allerdings nur die Default-ACLs vererbt, nicht die „normalen“ Datei ACLs und die Vererbung gilt nur für neu erstellte Dateien.

Abbildung des Attributsystems

Die Attribute, die unter Unix nicht vorhanden sind, können auf verschiedene Weise abgebildet werden. Zunächst wird das Flag *Schreibgeschützt* nicht wirklich benötigt, weil es im normalen Berechtigungssystem bereits enthalten ist. Es wird daher für Dateien und Verzeichnisse ohne Schreibberechtigung automatisch angezeigt. Die Flags *Archiv*, *Versteckt* und *System* können durch das nicht verwendete *Execute* Bit des Unix-Dateisystems abgebildet werden und sind daher vorhanden. Die Attribute *Komprimiert* und *Verschlüsselt* sind nicht abbildbar. Sie können allerdings über spezielle Dienste unter Unix zur Verfügung gestellt werden.

Abbildung der Überwachungsfunktionen

Das Auditing-System ist fest in Windows integriert. Es ist unter Unix mit anderen Mechanismen nachbildbar. Für den Samba-Server lässt sich das Auditing über ein VFS-Modul realisieren. Damit werden dann die Zugriffe auf Dateien und Verzeichnisse durch den Samba-Server protokolliert. Auf der Ebene des Dateisystems hat ein Auditing in dieser Form bislang nicht Einzug in den Linux-Kernel gefunden, obwohl mehrere Anläufe für eine Implementierung versucht wurden und in den vorhandenen Strukturen für erweiterte Attribute bei den Linux-Dateisystemen entsprechende Voraussetzungen vorhanden sind. In der Praxis scheint diese Funktionalität jedoch so wenig Bedeutung zu haben, dass alle Versuche bisher aus Mangel an Interesse wieder eingeschlafen sind.

Zusammenfassung der wichtigsten Folgen bei Verwendung von Samba mit POSIX ACLs

Für Schreiben als abstraktes Recht gilt:

- zwischen Daten schreiben und anhängen wird nicht unterschieden
- bei Ordnern wird ebenso nicht zwischen dem Erstellen von Ordnern und dem Erstellen von Dateien unterschieden
- das Schreiben von Ordnern bzw. Dateien und Attributen wird nicht unterschieden

Für das Lesen als abstraktes Recht gilt:

- das Lesen von Ordnern bzw. Dateien und von Attributen wird nicht unterschieden

Prinzipiell gilt, dass das Lesen von Berechtigungen immer erlaubt ist. Generell sind weder Überwachung noch Vererbung implementiert.

Benutzergruppen und Zugriffsrechte

Insbesondere bei den von Arbeitsgruppen gemeinsam genutzten Freigaben spielt die Vergabe von Zugriffsrechten an Gruppen eine herausragende Rolle. Unter NT werden (Server-)lokale und globale Gruppen unterschieden. Lokale Gruppen können als Alias-Definitionen verstanden werden, die auf eine oder mehr globale Gruppen verweisen. Auf diese Weise können lokale Gruppen mehrere globale

Gruppen enthalten. Unter Samba (wie unter UNIX/ Linux allgemein) ist eine Verschachtelung von Gruppen nicht möglich. Mit Samba lassen sich lediglich alle UNIX-Gruppen 1:1 als globale Gruppen für Windows Clients und Member-Server darstellen.

Diese globalen Gruppen können auf Windows-Member-Servern natürlich wieder in lokale Gruppen eingehen. Damit stehen auf solchen Servern weiterhin die Modelle B-G-L-R und B-G-R zur Verfügung, wie sie im Abschnitt 3.2.2.4 beschrieben wurden.

Die Einführung eines Konzepts von lokalen Gruppen auch für Linux-Server ist bislang nicht geplant, so dass hier typischerweise nur das Modell B-G-R zum Einsatz kommt. Eine äquivalente Funktionalität lässt sich mit entsprechender Business-Logik in einer LDAP-basierten Gruppenverwaltung realisieren.

Abschätzung der Auswirkungen für die Benutzer

Bei der Abbildung der Windows-ACL auf die POSIX-ACL geht die feine Granularität verloren, in der die Rechte unter Windows modifiziert werden können. Allerdings werden in der Praxis ganz überwiegend nur die wesentlich einfacheren Sammelberechtigungen der einfachen Sicherheitseinstellungen verwendet.

Die weiteren, abgestuften Berechtigungen kommen nur in Einzelfällen zur Anwendung. Besonders die Unterscheidung zwischen den Attribut- und den Dateirechten wird äußerst selten verwendet.

Auch die Berechtigung *Daten anhängen* wird nur in wenigen Fällen sinnvoll nutzbar sein. Diese Berechtigung kann bei Verwendung eines Extended 2/3 Dateisystems unter Linux auch als erweitertes Attribut auf der Kommandozeile für ausgewählte Dateien gesetzt werden.

Durch die konsistente Abbildung des einfacheren Rechtemodells von den POSIX ACL wird das Bild der einfachen Sicherheitseinstellungen für den durchschnittlichen Benutzer zuverlässiger.

Bestimmte Funktionen, wie Vererbung und Auditing, können nicht nachgebildet werden.

3.2.4 Fortführende Migration

3.2.4.1 Windows 2000

In diesem Abschnitt wird auf den Nachfolger von Windows NT4, Windows 2000, hinsichtlich des Themas „File Service“ eingegangen.

Funktionszuwachs

Mit Windows 2000 gehen hinsichtlich der File Services einige Neuerungen einher. Als Stichworte seien hier genannt:

- Dateisystem NTFS5
- HSM-API

- Vererbung
- Verschlüsselung (EFS)
- SMB over Native IP
- Dynamische Datenträgerverwaltung
- Defragmentierung
- Gruppenverschachtelung
- Remote Storage
- Indexing Service
- Distributed Link Tracking
- DFS
- Offline Folder
- Folder Redirection.

Im Folgenden wird auf diese Themen näher eingegangen.

Dateisystem NTFS5

Das Dateisystem NTFS5 bietet insgesamt folgende Verbesserungen:

Erstmals ist es möglich, die Zugriffsrechte durch Vererbung zu verwalten. Das bedeutet, dass durch das Setzen von Rechten auf übergeordneten Ordnern diese auf untergeordneten Ordnern und Dateien wirksam werden, ohne das Durchschreiben (Einbrennen) durchführen zu müssen. Die Nachteile des Durchschreibens (Lastproblem, Löschen von speziellen Rechten in Unterordnern) entfallen somit.

NTFS5 verfügt über ein Change Journal, in dem die Änderungen protokolliert werden.

NTFS5 formatierte Datenträger verfügen über einen versteckten Ordner namens „System Volume Information“, auf den nur das Betriebssystem Zugriff hat und in dem die zusätzlichen Funktionen verwaltet werden.

NTFS5 bietet ein so genanntes HSM-API (Programmierschnittstelle Hierarchical Storage Management), das von Drittherstellern genutzt werden kann.

NTFS5 bietet die Möglichkeit, Daten zu verschlüsseln. Das Encrypting File System (EFS) ermöglicht es Benutzern, Daten vor dem Lesen des Inhalts durch Dritte (auch der Administratoren) zu schützen. In Unternehmensnetzwerken ist hierzu eine PKI (Public Key Infrastructure) notwendig.

Die Integration von Quotas im Dateisystem bleibt vorhanden, unterliegt aber weiterhin den Beschränkungen von NT4.

Protokolle

Windows 2000 unterstützt nach wie vor die o. g. Protokolle. Erstmalig ist es bei Windows 2000 möglich, die Kommunikation über NetBIOS abzuschalten. Für die File Services bedeutet dies, dass das „Direct Hosting of SMB Over TCP/ IP“ bei der Kommunikation über den Port 445 erfolgt.

Datenträgerverwaltung

Windows 2000 bietet ferner die Möglichkeit, physische Festplatten in das System einzubinden, ohne Laufwerksbuchstaben vergeben zu müssen. Diese dynamischen Datenträger können als Ordner in traditionellen Datenträgern eingebunden und bereitgestellt werden. Windows 2000 liefert erstmals ein Werkzeug zum defragmentieren von Datenträgern.

Änderungen bzgl. Zugriffsteuerung

Unter Windows 2000 Active Directory kommen weitaus mehr Zugriffssteuerungen in Frage, da *mehr* Gruppentypen *stärker* verschachtelt werden können. Diese Gruppenverschachtelungen sind nur dann möglich, wenn ein Active Directory im „Native Mode“ eingesetzt wird. Im „Native Mode“ sind die neuen Gruppentypen „Domain Local“ und „Universal“ verfügbar. Die folgende Tabelle zeigt die Verschachtelungsmöglichkeiten.

Tab. 15: Gruppentypen

Gruppentyp	kann folgende Mitglieder haben	kann Mitglied sein von
Globale Gruppe	Benutzer und globale Gruppen derselben Domäne	globale Gruppen derselben Domäne Universelle und Domänenlokale Gruppen jeder Domäne
Domänenlokale Gruppe	Benutzer, universelle und globale Gruppe jeder Domäne Domänenlokale Gruppen derselben Domäne	Domänenlokale Gruppen derselben Domäne
Universelle Gruppen	Benutzer, globale und universelle Gruppen jeder Domäne	Domänenlokale oder universelle Gruppen jeder Domäne

Neben diesen neuen Gruppentypen muss in Umgebungen mit Active Directory und Exchange 2000 zwischen Sicherheits- und Verteilergruppen unterschieden werden. Bei den Verteilergruppen existieren Exchange-Umgebungen, sie lassen aber keinerlei Steuerung hinsichtlich File Services zu.

Remote Storage

Remote Storage ist ein neuer Dienst unter Windows 2000 und ermöglicht die Auslagerung von lange nicht genutzten Dateien auf Bandlaufwerke im Sinne eines HSM (Hierarchical Storage Management).

Indexing Service

Der Indexing Service kann optional für Dateiordner eingeschaltet werden, um die dort gespeicherten Dateien zu indizieren. Der erstellte Index ermöglicht eine schnellere Suche nach bestimmten Inhalten. Mit dem Indexdienst können folgende Typen von Dokumenten in verschiedenen Sprachen indiziert werden:

- HTML
- Text
- Microsoft Office 95 oder höher
- Internet Mail und News
- Alle anderen Dokumente, für die ein Dokumentfilter verfügbar ist.

Distributed Link Tracking

Windows 2000 File Server ermöglichen es, dass Anwendungen, die das Verknüpfen und Einbetten von Objekten unterstützen, so programmiert werden können, dass beim Verschieben der verknüpften Objekte Informationen über den aktuellen Speicherort vom Dateisystem abgerufen werden können. Damit bleibt die fehlerfreie Nutzung erhalten.

Distributed File System

Das Distributed File System (DFS) konnte bereits unter Windows NT 4 durch zusätzliche Installationen auf Server und Client bereitgestellt werden. Bei Windows 2000 sind diese Funktionalitäten sowohl auf Client- als auch Serverseite standardmäßig integriert und zusätzlich erweitert worden. DFS ermöglicht, dass Freigaben von Ordner, die auf verschiedenen Servern verteilt sind, dem Client als Unterordner einer einzelnen Freigabe dargestellt werden. Damit wird eine Einsparung von Laufwerksbuchstaben hinsichtlich der Netzlaufwerke, die dem Anwender zugeordnet werden sollen, erzielt. In Windows 2000 wurde DFS um die Integration von FRS (File Replication Service) dahingehend erweitert, dass die verknüpften Freigaben und deren Inhalte auf weitere Freigaben und anderen File Servern repliziert werden. Fällt ein Server und somit dessen Freigabe aus, dann stehen dem Client die Repliken zur Verfügung, ohne neue Netzwerkverbindungen aufbauen zu müssen. In Windows 2000 können die Informationen über den DFS-Baum im Active Directory gespeichert und repliziert werden. Dadurch verfügt der Client nahezu jederzeit über die benötigten Verbindungsinformationen.

Verbindungsherstellung

Dem Anwender kann die Suche nach Freigaben erleichtert werden, indem die Freigaben im Active Directory veröffentlicht werden.

Offline Folder und Folder Redirection

Die Funktionalitäten „Offline Folder“ und „Folder Redirection“ sind primär keine Eigenschaften der File Services von Windows 2000, sondern Funktionalitäten des Client (z.B. Windows 2000/Professional). Sie seien an dieser Stelle dennoch

erwähnt, weil sie hinsichtlich der Datenhaltung prinzipiell relevant sind und mit dem File Server zusammenarbeiten müssen. Offline Folder stellen quasi den Nachfolger des „Aktenkoffers“ der bisherigen Windows Versionen dar. Anwender, die z.B. über ein Notebook verfügen, können Ordner und Dateien, die normalerweise auf File Servern gespeichert werden, ohne Netzwerkverbindung bearbeiten. Sobald eine Verbindung zum File Server besteht, werden diese Daten wieder abgeglichen (repliziert). Aufgrund dieser Replikation sind auf beiden Seiten (Client und Server) die jeweiligen Dateieigenschaften von großer Bedeutung, um einen fehlerfreien Abgleich zu ermöglichen.

Mit der Funktionalität Folder Redirection trägt Windows 2000 dem Umstand Rechnung, dass die Größe von Benutzerprofilen auf Arbeitsplatzsystemen im laufenden Betrieb stark anwachsen kann. Dies geschieht z.B. dann, wenn der Anwender dort unter „Eigene Dateien“ seine Dateien speichert, die eigentlich auf File Servern abgelegt werden sollen. Unter Windows 2000 ist es möglich, die Systemordner des Benutzprofils („Eigene Dateien“, „Anwendungsdaten“) auf einen Netzwerkpfad zu „verbiegen“. Diese Ordner erscheinen dem Anwender transparent als lokale Ordner. Durch das Verschieben der Ordner auf File Server muss beachtet werden, dass die Zugriffsrechte gewahrt bleiben.

Datensicherung

Das Bordmittel NTBACKUP ist so modifiziert worden, dass nun Datensicherungen auf Laufwerke (lokal oder Netz) durchgeführt werden können. So können lokale Bandlaufwerke besser vermieden werden.

Versionsnachfolger

In der Produktnachfolge sind folgende Pfade zu beachten:

- Windows 2000 Server folgt Windows NT 4 Server
- Windows 2000 Advanced Server folgt Windows NT 4 Server Enterprise Edition (siehe Cluster Services).

Mit Windows 2000 DataCenter Server ist erstmals ein Betriebssystem von Microsoft verfügbar, dass nur in Kombination mit spezieller Hardware und nur von wenigen Herstellern bezogen werden kann. Diese Plattform adressiert sehr spezielle Verfügbarkeits- und/oder Lastszenarien. Sie wird in diesem Leitfaden nicht weiter betrachtet.

Network Attached Storage (NAS)

Einige Hardware-Hersteller haben in Zusammenarbeit mit Microsoft so genannte NAS-Systeme auf Basis Windows 2000 Server konzipiert. Diese Systeme sind auf File Services dediziert und I/O optimiert.

Aus der Praxis

Im Folgenden werden einige Anmerkungen zu den obigen technischen Neuerungen gemacht:

- Die Verbreitung von EFS reduziert sich in der Regel auf den Einsatz bei mobilen Computern, auf denen Daten vor Verletzung der Vertraulichkeit geschützt werden müssen. Der Einsatz von EFS wird zum einen durch die notwendige PKI (auch wenn Windows 2000 Active Directory diese mit anbietet) behindert und zum anderen angesichts der fehlenden Unterstützung für Zugriffsmechanismen auf Gruppenbasis (zum Zwecke der gruppenspezifischen Dateiablage auf File Servern) oftmals als nicht zielführend eingestuft.
- Das Abschalten der Kommunikation über die Schnittstelle NetBIOS ist nicht zwingend und wird in der Regel aufgrund der benötigten Abwärtskompatibilität aufgeschoben.
- Der Einsatz der bisherigen Werkzeuge zum Datei- und Zugriffsmanagement ist aufgrund des neuen Dateisystems zu beachten. Beispielsweise kann die Vererbung durch einen NT 4 Explorer nicht sinnvoll dargestellt werden.
- Der Einsatz von Windows 2000 hinsichtlich der weiteren Verwendung von Bestandshardware, die bereits unter NT 4 im Einsatz war, ist im Einzelfall zu prüfen. In der Mehrheit der Fälle ist damit zu rechnen, dass neue Hardware beschafft werden muss.

3.2.4.2 Windows 2003 Server

In diesem Abschnitt wird auf den Nachfolger von Windows 2000, Windows 2003 Server (ehemals „.NET Server“), hinsichtlich des Themas „File Service“ eingegangen.

Im Folgenden wird kurz beschrieben, welches die einschneidenden Neuerungen dieser Version sein werden:

- Windows 2003 Server wird das erste Betriebssystem von Microsoft sein, das auch in einer 64bit Architektur verfügbar sein wird.
- Die offizielle Unterstützung von SAN (Storage Area Networks) wird dahingehend verbessert, dass nun auch das Booten von Festplatten im SAN möglich wird.
- Das EFS ermöglicht nun auch den Zugriff für mehrere Anwender auf eine Dateiressource. Gruppen bleiben weiterhin unberücksichtigt.

Neu wird die Funktionalität Volume Shadow sein: Sie beinhaltet zum einen, dass die Datei- und Ordnerstruktur zu einem bestimmten Zeitpunkt als statisch betrachtet werden kann, so dass beispielsweise eine Datensicherung erfolgen kann, ohne auf offene Dateien Rücksicht nehmen zu müssen. Zum anderen ergeben sich die folgenden Möglichkeiten: Anwender werden in die Lage versetzt, versehentlich gelöschte Dateien aus einem „Snapshot“ wiederherzustellen, ohne extra eine Wiederherstellung beantragen zu müssen. Die Wiederherstellung (System Recovery) wird für die Administration vereinfacht.

3.3 Druckdienst

3.3.1 Überblick

Die nachfolgenden technischen Detailbetrachtungen kommen zu dem Ergebnis:

Unter Linux ist CUPS der de-facto Standard aller großen Distributionen (Suse, Debian, RedHat, usw.). CUPS ist das System der Wahl, sowohl in homogenen Linux-Systemlandschaften als auch in heterogenen Systemlandschaften mit windowsbasierten Clientsystemen. Mit windowsbasierten Clientsystemen wird in der Kombination von CUPS und Samba ein vollwertiges Drucksystem geboten.

Die Funktionalität von CUPS ist durch die Implementierung von IPP (Internet Printing Protocol) plattformübergreifend angelegt. CUPS unterstützt aber auch alle weiteren relevanten Druckprotokolle wie LPR/LPD, Socket/AppSocket, SMB/CIFS und MS-RPC (in Kombination mit Samba). Die CUPS/Samba-Kombination unterstützt auch einen automatisierten Treiber-Download zu den Windows-Clients.

Darüber hinaus bietet CUPS verschiedene Möglichkeiten, Datensicherheit auch beim Drucken zu gewährleisten. Hierzu gehören die SSL-verschlüsselte Übertragung bei IPP-Verwendung oder auch die Benutzer-Authentifizierung im Zusammenspiel mit Samba. Dies hat auch im Hinblick auf das Accounting von Druckerzugängen große Vorteile.

Im Vorfeld einer Migration sollte in jedem Fall die Unterstützung der eingesetzten Druckermodelle überprüft werden. Dies gilt insbesondere, wenn die Druckaufbereitung komplett auf den Print-Servern erfolgen soll, da in wenigen, vereinzelten Fällen eine Unterstützung nicht gegeben sein kann.

Auch bei einer clientseitigen fortführenden Migration können Windows 2000 Clients über CUPS-Server drucken, da Windows 2000 IPP-Unterstützung bietet.

3.3.2 Einleitung

Das Thema „Drucken“ wird in der IT-Welt oft stiefmütterlich behandelt. Das gilt für alle Betriebssystem-Umgebungen, für die Windows- oder die Unix-/ Linux-Welt gleichermaßen. Druckprobleme verursachen häufig die höchsten Reibungsverluste. Ein großer Teil der Administratoren-Zeit wird für die Lösung alltäglicher Druckprobleme verwendet. Andererseits ist Drucken in vielen Fällen eine „mission critical“ Anwendung, deren Ausfall finanzielle Verluste und den Verantwortlichen viel Kopfzerbrechen bereiten kann.

Ein gewisser „Wildwuchs in der Infrastruktur“ hinsichtlich der Druckdienste ist weit verbreitet. „Gewachsene Strukturen“ haben an vielen Stellen zu allerlei Unverträglichkeiten geführt: so herrscht oft ein Durcheinander von Seitenbeschreibungssprachen (PostScript, PCL, PreScribe, ESC/P, PDF...) vor. Die oft „unfriedliche“ Koexistenz von Druck- und Netzwerkprotokollen sorgt für vielerlei Probleme: LPR/ LPD, HP JetDirect, SMB/ MS-RPC usw.

Eine Migration von Druckdiensten auf eine neue Plattform wird nicht unbedingt ein möglichst genaues 1:1-Abbild der bestehenden Verhältnisse wiedergeben können, sollte jedoch als Chance wahrgenommen werden, bestehende Schwachstellen zu beheben.

Neben den technischen Schwachstellen spielt die Kostenfrage eine ebenso entscheidende Rolle. Die wahren Kosten für organisations- (abteilungs-, betriebs-, konzern-, amts-)weites Drucken sind häufig nicht zuverlässig bekannt. Hier besteht ein enormes Einsparpotential, das in der Regel erst bewusst wird, wenn eindeutige Daten vorliegen.

Die wichtigsten Kostenfaktoren sind:

- Anzahl der Drucker
- Papierverbrauch
- Toner-/ Tintenverbrauch
- Energieverbrauch

Im Vorfeld einer Migration sollten folgende Fragestellungen geklärt werden:

- Wie viele Drucker gibt es im Haus?
- Wie viel Papier wird verbraucht?
- Wie hoch ist Toner- oder Tinten-Verbrauch? Wie viel kosten diese Positionen im Jahr?
- Wo liegen die Servicekosten (Reparatur, Wartung)?
- Wie hoch ist der Aufwand des hausinternen Help-Desks?
- Wie viel Stromkosten werden verursacht?
- Wie hoch sind die Kosten pro Druck-Seite?
- Wie verteilen sich diese Kosten auf verschiedene Druckertypen?
- Können die verfügbaren Druck-Ressourcen effizienter genutzt werden?

Die wirklichen finanziellen Kosten sind meist nur durch eine entsprechende Studie herauszufinden Es ist oft lohnend, diesen Arbeitsaufwand zu betreiben. Eine genaue Analyse der Kostenfaktoren rechnet sich in jedem Fall, da praktisch immer ein Einsparpotential realisiert werden kann, das sich binnen Jahresfrist amortisiert.

Eine Migration der Druck-Umgebung ist ein Einschnitt – in ihrem Vorfeld sollte eine entsprechende Bedarfs-Analyse stattfinden, deren Ergebnisse in die konkrete Planung des Übergangs einfließt.

3.3.3 Ausgangssituation – Drucken unter Windows NT 4

Im Folgenden wird eine Ausgangssituation beschrieben, von der angenommen wird, dass sie auf den Großteil der bestehenden Windows Umgebungen zutrifft.

Es wird davon ausgegangen, dass die bestehende Umgebung auf einem der gängigen NT Domänenmodelle basiert. Weiterhin wird angenommen, dass diese Umgebungen Print Services auf Basis von Windows NT 4 Server bereitstellen. Des Weiteren seien die Print-Server Mitglied einer NT Domäne.

Die Enterprise Edition ermöglicht einen Print Service, der durch zwei Knoten (Server) in einem Cluster realisiert wird. Der Ausfall eines Servers (eines Knotens) wird durch die Übernahme des verbleibenden Knotens kompensiert. Der Client „spürt“ die Übernahme – wenn überhaupt – innerhalb eines Sekundenzeitraums. Der Verlust der aktiven Druckaufträge ist nicht auszuschließen. Der Einsatz eines solchen Clusters erfordert die Verwendung spezieller Hardware (siehe File Services).

Als Client-Computer (Print Clients) werden berücksichtigt:

- Windows NT 4 Workstation
- Windows 9x

Als Druckergeräte werden berücksichtigt:

- Drucker mit Netzwerkkarte
- Druckerboxen mit angeschlossenen Druckern

Die folgende Abbildung zeigt eine typische Konstellation hinsichtlich der Druckumgebung:

- Manche Arbeitsplatzsysteme verfügen über einen lokal an LPT1 angeschlossenen Drucker (lokaler Drucker).
- Andere Arbeitsplatzsysteme verfügen über keine direkt angeschlossenen Drucker, sondern funktionieren lediglich über am Netzwerk angeschlossene Drucker.
- Die Mehrheit der Laserdrucker kann mit einer Netzwerkkarte ausgestattet werden. Hingegen lassen sich Tintenstrahldrucker oftmals nur durch die Verwendung einer zusätzlichen Druckerbox netzwerkfähig installieren.

Bild 7: Druckumgebung[1]

Die Abbildung zeigt die zwei prinzipiell unterschiedlichen Datenströme: Zum einen druckt der Client direkt über das Netzwerk auf den Drucker, zum anderen verwendet der Client einen „freigegebenen Drucker“ auf einem Print Server. Dieser überträgt schließlich die Daten zum Drucker.

Im Folgenden wird auf diese verschiedenen Methoden und deren Varianten eingegangen.

3.3.3.1 LPR/ LPD unter Windows NT 4.0

Die aus dem Unix-Bereich bekannte Technik LPR-LPD (Line Printer Redirector-Line Printer Daemon) hat seit Windows NT auch Einzug in die Windows Welt gefunden und wird auf NT Print-Servern als Standard zur Kommunikation zwischen Server und Druckergerät verwendet. Grundsätzlich kann diese Technik auch als Kommunikation zwischen Client und Server oder Client und Druckergerät verwendet werden. Der grundsätzliche Nachteil von LPR-LPD besteht darin, dass druckerspezifische Rückmeldungen nicht verarbeitet werden.

3.3.3.2 Andere Netzwerkports

Unter Windows NT sind von namhaften Druckerherstellern zusätzliche Ports implementiert worden, z.B.:

- LexMark Mark Vision Print Monitor (Lexmon.dll)
- Hewlett-Packard Network Port Print Monitor (Hpmon.dll).

Diese Ports sind gegenüber dem LPR-Port in der Lage, auch andere Transportprotokolle zu nutzen. Beispielsweise werden hier

- DLC
- und IPX

[1] Microsoft Windows NT 4 Resource Kit

unterstützt.

Die neuen Netzwerk-Druckports ermöglichen in der Regel eine bidirektionale Kommunikation mit den Druckern oder Druckerboxen.

3.3.3.3 Direkter Druck vom Arbeitsplatzsystem

Der direkte Druck (siehe Bild 7 Pfeil 1) erfolgt über LPR/ LPD. Zu diesem Zweck muss auf dem Arbeitsplatzsystem unter Windows NT 4 der TCP/ IP Druckserver installiert sein. Windows 9x Systeme müssen hierfür eine Software von Drittherstellern verwenden. Auf dem Arbeitsplatzsystem wird ein so genannter LPR-Port als Anschluss konfiguriert. Zu diesem Zweck muss die IP-Adresse oder ein entsprechender Hostname (DNS) des Zieldruckers eingetragen werden. Zudem erfolgt die Aufforderung, ein Druckermodell und somit den entsprechenden Druckertreiber auszuwählen. Das Betriebsystem fasst einen solchen Drucker als „lokal“ auf. In Windows NT hat die direkte Kommunikation von Client und Druckgerät wenig Verbreitung gefunden, weil die administrativen Aufwände durch die lokale Verwaltung auf den Endgeräten deutlich höher sind.

3.3.3.4 Druck via Print-Server

Der Druck vom Arbeitsplatzsystem über den Print-Server erfordert zwei Datenströme:

- die Übertragung der Daten vom Arbeitsplatzsystem zum Print-Server (siehe Bild 7 Pfeil 2a)
- die Übertragung der Daten vom Server zum Druckgerät (siehe Bild 7 Pfeil 2b).

Die Übertragung der Daten vom Server zum Druckgerät basiert in der Regel auf LPR/ LPD (siehe Direkter Druck vom Arbeitsplatzsystem).

Die Übertragung der Daten zwischen Arbeitsplatzsystem und Print-Server kann auf verschiede Weise erfolgen.

Serverseitig müssen zwei prinzipielle Vorraussetzungen erfüllt sein, damit ein Client einen bestimmten Drucker über den Server ansprechen kann:

- der Drucker ist auf dem Print-Server eingerichtet (LPR-Port, Druckertreiber)
- der Drucker ist freigegeben

Die Freigabe ermöglicht in Windows Netzwerken unter anderem, dass der Drucker „gebrowst“ werden kann, indem der entsprechende Print-Server angeklickt wird.

Die Kommunikation zwischen Arbeitsplatzsystem und Print-Server (Druckerfreigabe) kann auf drei verschiedenen Wegen erfolgen:

- Mittels des Befehls NET USE kann ein bestehender lokaler LPT-Port auf die Druckerfreigabe umgeleitet werden (Beispiel: net use LPT3 \\servername\druckerfreigabename). Diese Methode erfordert, dass der Anwender einen Drucker (Druckertreiber) auf dem LPT-Port installiert und somit lokal konfiguriert. Dies ist oftmals erforderlich, wenn aus DOS-Anwendungen heraus gedruckt werden muss. Die Druckdaten werden im RAW-Format gesendet. D.h., dass die gesendeten Daten unmittelbar vom Druckgerät verwertet werden können.
- Es kann ein neuer LPR-Port eingerichtet werden, der als Zieladresse den Print-Server und den Namen der Druckerfreigabe beinhaltet. Die Druckdaten werden ebenfalls im RAW-Format gesendet.
- Mittels der so genannten „Point & Print“-Methode kann auf dem Arbeitsplatzsystem ein Netzwerkdrucker eingerichtet werden. Vorteil dieser Methode ist, dass im Idealfall eine manuelle Konfiguration oder Druckertreiberinstallation für den Anwender entfällt. Die Druckdaten werden im EMF-Format (Enhanced Meta Format) gesendet. Sie können vom Druckgerät nicht verwertet werden, sondern müssen auf dem Print-Server aufbereitet werden. Die „Point & Print“-Methode wird im folgenden Absatz genauer beschrieben.

3.3.3.5 „Point & Print“-Methode

Microsoft setzt bei der Kommunikation von Print Client und Server auf das Protokoll RPC (Remote Procedure Call) und verwirklicht damit die so genannte Point & Print-Technologie. Diese ermöglicht es zum einen, die Druckertreiber vom Server auf den Client zu übertragen und die gerätespezifischen Einstellungen (Papierschächte, Standard-Papierformate) an den Client zu übermitteln. Zum anderen wird dadurch ein Teil des Rendering-Prozesses auf den Server verlagert, so dass der Client bei der Druckaufbereitung entlastet wird. Diese Entlastung macht sich insbesondere beim Einsatz von Terminal Servern positiv bemerkbar.

Da diese Technologie Microsoft spezifisch ist, wird im Folgenden der Prozessablauf im Detail beschrieben. Es wird davon ausgegangen, dass sowohl das Arbeitsplatzsystem als auch der Print-Server Windows NT 4 verwenden.

Fügt der Anwender einen Netzwerkdrucker seiner Druckumgebung hinzu, wird zunächst ein Treiberabgleich durchgeführt. Ein Windows NT Client lädt den Druckertreiber vom Server, wenn folgende Bedingungen gleichzeitig erfüllt sind:

- der Print-Server verwendet Windows NT
- der Print-Server verfügt über den passenden Treiber (Plattform: x86, Alpha, etc. und Version: 3.1, 3.5, 4)
- der NT Client hat keinen Treiber oder eine ältere Version als auf dem Server

Nach dem Herunterladen wird der Treiber vom Client installiert; es werden also Einträge in der lokalen Registry des Clients vorgenommen.

Prozessabfolge beim Drucken:

Die nachfolgende Abbildung (Bild 8) skizziert die Prozessabfolge, die anschließend kurz beschrieben wird.

- Schritt 1:
  Der Anwender entschließt sich, aus einer Windows Anwendung heraus ein Dokument zu drucken. Die Anwendung ruft die GDI (Graphics Device Interface) auf. Die GDI lädt den Druckertreiber des ausgewählten Druckers. Anhand der Dokumenteninformation aus der Anwendung und der Druckertreiberinformationen wird der Druckauftrag in einem ersten Durchlauf für das EMF-Format “gerendert”. Die Anwendung ruft den lokalen Spooler (Winspool.drv) auf.
- Schritt 2:
  Da der Client Windows NT verwendet, ruft der lokale Spooler (Winspool.drv) per RPC (Remote Procedure Call) den Spooler des Servers (Spoolss.exe), der seinen Router (Spoolss.dll) direkt per API aufruft. Der Router “pollt” den “Remote print provider” (Win32spl.dll) des Clients. Dieser aktiviert per RPC den Prozess Spoolss.exe auf dem Print-Server, der dann den Druckauftrag und dessen Daten über das Netzwerk entgegennimmt.
- Schritt 3:
  Der Router des Servers empfängt den Druckauftrag als EMF (Enhanced Metafile) und übergibt diesen dem Local Print Provider. Die Druckdaten in Form von EMF sind gegenüber dem Format RAW noch relativ unabhängig vom Druckgerät und in den meisten Fällen von geringerem Volumen. Der erste Teil des “Renderings” fand auf dem Client statt, der zweite Teil erfolgt nun auf dem Print-Server durch den Print Processor des Local Print Provider, der das Ergebnis auf die lokale Festplatte schreibt (spoolt).
- Schritt 4:
  Der gespoolte Auftrag wird dem Print Monitor übergeben (despooling), der nun wiederum den Portmonitor aufruft. Der Portmonitor prüft, ob und wie mit dem Druckergerät bidirektional kommuniziert werden kann und sendet die entsprechenden Daten.
- Schritt 5:
  Das Druckgerät empfängt die Daten, wandelt jede Seite in ein Bitmap und druckt sie auf Papier.

Handelt es sich unter Schritt 2 nicht um einen Windows NT Client oder einen Windows NT Client, der einen umgeleiteten lokalen Anschluss (net use LPT) verwendet, wird der Druckauftrag bereits auf dem Client vollständig gerendert

und im RAW-Format über den NetBIOS Redirector an den Print-Server Service gesendet.

Auch wenn der Client LPR verwendet, wird der Auftrag im RAW-Format via TCP/ IP zum LPD des Print-Servers gesendet.

Bild 8: Prozessabfolge bei der „Point & Print“-Methode

3.3.3.6 Netzwerkprotokolle

Die Kommunikation via LPR/ LPD erfolgt ausschließlich mit TCP/ IP.

Hingegen kann die Kommunikation zwischen Arbeitsplatzsystem und Print-Server auf verschiedenen Transportprotokollen basieren:

- TCP/ IP
- NetBEUI
- SPX/ IPX

Die eigentliche Übertragung von Druckdaten erfordert:

- SMB
- oder RPC

3.3.3.7 Zugriffssteuerung

Die Zugriffssteuerung für die von Print-Servern betriebenen Netzwerkdrucker (Freigaben) wird von diesen Windows NT Print-Servern geregelt. Die Rechte auf diese Freigabe sind begrenzt auf die Stufen:

- Drucken
- Drucker verwalten
- Dokumente verwalten

3.3.3.8 Werkzeuge

Die Administrationswerkzeuge von Print-Servern unter Windows NT beschränken sich auf die Verwaltung der Druckerfreigaben und der Druckertreiber. Ein Management der Druckgeräte selbst ist nicht möglich.

Die Hersteller von Druckern stellen zusätzliche Werkzeuge zur Administration der Drucker bereit (MarkVision von LexMark, JetAdmin von HP, etc.).

Ähnlich wie bei Netzlaufwerken ist die automatische Verbindung zu Druckern beim Login des Anwender gewünscht. Dies kann entweder via VB-Script oder Tools wie con2prt.exe realisiert werden.

Hinsichtlich der Vergabe von Berechtigungen auf Druckerfreigaben sind Skriptprogramme (Perl) denkbar.

3.3.3.9 Besonderheiten in der Produktion

Die Geräteeinstellungen sind ausschließlich vom einzelnen Druckergerät abhängig; sie können selbst bei Modellgleichheit durch unterschiedliche Baureihen oder Ausstattungen verschieden sein. Bei der Einrichtung sind daher Einstellungen wie Arbeitsspeicher, Papierschächte und Papierformat zu beachten.

Drucker mit mehreren Schächten werden oftmals mit verschiedenen Papiersorten bestückt. Um dem Anwender die korrekte Auswahl zu erleichtern, wird der Drucker oft unter zwei verschiedenen Freigaben veröffentlicht. Jede Freigabe beinhaltet dann unterschiedliche Voreinstellungen hinsichtlich des Standardschachtes.

Um wandernde Benutzer optimal zu unterstützen, ist es denkbar, dass die Verbindung zu Druckern anhand des Rechnerstandortes erfolgt. Dies kann über zusätzliche Mechanismen im Logon-Script erfolgen, sofern eine Datenbasis befragt werden kann, die eine Zuordnung von Arbeitsplatzsystemen und Druckgeräten beinhaltet.

Für eine Vielzahl von Druckermodellen stellen die Hersteller eigene Druckertreiber bereit, auch wenn diese bereits in den Quellen von Windows NT enthalten sind. Die von Microsoft bereitgestellten Treiber sind von Microsoft geprüft, haben aber oftmals nicht den von den Treibern der Produzenten gebotenen Funktionsumfang (mehrere Schächte, Duplexeinheiten), so dass der Einsatz von Treibern der Hersteller notwendig wird. Die Hersteller realisieren oftmals ihre Treiber

durch zusätzliche dll-Dateien, was die Druckumgebung komplexer werden lässt. Dies impliziert ein Management der Treiberauswahl.

In bestehenden Druckkonzepten wird oftmals eine Priorisierung zwischen Postscript und PCL vorgenommen.

In einigen Umgebungen wird Gebrauch von selbst definierten Formularen (Forms) und Fonts gemacht.

In einer Windows NT Umgebung kann jeder Anwender in der Standardkonfiguration auf jeden Drucker zugreifen, der freigegeben ist, was jedoch oftmals nicht gewünscht ist. Die benutzerspezifische Rechtevergabe bei Druckerfreigaben ist im Vergleich zu den File Services deutlich schwieriger.

3.3.4 Ablösende Migration

In diesem Abschnitt wird davon ausgegangen, dass eine Druck-Infrastruktur besteht oder geschaffen werden soll, die mindestens einen Print-Server beinhaltet. Ein solcher Print-Server fungiert mindestens als zentraler Spooling Host, der darüber hinaus auch noch andere Dienste anbieten kann.

Als möglicher Migrationsweg wird im Folgenden ausschließlich das „Common UNIX Printing System“ evaluiert. Es ist auf praktisch allen Unix-Systemen etabliert. Seit Neuestem wurde es ebenfalls von Apple in sein Betriebssystem Mac OS X aufgenommen. Bei Linux ist CUPS der de-facto Standard aller großen Distributionen (Suse, Debian, Mandrake, RedHat, usw.).

Falls die bestehende Druckumgebung aus Windows-Clients besteht, die auf einen NT-Print-Server zugreifen, werden Möglichkeiten einer serverseitigen Migration untersucht.

3.3.4.1 Funktionale Anforderungen

Da Drucken häufig eine „mission critical“ Aufgabe ist, bestehen hohe Anforderungen an technische Infrastruktur und innere Organisation:

- Zuverlässigkeit
  Ein Mindestmaß an Ausfallsicherheit ist unabdinglich; Ausweichmöglichkeiten müssen leicht integrierbar sein – die Dienstbereitschaft der Printservices muss auch ohne Anwesenheit von IT-Experten gewährleistet sein.
- Getreue Wiedergabe
  Bewertungskriterien sind unverfälschte Fonts, unverzerrte Grafiken, Farbtreue.
- Druckqualität
  Rendern in Mindest-Auflösung wird erwartet.
- Accounting
  Kostenkontrolle durch detaillierte Protokollierungsmöglichkeiten sollte möglich sein.

- Quotas
  Anforderung, die eine Kostenkontrolle bzw. -begrenzung zum Ziel hat.
- Umleitung von Druckjobs
  Ein Ersatzdrucker sollte problemlos angesprochen werden können, ohne den Auftrag erneut vom Client abschicken zu müssen. (wichtig: falls der Ersatzdrucker ein anderer Typ ist, sollte er die vorliegende Druckdatei dennoch verarbeiten können).
- Erneutes Drucken
  In einer Umgebung mit zentraler Vervielfältigung sind häufig Nachdrucke abgeschlossener Druckaufträge erforderlich. Um „Printing on Demand“ umzusetzen und die Auflage nachträglich zu erhöhen, oder um technische Probleme (z.B. Papierstau/ Stromausfall) und Bedienerfehler (z.B. falsche Papierfarbe verwendet) auszugleichen, ist eine Funktion zum erneuten Nachdrucken erforderlich.
- Job History
  Hiermit steht ein Überblick über die gesamten Druckvorgänge zur Verfügung. Am Jahresende liegen aussagekräftige Zahlen über Gesamtmenge (Budgetplanung), Verteilung auf Modelle und Orte (Optimierung der Ressourcenverteilung) Spitzenbelastungen (sinnvolle Neuinvestitionen) vor.
- Integration in proprietäre Lösungen
  Oftmals müssen „alte“ oder neue proprietäre Speziallösungen übernommen oder integriert werden. Das sollte ohne große Anstrengungen möglich sein.
- Kostentransparenz und -kontrolle
  ist unverzichtbar – sowohl während der Migrationsphase als auch danach.
- Sicherheit
  „Abhören“ vertraulicher Daten sollte nicht möglich sein (auch nicht durch Abfangen von Druckdateien).
- Authentisierung
  Bestimmte Drucker sind nur für bestimmte Benutzergruppen – bzw. begrenzte „teure“ Einstellungen (1200 dpi im Vollbild-Modus auf Fotopapier) sind nur für bestimmte Benutzer (oder komplett disabled) erlaubt.
- Drucken „auf Halten“
  Zeitversetztes oder „nächtliches“ Drucken (automatisch gesteuerte Batch-Jobs).
- Ohne Spezialsoftware zur Übersicht
  Idealerweise ermöglicht ein Webbrowser den schnellen Einblick in die Warteschlangen. Ein zusätzlicher Kommandozeilenzugang ist garantiert, am besten „von überallher“. Idealerweise gilt dies nicht für jedermann, sondern nur für den berechtigten Personenkreis.

- Integration in heterogene Welten
  Eine Drucksoftware muss multiprotokollfähig sein, denn in der Praxis kommt noch kein allgemein verwendeter Standard zum Einsatz – Multiprotokoll-Fähigkeit muss sowohl Richtung Clients gegeben sein (die frei in der Wahl des Protokolls sein sollten, über das sie ihre Druckdaten schicken wollen) als auch Richtung Zieldrucker bzw. second-level Print-Server (die oft zu „altmodisch“ sind und deshalb bestimmte Konventionen verlangen). Zugleich muss eine umfassende Unterstützung des künftigen Standards IPP vorhanden sein.

3.3.4.2 Unterstützung etablierter[1] Standards bei Druckdaten-Übertragung

Die genannten funktionalen Anforderungen müssen durch die vorgeschlagenen technischen Lösungen erfüllt werden. Dabei ist vor allem eine entsprechende Offenheit durch die Konsolidierung auf bestehenden anerkannten offenen Standards anzustreben. Die für einen Übergangszeitraum noch erforderliche Unterstützung althergebrachter oder proprietärer Protokolle (und Geräte, die darauf beruhen) sollte weiterhin gewährleistet sein. Die Funktionalität von CUPS ist durch die Implementierung von IPP (Internet Printing Protocol – s.a IPP) plattformübergreifend angelegt. Das IPP wird als Protokoll zwischen den CUPS-Servern, -Clients und modernen Druckern mit direkter IPP-Unterstützung als Medium der Kommunikation- und Datenübertragung verwendet. Bei der Kommunikation mit herkömmlichen Druckern oder Print-Servern können CUPS-Module, so genannte „backends“, eingesetzt werden Diese Module ermöglichen die Kommunikation mittels anderer Protokolle. In Bild 9 wird die Verwendung der Protokolle an den jeweiligen Übergängen dargestellt. Die Funktionalitäten werden nachfolgend beschrieben.

LPR/ LPD

Das traditionelle Protokoll zur Druckdaten-Übertragung [vom Client zum Druckserver, von Server zu Server und vom Server zum Ziel(-netzwerk-)drucker, oder auch vom Client direkt zum Drucker], hat viele Nachteile: es ist unverschlüsselt, unautorisiert, wenig zuverlässig, nicht bidirektional (z.B. keine Rückmeldungen vom Drucker), kein „richtiger“ Standard (dadurch verschiedene Implementierungen, die wegen Inkompatibilitäten stellenweise zu Schwierigkeiten führen).

IPP

Internet Printing Protocol ist der Internetstandard für das Drucken sowohl im lokalen Netz (LAN) wie auch im großräumigen Netz (WAN, Internet). Das Protokoll deckt alle denkbaren Kommunikationsmöglichkeiten ab, vom Client zum Server, vom Server zum Server, vom Server zum Zieldrucker und auch den direkten Weg vom Client zum Zieldrucker. Die letzte und einzig verbindliche Spezifikation ist IPP-1.1. Das IPP wurde von einer Arbeitsgruppe (der PWG), bestehend aus Vertretern von Drucker- Betriebssystem und Software-Herstellern aus Europa, USA

[1] Sowohl offener als auch nicht offener Standard.

und Japan entworfen und von der IETF standarisiert. Es ist bereits in allen aktuellen Netzwerk-Druckern eingebaut. So lange allerdings noch „alte“ LPR/ LPD-Modelle im Einsatz sind (die auch noch auf Jahre hin funktionsfähig bleiben werden), wird die entsprechende Umstellung nur dort erfolgen, wo es auch unmittelbar sinnvoll ist.

Hinweis**:** Neuere Versionen von Microsoft Windows-Betriebssystemen haben eine gewisse clientseitige IPP-Unterstützung eingebaut (Windows 98SE, Windows ME, Windows 2000, Windows XP) oder lassen sich entsprechend kostenlos nachrüsten (Windows NT, Windows 95, Windows 98). Somit können diese Systeme quasi „ganz natürlich“ über CUPS-Server drucken. Allerdings wird derzeit durch Microsoft nur eine Implementierung der IPP-Version 1.0 angeboten, die bei der IETF nie „recommended standard“ wurde, sondern nur einen Diskussions-Zwischenstand widerspiegelte und z.B. den wichtigen Aspekt der Verschlüsselung von Druckdaten und der Authentisierung von Benutzern noch nicht definiert hatte. Somit muss ein CUPS-Server auf Authentisierung verzichten, will man ihn direkt vom Windows-Client aus nutzen. Kommt CUPS in Kombination mit Samba zum Einsatz, kann eine eventuell notwendige Authentisierung der Windows-Clients über die bei Samba implementierten Mechanismen erfolgen. Für Umgebungen mit erhöhten Sicherheitsanforderungen sind für Windows kommerzielle CUPS-Clients am Markt.

Socket/ AppSocket

AppSocket (oft besser bekannt als „HP JetDirect“) ist ein performantes Übertragungsprotokoll für Druckdaten. Es ist leistungsfähiger und zuverlässiger als LPR/ LPD: es beinhaltet ein gewisses Maß an bidirektionaler Kommunikation und es ist schneller. Für JetDirect gibt es freie und kommerzielle Administrations-Tools zur Strukturierung großer Netze (z.B. HP WebJet Admin). Allerdings bietet es weder Verschlüsselung von Druckdaten noch Authentisierung von Nutzern. Die Status-Rückmeldungen vom Drucker erfolgen in der Praxis nur vom Server zum Drucker oder bei direktem Weg vom Client zum Drucker.

SMB/ CIFS

Windows-Clients benutzen dieses Protokoll, um an Druckserver (oder andere Windows-Rechner, sofern diese „freigegebene“ Drucker anbieten) Druckdaten zu übertragen. Der Weg vom nächsten Windows-Rechner zum Ziel(-netzwerk-)drucker muss dann häufig wieder über ein anderes Protokoll geregelt werden (außer dieser ist lokal – über Parallel-, USB-, FireWire- oder Serielle Schnittstelle – angeschlossen).

MS-RPC

Windows-Clients ab NT4 können dieses Protokoll verwenden, um Druckdaten an einen Windows-Print-Server (ab NT4) zu übertragen. Ebenso kann eine automatische Treiberinstallation auf den Clients über RPC-Methoden erfolgen, sofern der Print-Server die entsprechenden Dateien vorhält. (Das „Hochladen“ der Treiber auf den Print-Server durch einen Administrator von einem Client-Rechner aus

basiert ebenfalls auf RPC). Da Samba SMB/CIFS beherrscht, kann dieses Protokoll auch für CUPS nutzbar gemacht werden.

Multiprotokoll-Fähigkeiten bei CUPS (Übersichtsdarstellung)

Bild 9: Drucken unter CUPS[1]

3.3.4.3 Integration in Windows Client-Umgebungen

CUPS/ Samba-Integration Hinweis

CUPS ist optimal in Samba integriert – weitaus besser als anderer verfügbarer UNIX-Druck Subsysteme. Es ist das einzige Drucksystem, das seine Funktionen in eine Library (Software-Bibliothek) eingebaut hat. Dadurch können andere Programme seine Funktionen nutzen, indem sie gegen diese Bibliothek „linken". Samba macht davon Gebrauch. Per Default ist Samba gegen libcups. so gelinkt. Ein Samba-Print-Server kann dadurch seine ankommenden Druckaufträge per IPP an CUPS-Print-Server weiterleiten. Diese CUPS Print-Server können auf anderen, für den Druckdienst dezidierten Hosts installiert sein oder auf demselben wie Samba. Die Verwendung von IPP geschieht hier völlig transparent für den Administrator oder Nutzer und erfordert keine weitere Konfiguration.

[1] Öffentlich zugänglich unter http://www.linuxprinting.org/kpfeifle/Linux-Kongress2002/Tutorial/

Tab. 16: Client-Anbindung an CUPS

Client-Betriebssystem	Anbindung
Windows 9x	Win98SE mit IPP (Version 1.0) ausgeliefert – Win98 nachrüstbar über SMB/ CIFS (mit Hilfe von Samba) über LPR/ LPD (erfordert Zusatzinstallation eines LPR-Clients)
Windows NT	IPP nachrüstbar über SMB/ CIFS + MS-RPC (mit Hilfe von Samba) über LPR/ LPD
Windows 2000/ XP	IPP (Version 1.0 eingebaut) über SMB/ CIFS + MS-RPC (mit Hilfe von Samba) über LPR/ LPD
Citrix Metaframe und Windows Terminal-Server	IPP nachrüstbar über SMB/ CIFS + MS-RPC (mit Hilfe von Samba) über LPR/ LPD
Linux	CUPS und IPP eingebaut über LPR/ LPD
UNIX	CUPS und IPP nachrüstbar über LPR/ LPD
NetWare	IPP eingebaut in NPDS (seit Novell 5.0) über SMB/ CIFS (mit Hilfe von Samba) über LPR/ LPD
Mac OS 9	über AppleTalk
	über LPR/ LPD (erfordert Zusatzinstallation eines LPR-Clients)
Mac OS X	über CUPS und IPP eingebaut seit OS X 10.2 über LPR/ LPD (erfordert Zusatzinstallation eines LPR-Clients)

Treiber-Download & -Installation durch Clients mit „Point and Print“

Die CUPS/Samba-Kombination unterstützt den automatisierten Treiber-Download zu Windows-Clients mittels „Point and Print“. Samba muss hierfür so konfiguriert sein, dass es einen NT-Print-Server nachbildet. Die Konfiguration ist in der Samba HOWTO Collection detailliert beschrieben. Es erfordert jedoch nur wenige Handgriffe. Das Hochladen von Treibern durch einen Administrator von einer Client-Maschine aus wird ebenfalls unterstützt.

Die Druckertreiber liegen hierbei auf dem Samba-Server. Sie werden automatisch im Hintergrund auf den Windows Client-Systemen installiert, sobald der Nutzer erstmals den Drucker in der Netzwerkumgebung sucht oder erkennt und (per „Rechts-Mausklick“) im Kontext-Menü „Verbinden...“ auswählt.

Automatische Treiberinstallation per Logon-Scripts

Noch komfortabler wird es für Benutzer und Administratoren innerhalb einer Domäne, wenn „Logon-Scripts“ eingesetzt werden. In diesem Logon-Script braucht lediglich die Zeile

„rundll32 printui.dll,PrintUIEntry /in /n„\\SAMBASERVERNAME\druckerfreigabename“

vorzukommen. Sie installiert den entsprechenden Drucker automatisch für den sich einloggenden Benutzer (weitere diesbezügliche Möglichkeiten sind die Installation mehrerer Drucker, die Setzung eines Standard-Druckers, die Löschung hinfällig gewordener Druckerwarteschlangen usw.). Diese Möglichkeit offeriert eine komfortable Administration der Druckertreiber und eine Verringerung der Aufwände für die Administratoren. Verschiedene Benutzer-Gruppen können über verschiedene Logon-Scripts verschieden angepasste Umgebungen erhalten.

Sicherheit und Authentisierung

Die Kommunikation zwischen den Client- und Serversystem kann unter CUPS auch in verschlüsselter Form erfolgen. Sofern IPP verwendet wird, kann für die Übertragung der Daten SSL 3 oder TLS genutzt werden.

Windows-Clients authentisieren sich typischerweise nicht bei CUPS, sondern bei Samba. Diese Authentisierung wird automatisch genutzt, wenn über Samba gedruckt wird. Die Rechteverwaltung wird dabei von Samba übernommen. Es ist dann lediglich auf geeignete Weise sicherzustellen, dass der Samba-Server zur Benutzung des CUPS-Print-Servers autorisiert ist.

Publikation von CUPS-Druckern in LDAP und Active Directory

Samba kann seine Dienste in einem LDAP- oder Active Directory-Verzeichnis eintragen. Davon profitieren selbstverständlich auch CUPS-Drucker und CUPS-Print-Server. Weitere Ausbaustufen der Integration in eine AD- (oder in eine diese weitgehend nachbildende LDAP-) Umgebung sind möglich. Eine kommende CUPS-Version, die eine Anbindung an LDAP „aus eigener Kraft“ beherrscht, befindet sich bereits in einer fortgeschrittenen Beta-Test-Phase.

Plattformunabhängiges Web-Interface

CUPS hat ein „eingebautes“ Web-Interface. Erreichbar ist es über die URL „http://CUPS-DRUCKSERVER:631/“. Es ermöglicht den informativen Zugang aller Nutzer zu den Funktionen des Druckservers. Benutzer können standardmäßig den Status von Druckaufträgen überwachen, sie abbrechen, neustarten, alte Aufträge nachdrucken etc. (abhängig von der jeweiligen Konfiguration).

Administratoren oder Help-Desk-Mitarbeiter können über das Web-Interface Drucker(-Wartenschlangen) neu anlegen, löschen, umkonfigurieren, starten, stoppen, schließen oder öffnen sowie Druckaufträge stornieren, auf Halde legen oder neustarten. Die Möglichkeiten zur Verwendung des Web-Interface können durch Konfiguration des CUPS-Servers eingeschränkt bzw. erweitert werden. Das Web-Interface unterliegt denselben Zugangskontrollen wie die allgemeinen CUPS-Ressourcen. Jedes Objekt des Druckservers (Zugriff auf eigene Jobs oder

einzelne Drucker, Zugriff auf alle Drucker oder alle Jobs usw.) lässt sich mit differenzierten Zugriffsrechten versehen: „User Müller darf administrieren, aber nur wenn er von Rechner A oder B zugreift“, „Alle User dürfen eigene Druckjobs löschen, aber keine fremden“, usw.)

3.3.4.4 Anpassungsfähigkeit

Über den unmittelbaren Funktionsumfang von CUPS hinaus lässt sich das Drucksystem vielfältig und einfach um Filter und BackEnds erweitern.

Filter

CUPS verwendet intern ein modular aufgebautes Filtersystem. Es setzt auf offenen Schnittstellen auf. Es kann jederzeit erweitert werden. Dabei können beliebige Scriptsprachen (Shell, Perl, Python) oder Programmiersprachen (C, C++, Java etc.) zum Einsatz kommen. Einbindung proprietärer Binär-Programme ist auf einfachste Weise über Wrapper-Skripte möglich.

BackEnds

Neue BackEnds sind leicht „andockbar“. Sei es zur umgebungsspezifischen Anpassung an spezielle Anforderungen (z.B. automatische Replikation bestimmter Druckaufträge in einer anderswo lokalisierten Abteilung, z.B. zwecks Ablage von Geschäftsbriefen im Archiv), sei es weil technologische Neuerungen dies attraktiv machen (Wireless LAN, Bluetooth, FireWire).

3.3.4.5 Seitenbeschreibungssprachen

Für die Druckeransteuerung verwendet CUPS die so genannte PostScript Printer Descriptions (PPD). Die PPD-Spezifikation ist ursprünglich durch die Firma Adobe definiert worden und wird von praktisch jedem Drucksystem beherrscht, das PostScript-Drucker ansteuert und deren gerätespezifischen Optionen (Duplexdruck, Fachanwahl, Lochen, Heften usw.) benutzt. Solche PPD Dateien gibt es zusammen mit CUPS auch für Drucker, die keinen eigenen PostScript-Interpreter besitzen. CUPS benutzt diese wohldefinierten Druckerbeschreibungen um die entsprechenden Konfigurationseinstellungen über das Web-Frontend oder über die Konfigurationsmasken der Clients zu ermöglichen.

Für Drucker, die nicht postscriptfähig sind, konvertiert der CUPS-Server die vom Client gelieferten Daten durch den Einsatz so genannter „Filter“. Unter Linux beinhaltet das Programm ghostscript bereits umfangreichste Filterpakete zur Konvertierung von PostScript in verschiedene hersteller- und gerätespezifische Seitenbeschreibungssprachen. In CUPS ist eine angepasste Version von ghostscript integriert.

3.3.4.6 Technische Umsetzung der Treiberfunktion

Die Umsetzung der Druckdatei in druckergerechte Bitmaps kann über zwei unterschiedliche Modelle realisiert werden. Dies sind:

- Die komplett clientseitige Ausführung der Treiberfunktionen
  Hier wird die Druckdatei auf dem Client druckfertig aufbereitet. Der Druckserver hat reine Spooling-Funktionen für „raw“ Druckdaten. Treiber können dem Client zum Download und automatischer Installation angeboten werden.
- Die Druckdaten-Aufbereitung erfolgt auf dem Print-Server
  Hierbei werden die Druckdaten von den Clients im PostScript-Format an den Print-Server gesendet. Auf den Clients wird hierzu ein entsprechender PostScript-Treiber benötigt, dieser kann vom Server zur automatischen Installation angeboten werden. Die aufbereiteten Druck-Daten werden vom Server an den gewünschten Drucker weitergeleitet. Sofern es sich um einen Nicht-PostScript Drucker handelt, erfolgt die Druckaufbereitung mittels spezieller Software (s.a. 3.3.4.5).

Das zweite Modell bietet gegenüber dem Ersten mehrere Vorteile:

- Es unterstützt automatisch alle PostScript-Geräte mit allen Druckoptionen (wie unter Windows NT).
- Es unterstützt zusätzlich die allermeisten gängigen Nicht-PostScript Drucker (abhängig von der Unterstützung durch ghostscript oder andere Treiberpakete).
- Automatisches Accounting
  Über jede Seite werden Druckzeit, Auflage, Zieldrucker, Anwendername, Druck-ID und Absender-IP automatisch mitgeloggt und stehen für spätere Auswertungen (Kostenkontrolle, Statistiken) zur Verfügung.
- Quotierungsoption
  Druck-Quotas (nach Anzahl der Seiten und/oder Größe der Druckdaten-Menge) können den Nutzern pro Drucker zugeordnet werden.
- Reprint-Funktion
  Aufträge können über einen gewissen Zeitraum aufbewahrt werden und stehen zur Verfügung, sollte ein Neu- oder Nachdruck erforderlich sein (ohne dass der Client die Datei nochmals suchen, öffnen und abschicken muss).
- Redirect-Funktion
  Druckdateien können jederzeit auf einen anderen Zieldrucker umgeleitet werden (selbst dann, wenn der ursprüngliche Drucker ein PostScript-Modell war und der neue ein nicht-PS-Gerät ist). Druckoptionen können modellgerecht auf das neue Zielgerät angepasst werden.
- Treiber-Konsolidierung
  Alle Clients verwenden im Endeffekt denselben Core-PostScript-Treiber (der nur durch eine ASCII-Datei, die „PPD“ modifiziert wird).

Allerdings beinhaltet dieses Modell folgende Einschränkungen:

- Erhöhter Ressourcenbedarf
  Die zentrale Druckdatenaufbereitung auf dem Server erfordert mehr RAM, CPU und HD-Platz (kann zuverlässig im Voraus ermittelt werden, wenn das erwartete Druckaufkommen bekannt ist).
- Leichte Einschränkungen bei unterstützten Druckermodellen
  Zwar werden die Mehrzahl der gängigen Druckermodelle unterstützt – allerdings gibt es hin und wieder Fälle, wo dies nicht der Fall ist. Eine Liste der unterstützten Hersteller und Modelle kann der „Linuxpriniting.org"-Datenbank entnommen werden.

3.3.4.7 Drucksystem-Architekturen

In der folgenden Auflistung werden die potentiellen Architekturmöglichkeiten beim Einsatz von CUPS skizziert, wobei die Erhöhung der Ausfallsicherheit für viele Einsatzszenarien von entscheidender Bedeutung ist:

- **Server:**
  Jeder CUPS-Rechner, der direkt mit einem Drucker kommuniziert, kann die Druckfunktion anderen Rechnern als Dienst anbieten und fungiert somit als CUPS-Server. Voraussetzung dafür sind die entsprechenden PPDs und Filter für die druckgerechte Aufbereitung der Druckdateien.
- **Client:**
  Jeder Rechner, der Druckdateien an einen Server weiterschickt, ist ein CUPS-Client. Ein Client benötigt lokal keine Filter oder PPDs. Wenn jedoch auf dem Client festgelegt werden soll welche Druckmöglichkeiten beim Drucken verwendet sind, werden die PPDs vom Server automatisch auf den Client übertragen.
- **Zero-Administration für native CUPS Clients**:
  CUPS-Server verbreiten innerhalb des Netzwerkes Informationen über die installierten Drucker an die Clients. Damit wissen die Clients, welche Drucker im Netzwerk verwendet werden können. Die Informationen werden mittels UDP-Broadcasting publiziert. Alternativ kann der Client gezielt die Informationen bei den Servern nachfragen (Polling). Das Polling kann auch gezielt bei Servern eingesetzt werden, die durch Router getrennt sind. Server, die in unterschiedlichen Netzen stehen, können als Browse-Relay konfiguriert werden und die Daten über die verfügbaren Drucker abholen und an die Clients der eigenen Broadcast-Domäne weiterleiten.
- **Clustering für Ausfallsicherheit und Failover:**
  Zwei oder mehrere CUPS-Server können so konfiguriert werden, dass Ausfallsicherheit bezüglich der Druckdienste implementiert werden kann. Das Ziel kann erreicht werden, wenn die Server mit denselben Druckern und Druckernamen konfiguriert werden. Auf den CUPS-Servern werden automatisch implizite Klassen gebildet, die aus den Druckern mit demsel-

ben Namen bestehen. Der Server, der zuerst bereit ist, übernimmt dann den Druckauftrag des Clients und schickt ihn an den Drucker. Diese Konfiguration kann auch durch die manuelle Bildung von Klassen hergestellt werden, wobei diese Klassen auch aus Druckern mit unterschiedlichen Namen bestehen können.

3.3.5 Fortführende Migration

3.3.5.1 Windows 2000

In diesem Abschnitt wird auf den Nachfolger von Windows NT4, Windows 2000, hinsichtlich des Themas „Print Service“ eingegangen.

Funktionszuwachs

Mit Windows 2000 sind hinsichtlich der Print Services einige Neuerungen verbunden. Als Stichworte seien hier genannt:

- Standard TCP/IP Port Monitor
- Internet Printing
- Veröffentlichung im Active Directory.

Im Folgenden werden diese Themen näher erläutert.

Server-Drucker-Kommunikation

Mit Windows 2000 hat Microsoft SPM (Standard TCP/IP Port Monitor) eingeführt. SPM ist kompatibel mit SNMP. Neben SPM existiert weiterhin der Porttyp LPR. SPM liefert im Vergleich zu LPR die Möglichkeit, detaillierte Statusinformationen abzurufen.

SPM kann zwei verschiedene Druckerserverprotokolle verwenden: RAW oder LPR. Standard für die meisten Druckgeräte ist RAW.

Veröffentlichung im Active Directory

Mit Hilfe des Active Directory kann die Druckerfreigabe (auf Windows NT oder 2000 Servern) dahingehend veröffentlicht werden, dass der Anwender nicht mehr wissen muss, auf welchem Server sich die Druckerfreigabe befindet. Der Anwender kann einfach das AD durchsuchen lassen.

Internet Printing

Mit Windows 2000 besteht die Option, Drucker im Web zu veröffentlichen und die Installation zu ermöglichen.

Gemischte Umgebungen

Auf Windows NT Servern lassen sich keine Treiber für Windows 2000 oder XP Clients hinterlegen. In solchen Umgebungen müssen die Treiber separat installiert werden.

Auf Windows 2000 Servern können Treiber für Windows NT Clients hinterlegt werden. Die Übertragung der gerätespezifischen Einstellungen kann allerdings

scheitern, wenn herstellerspezifische Treiber eingesetzt werden (müssen). Ursache hierfür ist die Verlagerung der Druckertreiber vom Kernel Mode unter NT in den User Mode unter Windows 2000.

3.3.5.2 Windows 2003 Server

Hinsichtlich der Version Windows 2003 sind zum Zeitpunkt der Erstellung dieses Leitfadens keine Neuerungen gegenüber Windows 2000 bekannt gewesen.

3.4 Authentisierungsdienste

3.4.1 Überblick

Die nachfolgenden technischen Detailbetrachtungen kommen zu dem Ergebnis, dass sowohl bei der fortführenden Migration als auch bei der ablösenden Migration und letztendlich auch in heterogenen Umgebungen mit Hilfe der verfügbaren Hilfsmittel eine gesicherte Authentifizierung der Benutzer- und Computerobjekte vorgenommen werden kann. Hierbei spielen Samba und OpenLDAP die wesentliche Rolle.

In einer heterogenen Systemumgebung bietet Samba als eine Alternative zum Windows NT-Server für die Windows-Clients ähnliche Funktionalitäten wie ein NT-basierter primärer Domänencontroller. Samba kann als Datenbank für Benutzerkonten auf OpenLDAP als Verzeichnisdienst zurückgreifen. Für den Windows-Clients realisiert Samba in Zusammenspiel mit OpenLDAP eine Windows NT-Domäne. Bezüglich der Administration von Benutzer-, Gruppen- und Host-Informationen wird eine Verzeichnisdienst-basierte Lösung mit allen daraus resultierenden Vorteilen realisiert. Beispielsweise entfällt bei einer solchen Lösung das von Windows NT bekannte Skalierungsproblem, das oft die Aufteilung einer Infrastruktur in unterschiedliche Domänen erfordert.

Mittels Samba können Vertrauensstellungen zwischen unterschiedlichen Domänen eingerichtet werden, ebenso ist es möglich, mit Samba einen WINS-Service zu realisieren. Mit Samba 3.0 steht auch ein Programm zur WINS-Replikation zur Verfügung. Aus Kompatibilitätsgründen unterstützt Samba das Konzept von PDC und BDCs. Diese Unterstützung besteht unter anderem darin, dass Samba-Server sich je nach Konfiguration gegenüber Windows Clients als PDC bzw. BDC ausgeben und bestimmte Aufgaben nur von dem PDC ausgeführt werden (Passwortänderungen von Benutzern, Aufnehmen neuer Computer in die Domäne, etc.). Samba selbst unterstützt keine Replikation der SAM-Datenbank zwischen PDC und BDC. Die Replikation der SAM kann jedoch von OpenLDAP übernommen werden.

Mit der fortführenden Migration kommt es bei der Authentifizierung in heterogenen Systemumgebungen zu kleineren Einschränkungen. Diese liegen im Zusammenspiel zwischen Samba/OpenLDAP und Active Directory sowie zwischen Samba/OpenLDAP und der Kerberos-Authentifizierung.

Hervorzuheben ist hierbei, dass keine Kerberos-Authentifizierung von Windows 2000/XP Clients gegenüber Samba/OpenLDAP möglich ist, sondern dass hier das NTLM-Protokoll verwendet werden muss. Solange Microsoft dies weiterhin unterstützt, damit z.B. Windows NT-Clients ebenfalls noch integriert werden können, ist dies unproblematisch. Demgegenüber kann einen linuxbasierter Kerberos Server mit einer Active Directory Domäne verwendet werden, so dass sich auf Basis von Linux ein einheitliches Credential-Management für Windows und Linux aufbauen lässt.

In einer reinen linuxbasierten Systemumgebung kann die Authentifizierung der Benutzer mittels Kerberos erfolgen, alternativ kann auch die Authentifizierung mittels OpenLDAP realisiert werden.

3.4.2 Ausgangslage – Windows NT 4

Thema dieses Unterabschnitts sind die Anmeldedienste bzw. die Authentifizierungsdienste der Microsoft Produkte. Unter anderem werden die Aspekte

- Benutzerdatenbanken
- Integration von Computern und Netzwerkdiensten
- Authentifizierung

betrachtet.

Dafür sollen zunächst die technischen Grundlagen einer Windows NT Umgebung hinsichtlich der Anmeldedienste aufgeführt werden.

3.4.2.1 Domäne

Kerntechnologie der Anmeldedienste unter Windows NT ist die Struktureinheit „Domäne“. Die Domäne ist eine Verwaltungseinheit, die Computer- und Benutzerkonten mittels einer gemeinsam genutzten Datenbank in einem gemeinsamen Sicherheitskontext zusammenfasst. Diese Datenbank wird als SAM (Security Accounts Manager) bezeichnet. Sie wird zur Laufzeit in der Registry (Registrierungsdatenbank) spezieller Serversysteme gehalten, den Domain Controllern (Domänenkontrollern). Neben Benutzer- und Computerobjekten werden auch Gruppen in der SAM administriert. Jede dieser drei Objekttypen lässt sich durch eine so genannte SID (Security Identifier) eindeutig kennzeichnen, die sich auch in verschiedenen Domänen nicht wiederholen soll. Zu jeder SID (ein relativ langer Zahlenkonstrukt) existiert ein SAM-Accountname, der in der Regel maximal 15 alphanumerische Zeichen umfassen kann (einige Sonderzeichen sind erlaubt). Der SAM-Accountname ist der Name, den die Anwender zur Identifikation verwenden.

Computer auf der Basis

- Windows NT
- Windows 2000
- Windows XP

können Mitglied einer Domäne sein. Für Systeme wie beispielsweise Windows 3.11 oder 9x kann hingegen kein Computerkonto in einer Domäne erstellt werden. Wenn ein Computer Mitglied einer Domäne wird, werden in der SAM des Computers Gruppen der Domäne (Globale Gruppen) Mitglied der lokalen Gruppen des Computers. So „wandelt“ sich die Gruppe „Domänenbenutzer“ zum Mitglied der lokalen Gruppe „Benutzer“. Auf diese Weise wird z.B. ermöglicht, dass Anwender, die sich auf einem NT Computer gegen eine Domäne anmelden können, lokalen Zugriff auf die Ressourcen des benutzten Computers erhalten.

Eine Domäne benötigt mindestens einen Domain Controller, den so genannten PDC (Primary Domain Controller). Er hält die SAM der Domäne, die Inhalte der SAM können nur bei ihm verändert werden. Zur Lastverteilung und Redundanz der SAM werden so genannte BDC (Backup Domain Controller) eingesetzt; sie halten eine Kopie der SAM, die regelmäßig um die Änderungen auf dem PDC aktualisiert wird.

Der Vorteil der Verwaltungseinheit „Domäne“ liegt auf der Hand: Damit Anwender lokale Ressourcen oder Ressourcen auf Systemen im Netzwerk nutzen können, muss nicht auf jedem System ein Benutzerkonto eingerichtet werden, sondern lediglich ein Benutzerkonto in der SAM der Domäne. Der Schutz der Ressourcen, die Autorisierung, erfolgt separat auf den Systemen, die die Ressourcen zur Verfügung stellen. Benutzer, die Windows 9x nutzen, können sich ebenfalls an einer Domäne anmelden und somit Ressourcen im Netzwerk nutzen, ohne zusätzliche Anmeldungen durchführen zu müssen.

3.4.2.2 Mehrere Domänen und Vertrauensstellungen

Es ist möglich, mehrere Domänen über Vertrauensstellungen miteinander zu verknüpfen. Dadurch ist es möglich, Benutzer oder Gruppen anderer Domänen für den Zugriff auf Ressourcen (z.B. File Services) der eigenen Domäne zu autorisieren. Der primäre Zweck ist also, den Zugriff auf Ressourcen über Domänengrenzen hinweg zu erreichen.

Eine Vertrauensstellung zwischen NT Domänen ist nicht zwingend beidseitig (bidirektional): wenn Domäne A der Domäne B vertraut, muss B nicht auch A vertrauen. Vertrauensstellungen sind auch nicht transitiv: wenn A B vertraut und B der Domäne C, dann vertraut A nicht implizit auch C. Jede Vertrauensstellung muss also explizit eingerichtet werden.

Folgende Umstände haben zur Etablierung mehrerer Domänen in IT-Umgebungen geführt:

- Oftmals sind parallele Insellösungen innerhalb einer Infrastruktur entstanden, die später aufgrund von gemeinsamen Arbeitsprozessen mit Hilfe von Vertrauensstellungen zusammengeführt werden mussten. Dies gilt auch, wenn zwei Infrastrukturen zusammengeführt werden.

- Die Domänengrenzen sind Grenzen der Sicherheit: Administratoren der Domäne A sind nicht automatisch Administratoren der Domäne B, der man vertraut oder die einem vertraut. Politische Überlegungen spielen hier eine Rolle.
- Die unvorteilhafte Möglichkeit, Aufgaben zu delegieren, wurde durch mehrere Domänen kompensiert
- Die Anzahl der Objekte (Computer, Benutzer, Gruppen) in der SAM ist beschränkt, da die SAM zur Laufzeit in der Registry der Domain Controller, deren Größe ebenfalls beschränkt ist, gehalten wird. Abhilfe konnte nur die Aufteilung der Objekte auf mehrere Domänen bringen.
- Die Skalierung von einer Domäne in stark verteilten, dezentralen Umgebungen wird durch das Single-Master-Prinzips des PDCs eingeschränkt, da sämtliche Änderungen der SAM nur über ihn realisiert werden können.

Diese Tatsachen haben zu verschiedenen Domänenmodellen geführt, die unter anderem von Microsoft selbst vorgeschlagen wurden:

- Single Domain (eine Domäne)
- Master Domain (mehrere Domänen vertrauen alle einer Master Domäne, typischerweise vertrauen Ressourcendomänen der Account-Domäne)
- Multiple Master Domain (mehrere Ressourcendomänen vertrauen allen (mehreren) Account-Domänen
- Complete Trust Domain (jede Domäne vertraut den anderen)

3.4.2.3 NT als Verzeichnisdienst

Im weitesten Sinne sind Windows NT Domänen auch Verzeichnisdienste, denn in einer Domäne sind Benutzerobjekte verzeichnet. Microsoft bezeichnet diesen mit NTDS (Windows NT Directory Service).

Die Anzahl der Attribute eines Benutzerobjektes in einer NT Domäne ist relativ klein und beschränkt sich mehr auf technisch relevante Attribute und Eigenschaften. Die Attribute sind daher nicht vergleichbar mit dem Verzeichnisdienst basierend auf X.500.

Die Benutzereigenschaften umfassen unter anderem:

- Benutzername (SAM-Accountname)
- vollständiger Name und Beschreibung (technisch nicht relevant)
- Kontoinformationen (z.B. Konto deaktiviert, Kennwort läuft nie ab, Ablauf des Konto, Kontotyp)
- Gruppenmitgliedschaften
- Umgebungsparameter (Logon-Script, Home-Verzeichnis, Pfad des servergestützten Profils)

- erlaubte Anmeldezeiten, erlaubte Clientcomputer
- RAS- (Remote Access Service)/ Einwahlparameter: erlaubt, mit/ ohne Rückruf

Darüber hinaus werden Attribute gespeichert, die vom Betriebssystem verwaltet werden, wie z.B.:

- SID
- LastLoginTime
- etc.

Eine Erweiterbarkeit um selbst definierte Attribute ist nicht vorgesehen. Microsoft selbst hat mit der Einführung von „Windows NT 4 Server Terminal Edition“ und Citrix Metaframe zusätzliche Eigenschaften für das Benutzerobjekt implementiert (zusätzliche Home- und Profilpfade und weitere Citrix Parameter).

Das NTDS kann nicht hierarchisch strukturiert werden, die Vergabe von Rechten auf Attributebene ist nicht möglich. Eine flexible Vergabe von Rechten auf Benutzerobjekte ist stark eingeschränkt.

3.4.2.4 Delegation

Die Delegation von administrativen Aufgaben innerhalb einer NT Domäne reduziert sich

- auf die Nutzung der eingebauten (Built-In) Gruppen (Domänen-Administratoren, Konten-, Server-, Sicherungs- Druck- und Reproduktionsoperatoren); diese Variante ist allerdings sehr unflexibel.
- auf die Installation zusätzlicher Domänen.

Diese Restriktionen bzw. Nachteile haben wohl dazu geführt, dass die Delegation und bestehende Rollenkonzepte auf webbasierenden Anwendungen abgebildet wurden.

3.4.2.5 Netzwerkbasis

Eine Windows NT Domäne kann auf den Transportprotokollen

- TCP/IP
- NetBEUI
- SPX/IPX

basieren.

In jedem Fall ist die NetBIOS Schnittstelle notwendig.

In den TCP/IP Netzwerken, die in diesem Leitfaden als Standard angesehen werden, ist für die fehlerfreie Kommunikation die Namensauflösung von NetBIOS-Namen (Computernamen als auch Benutzernamen sowie weitere Namenstypen wie z.B. Arbeitsgruppe) zwingend erforderlich. Will z.B. ein Benutzer sein

Domänenkennwort ändern, muss er den PDC lokalisieren bzw. seine IP-Adresse kennen.

Die NetBIOS-Namensauflösung kann in Windows Netzwerken auf verschiedene Weisen erfolgen:

- durch Broadcast
- durch Befragung eines WINS Servers (Windows Internet Name Service)
- oder durch Auswerten der Datei LMHOSTS

Die wohl eleganteste Lösung dieser Aufgabe ist der Einsatz von WINS Servern. Nur diese ermöglichen die Namensauflösung über IP-Subnetze hinweg, dynamische Inhalte und eine Minimierung der Broadcasts. Oftmals ist der WINS-Dienst auf den Domain Controllern realisiert.

Unabhängig vom gewählten Transportprotokoll wird in Windows Netzwerken der Computersuchdienst (Browser Service) ausgeführt. Er kann theoretisch auf allen Windows Betriebssystemen beheimatet sein. Der Computersuchdienst ermöglicht es, einem anfragenden Client (z.B. durch den Befehl „net view“) eine Liste der im Netzwerk aktiven Computer zu liefern. Sofern diese Liste auch über IP-Subnetze hinweg gelten soll, muss der Computersuchdienst im lokalen Subnetz die Informationen des „Domänen Master Browser“ abfragen können, was durch den Einsatz von WINS möglich wird.

3.4.2.6 File Replikation

Die Domain Controller (PDC als auch BDCs) stellen unter ihrer NETLOGON-Freigabe Logon-Scripte und Systemrichtlinien zur Verfügung, die von den sich anmeldenden Benutzern abgefragt werden.

Die Inhalte dieser Freigabe sollten auf allen Domain Controllern einer Domäne identisch sein, damit der Benutzer immer dieselben Anpassungen seiner Umgebung erfährt.

Zu diesem Zweck müssen die Server die Inhalte miteinander austauschen. Der so genannte Verzeichnisreplikrationsdienst (LMRepl) sorgt dafür, dass die Inhalte des so genannten Exportservers auf die Importserver repliziert werden. Änderungen der Inhalte dürfen nur auf dem Exportserver durchgeführt werden:

3.4.2.7 Verwaltungsinstrumente

Zur Administration von Benutzerobjekten, Gruppen und Computer werden unter Windows NT 4 graphische Bordmittel wie Benutzermanager Servermanager bereitgestellt.

Darüber hinaus werden mit dem „NT Resource Kit“ Tools geliefert, die überwiegend auf der Kommandozeile ausgeführt können und mit deren Hilfe man Skripte zur automatischen Administration erstellen kann.

Des Weiteren kann eine Domäne auch per Web-Interface verwaltet werden. Notwendig hierfür ist der Einsatz des Internet Information Servers (IIS) von Microsoft.

Eine gewisse fehlende Komfortabilität der Bordmittel hat Dritthersteller dazu veranlasst, weitere Werkzeuge zu entwerfen. Diese nutzen vorrangig die APIs von Windows NT.

Microsoft selbst produzierte nachträglich die Microsoft Management Console (MMC), die schließlich in Windows 2000 integriert wurde.

Ebenfalls nachträglich hat Microsoft mit ADSI (Active Directory Service Interface) eine COM-basierende Schnittstelle geliefert, mit der auch Windows NT Domänen verwaltet werden.

3.4.2.8 Speicherung von Kennwörtern

Die Kennwörter der Benutzer (auch der Computer) werden in einer Domäne in der SAM der Domain Controller gespeichert. Es wird nicht das Kennwort im Klartext, sondern in einem Hash-Wert gespeichert. Unter Windows NT kann die SAM selbst zusätzlich verschlüsselt werden (SYSKEY.EXE), die Verschlüsselung erfolgt seit dem Service Pack 3 automatisch. Die Hash-Werte der Kennwörter werden nach verschiedenen Verfahren gebildet, die sich wie folgt weiter entwickelt haben:

- LM (LAN Manager)
- NTLM
- NTLMv2

Auf NT Systemen, die kein Domain Controller sind, werden die Anmeldeinformationen der zuletzt angemeldeten Benutzer zwischengespeichert, um so die Anmeldung zu ermöglichen, auch wenn kein Domain Controller erreichbar ist (typischerweise: Notebooks). Diese Informationen werden wiederum in einem Hash-Wert gespeichert.

3.4.2.9 Authentifizierungsmechanismus

Die Authentifizierung innerhalb einer NT Domänenlandschaft basiert auf dem Mechanismus NTLM.

Es wird folgendes Szenario betrachtet. Eine Ressourcendomäne vertraut einer Account-Domäne. Eine funktionsfähige WINS Umgebung ist vorhanden. Ein Benutzer startet eine Windows NT Workstation, die Mitglied der Ressourcendomänen ist, und meldet sich an der Account-Domäne an. Die folgende Abbildung (Bild 10) illustriert das Szenario.

Bild 10: Anmeldeszenario

Beim Starten der Windows NT Maschine erfragt diese per WINS eine Liste der Domain Controller (DC) der Ressourcendomäne. Zunächst wird per Broadcast ein Netlogon-Request gesendet. Falls dieser nicht von einem DC der Ressourcendomänen beantwortet, wird der Netlogon-Request an die DCs der erfragten Liste gesendet. Über einen so genannten „Secure Channel“ mit dem als Ersten antwortenden DC erfolgt die Validierung der Anmeldeinformation.

Die NT Maschine erfragt im Anschluss eine Liste der vertrauten Domänen vom DC der Ressourcendomänen.

Nachdem der Benutzer in der Anmeldemaske die Account-Domäne ausgewählt sowie seine Kennung und sein Kennwort eingegeben hat, erfolgt der Anmeldeprozess des Benutzerkontos. Der NT Client sendet die Anmeldeinformationen zur so genannten „pass-through validation“ an den DC der Ressourcendomäne, mit dem die Maschine über einen Secure Channel verfügt. Der DC der Ressourcendomäne sendet diese Anfrage an einen DC der Account-Domäne (zunächst lokal, dann gerichtet über Secure Channel). Die validierten Anmeldeinformationen werden über den DC der Ressourcendomäne an den NT Client zurückgeliefert. Dieser öffnet nun eine direkte Verbindung zum DC der Account-Domäne, um dort das Logon-Script, Systemrichtlinien oder Benutzerprofil zu laden.

Ergänzend ist noch folgender Anmeldeprozess zu beachten: Verbindet sich der Benutzer zu Ressourcen (z.B. Dateiablagen unter der Freigabe eines File Servers, z.B. net use), muss der File Server die Anmeldeinformation überprüfen, indem er erneut die Domain Controller kontaktiert.

3.4.2.10 Single Sign On

Das Domänenkonzept von Windows NT ermöglicht quasi ein Single Sign On (einmalige Anmeldung) innerhalb der Microsoft Produktpalette. Der Anwender meldet sich einmalig an seiner Windows NT Workstation an und kann dann, sofern die Ressourcen bzw. die Serversysteme Mitglied der eigenen oder einer vertrauenden Domäne sind, auf Dienste wie

- File- und Print Services
- Exchange
- SQL
- Intranet (Web, Internet Information Server)

zugreifen.

Drittthersteller von Software können ihre Produkte so implementieren, dass die einmalige Anmeldung erhalten bleibt. In der Regel müssen sie aber ihre Anwendungen auf Windows NT 4 Servern bereitstellen, die Mitglied einer Domäne sind.

3.4.2.11 Richtlinien

In Windows NT Domänen können Richtlinien erlassen werden,

- wie mit Kennwörtern umgegangen werden soll (Laufzeit, Mindestlänge, wiederholte, falsche Kennworteingabe
- welche Privilegien (Benutzerrechte) Benutzer oder Gruppen haben sollen (Ändern der Systemzeit, Lokale Anmeldung etc.)

3.4.2.12 Auditing

In Windows NT Domänen kann ein Auditing (Überwachen) der erfolgten Zugriffe bzw. der Zugriffsversuche eingeschaltet werden. Auf diese Weise können z.B.

- das An- und Abmelden
- das Verwenden von Benutzerrechten
- die Benutzer- und Gruppenverwaltung
- Änderungen der Sicherheitsrichtlinien

überwacht werden.

3.4.2.13 Smart Card (Starke Authentifizierungsmechanismen)

Für Windows NT 4 und Windows 9x sind die so genannten „Smart Card Base Components“ erschienen, mit deren Hilfe Windows-Anwendungen mit Smart Card Funktionalität von Drittherstellern erstellt werden können.

Lösungen zur strengen Authentifizierung werden von Drittherstellern angeboten.

3.4.3 Ablösende Migration – Linux, Samba und OpenLDAP

Bei der Betrachtung einer ablösenden Migration sind vor allem auch die Anforderungen an einen Authentifizierungsdienst in einer heterogenen Systemumgebung mit Linux- und Windows-Systemen zu berücksichtigen. In diesem Zusammenhang steht verständlicherweise die Nutzung eines Verzeichnisdienstes, auch mit Blick auf Active Directory ab Windows 2000, im Vordergrund. Außerdem hat sich die nachfolgend betrachtete Kombination von Linux, Samba und OpenLDAP schon vielfach und lange vor Active Directory als Authentifizierungs-Lösung bewährt. Daher ist eine klare Trennung bei der Betrachtung des Verzeichnisdienstes als Integrationsdienst und als Teil des Authentifizierungsdienstes nur schwerlich möglich. (Ausführlich dazu siehe Kapitel 3.7)

3.4.3.1 Authentifizierung mit Linux / OpenLDAP und Samba

Samba kann Windows-Clients ähnliche Funktionalitäten wie ein Windows NT-basierter primärer Domänencontroller (also u.a. File-, Print- und Authentifizierungsservices) zur Verfügung stellen. Als Datenbank für Benutzerkonten kann Samba dabei auf OpenLDAP als Verzeichnisdienst zurückgreifen. Insofern stellt die Kombination Samba/OpenLDAP eine Art Mischform zwischen Windows NT-Domänen und Active Directory dar. Aus der Sicht von Windows-Clients handelt es sich um eine Windows NT-Domäne (die frühestens 2005 erscheinende Version Samba 4 wird sich in Richtung der Windows Clients wie ein Active Directory Domänencontroller präsentieren). Hinsichtlich der Administration von Benutzer-, Gruppen- und Host-Informationen geht es jedoch um eine vollständig verzeichnisdienstbasierte Lösung mit allen daraus resultierenden Vorteilen. Insbesondere entfällt bei einer Samba/OpenLDAP-basierten Lösung das von Windows NT bekannte Skalierungsproblem, das oft die Aufteilung einer Infrastruktur in unterschiedliche Domänen erforderlich macht.

3.4.3.2 Passwort-Synchronisation

Bei Verwendung von Linux/OpenLDAP als Verzeichnisdienst für Windows-Clients in Verbindung mit Samba findet die Authentifizierung der Windows-Clients über das NTLM-Protokoll statt. Darum müssen im Verzeichnis die gleichen verschlüsselten Passwörter gespeichert werden wie in der SAM-Datenbank unter Windows NT/2000/2003. Mit dieser qualitativen Einschränkung (keine Kerberos Authentifizierung für Windows 2000/XP Clients) ist es somit möglich, auf der Basis von Linux, OpenLDAP und Samba eine vollwertige Authentifizierung für Windows-Clients aufzubauen.

Dabei scheint es zunächst problematisch zu sein, dass UNIX- und Linux standardmäßig einen anderen Algorithmus zur Passwort-Verschlüsselung verwenden als Windows NT/2000. Es ist deswegen bei einer OpenLDAP/Samba-basierten Lösung notwendig, UNIX- und Windows-Passwörter nebeneinander im LDAP-Verzeichnis zu speichern und miteinander zu synchronisieren. Aus technischer Sicht ist dies tatsächlich jedoch weniger problematisch, denn Samba kann so konfiguriert werden, dass es bei einer Passwort-Änderung vom Windows-Client aus auch das UNIX-Passwort ändert. Und umgekehrt können UNIX-Programme

über den PAM- (Pluggable Authentication Module) Mechanismus so eingerichtet werden, dass sie auch das Windows-Passwort ändern, wenn das UNIX-Passwort gewechselt wird. Durch richtige Konfiguration stellt die Passwort-Synchronisation somit kein Problem dar.

Die Authentifizierung von UNIX-basierten Diensten kann darüber hinaus, ebenso wie mit Active Directory, über Kerberos erfolgen. Dazu stehen mit „MIT Kerberos“ und „Heimdal“ zwei gleichwertige Kerberos-Implementierungen für Linux zur Verfügung. Die Heimdal-Implementierung kann seine Benutzer- und Passwortdatenbank zusammen mit den übrigen Benutzerinformationen ebenfalls im Verzeichnis speichern. Bei der Verwendung von Kerberos kann die Passwort-Synchronisation ebenfalls über die aufgeführten Mechanismen gewährleistet werden. (Eine ähnliche Passwort-Synchronisation muss intern auch von Active Directory geleistet werden, um sowohl die Anmeldung über Kerberos als auch von älteren Clients über NTLM zu gewährleisten.)

3.4.3.3 Vertrauensstellungen

Samba 3.0 unterstützt die von Windows NT bekannten Vertrauensstellungen. Diese können sowohl zwischen Windows- und Samba-Domänen als auch zwischen zwei Domänen, die beide auf Samba basieren, eingerichtet werden.

3.4.3.4 WINS-Dienst

Samba verfügt über einen eingebauten WINS-Service. Mit Samba 3.0 steht auch ein Programm zur WINS-Replikation zur Verfügung. Dieses Programm gilt jedoch als noch nicht ausreichend getestet.

3.4.3.5 Einschränkungen bei der Verwendung von OpenLDAP und Samba

Wie bereits erwähnt, entspricht Samba aus der Sicht von Windows-Clients einem Server auf der Basis von Windows NT. Das bedeutet, dass die mit Active Directory neu eingeführten Eigenschaften zur Verwaltung von Windows Clients nicht zur Verfügung stehen. Insbesondere werden Group Policy Objects (GPOs) und die Softwareverteilung via Active Directory nicht unterstützt. In der Praxis ist es allerdings oft völlig ausreichend, diese Features durch andere Techniken zu ersetzen.

GPOs

Samba unterstützt die so genannten System Policies, mit denen sich Registry-Einstellung für Benutzer, Benutzergruppen und Client-Computer festlegen lassen. Über Systempolicies kann ein Großteil der mit GPOs verfügbaren Einstellungen ebenfalls vorgenommen werden (Einschränkungen in der Funktion der Windows-Oberfläche, Auswahl ausführbarer Programme usw.). Die Systemrichtlinien können dynamisch mit dem in Samba integrierten Werkzeug „editreg“ erstellt werden.

Außerdem lassen sich in einer Samba-basierten Umgebung lokale Policies verwenden, mit denen prinzipiell dieselben Einstellungen vorgenommen werden können wie mit GPOs. Weil lokale Policies einfach im Dateisystem abgelegt wer-

den, können diese leicht von einem Prototypen auf eine große Anzahl von Clients synchronisiert werden.

Softwareverteilung

Die mit Active Directory angebotenen Funktionen zur Softwareverteilung beschränken sich auf Software, die in Form von MSI-Paketen vorliegt. In der Praxis wird meist eine umfassendere Softwareverteilungslösung gewählt. Hier stehen eine Reihe kommerzieller Lösungen zur Verfügung, die auch ohne Active Directory funktionieren und oft sogar Linux als Basisbetriebssystem verwenden.

Samba unterstützt serverbasierte Profile. Dadurch lassen sich auch Pflichtprofile einrichten, mit denen Benutzern die Konfiguration von Benutzeroberfläche und Anwendungen vorgeschrieben werden kann.

Mit Hilfe von Anmelde-Skripten lassen sich eine Reihe von weiteren Host-, Gruppen- und Benutzer-spezifischen Einstellungen auf windowsbasierten Clients vornehmen.

3.4.3.6 Kombination von OpenLDAP und Active Directory

Dort, wo auf die Features von Active Directory nicht verzichtet werden kann, ist es möglich, Benutzer- und Gruppendaten aus OpenLDAP in das Active-Directory zu replizieren. Benutzer und Gruppen müssen dann weiterhin nur im OpenLDAP-Verzeichnis gepflegt werden, stehen aber auch im Active Directory zur Verfügung, so dass die entsprechenden Eigenschaften (wie etwa GPOs) genutzt werden können und der Single-Point-of-Administration erhalten bleibt. Dabei kann Windows so konfiguriert werden, dass für beide Teile der Umgebung ein gemeinsamer (linuxbasierter) Kerberos-Server genutzt werden kann. Allerdings ist dies mit der Einschränkung verbunden, dass Windows 95/98/NT basierte Systeme sich dann nicht mehr gegen Active Directory/Kerberos authentifizieren können. In einer solchen Konstruktion wird deswegen die Authentifizierung dieser Clients gegen Samba/OpenLDAP empfohlen.

3.4.3.7 Tools zur Migration von Windows NT nach Samba/OpenLDAP

Mit Hilfe Samba eigener Werkzeuge ist es möglich, die Benutzerdatenbank eines vorhandenen windowsbasierten Domänencontrollers auszulesen und in ein OpenLDAP-Verzeichnis zu schreiben. Mit diesem Verfahren kann die Migration für Benutzer und Client-Systeme vollkommen transparent geschehen; es ist dann keine Neu-Aufnahme der Clients in die migrierte Domäne mehr notwendig und die Benutzer können ihre unter NT verwendeten Login-Name/Passwort-Paare weiterverwenden.

Während der Migration sollten zunächst alle Dienste, mit Ausnahme der Authentifizierung, von den Domänencontrollern entfernt und auf Member-Servern migriert werden. Im nächsten Schritt können dann die Windows NT basierten Domänencontroller nach Samba/OpenLDAP migriert werden. Die windowsbasierten Member-Server können dann für eine Übergangszeit auch in der nun Sam-

ba/OpenLDAP basierten Domäne weiterverwendet und langsam nach Samba migriert werden.

3.4.3.8 PDC und BDCs in einer Samba-Domäne

Aus Gründen der Kompatibilität zu Windows NT Domänen unterstützt Samba ebenfalls das Konzept von PDC und BDCs. Diese Unterstützung beschränkt sich jedoch darauf, dass Samba-Server sich, je nach Konfiguration, gegenüber Windows Clients als PDC bzw. BDC ausgeben. Samba selbst unterstützt keine Replikation der SAM-Datenbank zwischen PDC und BDC. In Verbindung mit der Speicherung der SAM in einem LDAP-Verzeichnis kann die Replikation jedoch von OpenLDAP übernommen werden. Dabei hat der als PDC konfigurierte Samba-Server üblicherweise schreibenden Zugriff auf den OpenLDAP-Master-Server, so dass er Änderungen an der Benutzerdatenbank vornehmen kann. Die BDCs werden so konfiguriert, dass sie nur lesend auf einen OpenLDAP-Slave-Server zugreifen, der typischerweise auf dem gleichen Rechner ausgeführt wird, wie der Samba-BDC. Wird nun über den PDC eine Änderung an der SAM-Datenbank vorgenommen, schreibt dieser die Änderung in das LDAP-Verzeichnis. Von dort wird die Änderung per LDAP-Replikation auf die BDCs übertragen, so dass diesen nun ebenfalls die veränderte Datenbank zur Verfügung steht.

In einer Windows NT Domäne wird außerdem der Inhalt des Netlogon-Shares (auf dem sich u.a. Policies und Logon-Scripte befinden) synchron gehalten. Dies kann unter Linux beispielsweise mit dem Programm rsync realisiert werden.

3.4.3.9 Samba als Mitglied einer Active Directory Domäne

Samba ist außerdem in der Lage, Kerberos-Tickets eines Active Directory Servers zur Authentifizierung zu verwenden und Benutzer-spezifische Informationen aus AD über das im Samba-Paket enthaltene Programm winbind auch unter Linux verfügbar zu machen. Das bedeutet, dass Samba als vollwertiger Member-Server in AD-Domänen eingesetzt werden kann.

3.4.3.10 Administrationswerkzeuge

Die Benutzer- und Gruppenverwaltung in einer Samba/OpenLDAP-basierten Domäne kann mit den Verwaltungstools von Windows NT (usrmgr.exe) geschehen. Allerdings lassen sich damit nicht die besonderen Vorteile der verzeichnisdienstbasierten Lösung nutzen (z.B. unterschiedliche Berechtigungsebenen, verschachtelte Verzeichnisstruktur), weil diese Features von Windows NT nicht unterstützt werden. Bezüglich der Administrationswerkzeuge für OpenLDAP wird auf Kapitel 3.7.4.7 verwiesen.

3.4.4 Fortführende Migration

3.4.4.1 Windows 2000

Hinsichtlich der Anmeldedienste trifft es nicht zu, dass Windows 2000 lediglich ein „Update“ des Betriebssystems darstellt. Nicht nur der Aktualisierungs- bzw.

Installationsprozess ist umfangreich und komplex sondern auch der grundlegende Architekturwechsel hin zum „Active Directory Service“.

Es wird an dieser Stelle des Leitfadens davon abgesehen, den Anmeldedienst von Windows 2000 losgelöst vom Thema Active Directory und damit vom Thema Verzeichnisdienst zu beschreiben. Hier liegen die gleichen Probleme hinsichtlich einer klaren Abgrenzung von Active Directory als Infrastrukturdienst sowie als Teil des Authentifizierungsdienstes vor. Es sei daher auch hier auf das Kapitel 3.7.5 verwiesen, wo ebenfalls der Nachfolger Windows Server 2003 untersucht wird.

3.5 Netzwerkdienste

3.5.1 Überblick

Im Ergebnis der technischen Detailbetrachtungen, die nachfolgend aufgeführt sind, ist festzuhalten, dass eine Migration problemlos möglich ist. Sowohl in migrieren heterogenen als auch homogenen (vollständig ablösende Migration oder fortführende Migration) Systemlandschaften sind keine Einschränkungen zu erwarten.

3.5.2 Ausgangslage – Netzwerkdienste unter Windows NT

In diesem Unterabschnitt wird auf die Netzwerkdienste

- WINS
- DNS
- DHCP

eingegangen. Es wird bei Bedarf zwischen Client- und Serversystemen unterschieden.

Im erweiterten Sinne können auch die Dienste

- RAS (Remote Access Service) und Routing
- Web Proxy
- SNA Gateway

als Netzwerkdienste betrachtet werden. Microsoft sieht hierfür separate Serverprodukte oder Zusatzprodukte (z.B. SNA Server 4.0 oder Proxy Server 2.0) vor. Sie werden in diesem Unterabschnitt nicht behandelt.

Stattdessen wird an dieser Stelle nur kurz auf Neuerungen bei den genannten Netzwerkdiensten eingegangen, die mit der Einführung von Windows 2000 verbunden sind.

3.5.2.1 Windows Internet Name Service (WINS)

Microsoft Windows Internet Name Service (WINS) ist ein Dienst, der auf den Betriebssystemen Windows NT 4 Server installiert werden kann.

WINS ist ein RFC-konformer Dienst, der die Namensauflösung von NetBIOS Namen in eine IP Adresse ermöglicht und zugleich ein Serverdienst, der die NetBIOS Namensauflösung mittels

- Broadcast
- lokal, gespeicherter LMHOSTS-Datei

überflüssig macht.

WINS ermöglicht somit eine Namensauflösung von NetBIOS-Namen über IP Subnetze hinaus.

WINS ist sowohl dynamisch als auch statisch einsetzbar. Dynamisch bedeutet, dass die WINS-Clients sich selbst dynamisch eintragen können. Statisch heißt, dass Administratoren Namen und deren IP-Adressen manuell eintragen.

WINS speichert seine Daten in einer Datenbank (Jet-Engine, wins.mdb), deren Inhalt von mehreren WINS Servern miteinander abgeglichen werden kann. Dafür werden die WINS Server als so genannte „Push-„ und/oder „Pull-Partner“ konfiguriert. Die Inhalte werden nach dem Multi-Master-Prinzip geschrieben. D.h. jeder WINS Server kann Einträge vornehmen.

Zudem existiert die Möglichkeit, einen WINS-Proxy einzusetzen. Ein Rechner, der einen WINS-Proxy darstellt, hält selbst keine Datenbank, nimmt Anfragen von Clients entgegen und leitet diese an einen vollwertigen WINS Server weiter.

Sämtliche bisher erschienenen Windows Betriebssysteme (Windows 9x bis Windows XP und sämtliche Serverbetriebssysteme) können einen WINS Client darstellen. Der WINS Client selbst kann anhand seines so genannten Knotentyps konfiguriert werden, ob und wie er NetBIOS-Namen auflösen soll.

Der NetBIOS Namensraum ist ein flacher Namensraum und beschränkt sich nicht nur auf Rechnernamen, er umfasst auch Benutzernamen, Dienste, Namen von Windows Domänen oder Windows Arbeitsgruppen etc.

Die folgende Tabelle zeigt in einer Übersicht, die NetBIOS-Namenstypen, die anhand des 16. Byte des NetBIOS Namen identifiziert werden können.

Es wird zwischen eindeutigen (unique) Namen und Gruppennamen unterschieden. Gruppennamen können von mehreren Rechnern gleichzeitig verwendet und somit eingetragen werden.

Die folgende Tabelle zeigt die eindeutigen Kennzeichnungen.

Tab. 17: Eindeutige Kennzeichnungen NetBIOS-Namen

16.Byte	kennzeichnet eindeutig
<00>	*den NetBIOS Namen des Computers*.
<03>	den Nachrichtendienst, sowohl für den Computer als auch den angemeldeten Benutzer
<1B>	den Domain Master Browser (Computersuchdienst), der vom PDC einer Domäne bereitgestellt wird.

16.Byte	kennzeichnet eindeutig
<06>	einen RAS Dienst (Remote Access Service) auf einem Computer
<1F>	einen NetDDE Dienst auf einem Computer
<20>	den Serverdienst eines Computers (insbesondere wichtig bei Ordnerfreigaben).
<21>	einen Computer mit RAS Client
<BE>	einen Netzwerkmonitoragenten (network monitor agent)
<BF>	einen Computer mit dem so genannten „network monitor utility“

Die folgende Tabelle zeigt die Kennzeichnungen, die von mehreren verwendet werden können.

Tab. 18: Mehrwertige Kennzeichnungen NetBIOS-Namen

16.Byte	kennzeichnet mehrwertig
<1C>	einen Namen einer Domäne
<1D>	den Namen der Master Browser
<1E>	einen normalen Gruppennamen
<20>	einen speziellen Gruppennamen (genannt die Internet group
MSBROWSE,	anstatt eines einzigen 16. Bytes, kann “_MSBROWSE_,” an einen Domänennamen angehängt werden, damit die Domäne anderen Master Browser bekannt gemacht werden kann

3.5.2.2 Domain Name System (DNS)

Domain Name System (DNS) ist ein Dienst, der auf den Betriebssystemen Windows NT 4 Server installiert werden kann. Er unterstützt die RFCs 1033, 1034, 1035, 1101, 1123, 1183 und 1536 und ist kompatibel zur Berkeley Internet Name Domain (BIND) Implementation.

DNS von Windows NT 4 Server unterstützt BIND in der Version 4.9.4.

DNS ist der Internetstandard, der es unter anderem ermöglicht, innerhalb eines hierarchischen Namensraums Rechnernamen in eine IP Adresse und auch umgekehrt (Reverse Lookup) aufzulösen. Die Verwendung eines DNS Servers macht die Verwendung von lokal gespeicherten Einträgen in der Datei HOSTS überflüssig.

Die Hierarchie des Namensraums macht sich in der Notation der Namen durch das Trennzeichen „.“ bemerkbar. Der so genannte „vollqualifizierte“ Name (Fully Qualified Domain Name, FQDN) besteht aus zwei Teilen: der erste Teil bis zum ersten Punkt kennzeichnet den Hostnamen, der zweite Teil die DNS Domäne. Beispiel: computer1.microsoft.com beschreibt den Rechner namens computer1 in der DNS Domäne microsoft.com. Es ist nicht zwingend notwendig, dass der FQDN zwingend aus drei Teilen bestehen muss. Als zulässige Zeichen in FQDN sind die Zeichen a bis z, A bis Z und das Minuszeichen anzusehen.

Da DNS ein Internetstandard ist, ist keine freie Wahl des Domänennamens möglich. Die Domänen müssen bei den aktuellen nationalen oder internationalen

Verwaltungseinrichtungen registriert werden. Ist der DNS Namensraum allerdings nur innerhalb der eigenen Organisation (Unternehmen) sichtbar, können auch nicht registrierte Namen zum Einsatz kommen. Es sollten entweder registrierte Namen bzw. Zonen zur Anwendung gelangen, die nicht im Internet verwendet werden. So wird vermieden das für andere Organisationen bzw. Personen registrierte Zonen verwendet werden.

DNS verfügt über Mechanismen, die es ermöglichen, die zugrunde liegende Datenbank zu partitionieren, also auf verteilte Umgebungen anzupassen. Zum einen kann die Namensauflösung für spezielle Domänen delegiert werden, zum anderen können über die Erstellung von Zonen die Replikation (Zonentransfer) und die Verwaltung gesteuert werden.

Die Implementation unter Windows NT 4 ist dahingehend mit BIND 4.9.4 konform, dass DNS rein statisch arbeitet (also keine dynamischen Eintragungen unterstützt) und nur im primären Server einer Zone Änderungen vorgenommen werden können (Single Master Prinzip).

Besonderheit der DNS Implementation unter Windows NT 4 ist die Möglichkeit, den DNS Dienst zu veranlassen, zusätzlich einen WINS Server zur Namensauflösung heranzuziehen.

DNS unterstützt neben den Einträgen für Rechnernamen noch weitere Eintragstypen (resource records). Die folgende Tabelle zeigt eine Übersicht der in Windows NT unterstützten DNS Resource Record Typen.

Tab. 19: Übersicht der unterstützten DNS Resource Record Typen

Record Typ	Kurzbeschreibung
A	Adresseintrag (klassischer Eintrag für einen Host, der in eine IP Adresse aufgelöst werden soll)
AFSDB	Spezieller Eintrag für das Andrew File System (AFS)
CNAME	Alias (oder canonical name)
HINFO	Spezieller Eintrag für Hardware Informationen gem. RFC 1700.
ISDN	Eintrag für ISDN (Integrated Services Digital Network) in Zusammenspiel mit dem Typ RT (route through)
MB, MG, MINFO, MR	Spezieller Einträge für Mailboxen, Mailgruppen, Mailboxinformationen
MX	Eintrag für das Mailrouting via SMTP (Simple Message Transfer Protocol)
NS	Eintrag für einen DNS Server (name server) einer DNS Domäne.
PTR	Reversiver Adresseintrag (pointer resource record), der eine IP Adresse in einen Hostname auflöst
RP	Eintrag für die verantwortliche Person einer speziellen DNS Domäne
RT	The route through resource record specifies an intermediate host that routes packets to a destination host. The RT record is used in conjunction with the ISDN and X25 resource records. It is syntactically and semantically similar to the MX record type and is used in much the same way.

Record Typ	Kurzbeschreibung
SOA	Eintrag für den primären DNS Server (start of authority)
TXT	Eintrag für Textinformationen
WINS	Eintrag für die IP Adresse für WINS Server, die zusätzlich zur Vorwärts-auflösung verwendet werden sollen
WINS_R	Eintrag den Reverse Lookup via WINS Server
WKS	Eintrag für well-known service
X.25	Eintrag für eine X.121 Adresse

Sämtliche bisher erschienenen Windows Betriebssysteme (Windows 9x bis Windows XP und sämtliche Serverbetriebssysteme) können einen DNS Client darstellen. Systeme mit Windows 2000 oder höher unterstützen als Client auch dynamisches DNS (DDNS). Zu DDNS siehe Kapitel 3.5.2.3.

3.5.2.3 Dynamic Host Configuration Protocol (DHCP)

DHCP (Dynamic Host Configuration Protocol) ist der Industriestandard zur dynamischen IP Konfiguration von Computern oder anderen TCP/ IP Netzwerkgeräten (z.B. Netzwerkdrucker). DHCP basiert auf den RFCs 1533, 1534, 1541 und 1542.

Die Implementation in Windows NT 4 Server unterstützt die Optionen gem. RFC 1541, die in der folgenden Tabelle abgebildet sind. Die fett dargestellten Optionen sind diejenigen Optionen, die von DHCP-Clients bis Windows NT 4 genutzt werden.

Tab. 20: DHCP-Optionen

Nr.	Optionsname	Erklärung
0	Pad	
255	End	
1	**Subnet mask**	Subnetzmaske
2	Time offset	
3	**Router**	IP Adresse des Standard-Router (Gateway)
4	Time server	
5	Name servers	
6	**DNS servers**	IP Adressen der DNS Server
7	Log servers	
8	Cookie servers	
9	LPR servers	
10	Impress servers	
11	Resource Location servers	
12	Host name	
13	Boot file size	
14	Merit dump file	
15	**Domain name**	DNS Suffix des Clients
16	Swap server	

Nr.	Optionsname	Erklärung
17	Root path	
18	Extensions path	
19	IP layer forwarding	
20	Nonlocal source routing	
21	Policy filter masks	
22	Max DG reassembly size	
23	Default time-to-live	
24	Path MTU aging timeout	
25	Path MTU plateau table	
26	MTU option	
27	All subnets are local	
28	Broadcast address	
29	Perform mask discovery	
30	Mask supplier	
31	Perform router discovery	
32	Router solicitation address	
33	Static route	
34	Trailer encapsulation	
35	ARP cache timeout	
36	Ethernet encapsulation	
37	Default time-to-live	
38	Keepalive interval	
39	Keepalive garbage	
40	NIS domain name	
41	NIS servers	
42	NTP servers	
43	Vendor-specific information	
44	**WINS/ NBNS servers**	IP Adressen der WINS Server
45	NetBIOS over TCP/ IP NBDD	
46	**WINS/ NBT node type**	Knotentyp des WINS Clients.
47	NetBIOS scope ID	
48	X Window system font	
49	X Window system display	
51	**Lease time**	Gültigkeitsdauer der Vergabe
58	**Renewal (T1) time value**	Erneuerungsintervall 1
59	**Rebinding (T2) time value**	Erneuerungsintervall
64	NIS + Domain Name	
65	NIS + Servers	
66	Boot Server Host Name	
67	Bootfile Name	
68	Mobile IP Home Agents	

Ferner existiert die Möglichkeit, einen DHCP Relay Agent einzusetzen. Ein Rechner, der einen DHCP Relay Agent Dienst ausführt, hält selbst keine Daten-

bank, nimmt Anfragen von Clients entgegen und leitet diese an einen vollwertigen DHCP Server weiter.

3.5.3 Ablösende Migration – Netzwerkdienste unter Linux

Die infrastrukturbildenden Dienste für TCP/IP-basierte Netzwerke (DNS, DHCP, NTP, Routing, VPN, Filtering) lassen sich durchweg in Open Source Software realisieren. Die umfassende Verfügbarkeit dieser Netzwerkdienste als OSS erklärt sich aus der Entwicklungsgeschichte des Internet. Dieses weltweite Datennetz zeichnet sich dadurch aus, dass alle daran angeschlossenen Computer ein und dieselbe Sprache sprechen. Diese Sprache besteht aus einer ganzen Familie von Protokollen, die unter der Bezeichnung TCP/IP zusammengefasst werden. Damit die Kommunikation zwischen den unterschiedlichsten Systemen weltweit reibungslos funktioniert, muss das „Sprachverständnis“ unbedingt übereinstimmen. Um diese Übereinstimmung zu erreichen, sind die meisten der bei der Internet Engineering Task Force (IETF) formell verabschiedeten Standards für Internetprotokolle durch Open Source Referenzimplementationen unterstützt. Auf Grundlage dieser Referenzen können alle Hersteller unabhängig voneinander vollständig interoperable Software entwickeln. Die Internetprotokolle sind selbst herstellerunabhängig und sowohl in ihren Definitionen als auch in ihren Open Source Implementationen offene Standards. Dieser besondere Charakter der Internetprotokolle hat entscheidend dazu beigetragen, dass sich TCP/IP gegenüber den gleichzeitig am Markt befindlichen proprietären Netzwerkprotokollen durchgesetzt hat.

Auch wenn im lokalen Netz die Anforderungen bezüglich Interoperabilität wegen der begrenzten Anzahl beteiligter Systeme überschaubar bleiben, ist die Bewahrung der offenen Standards von essenzieller Bedeutung. Insbesondere bei herstellerspezifischen Änderungen bzw. Erweiterungen von Standards ist regelmäßig die Gefahr eines „Vendor Lock-In“ gegeben: einerseits wird die Bindung an diesen Hersteller bis hin zur Abhängigkeit gefestigt, andererseits geht die Definitionsmacht bezüglich der Fortentwicklung und der Interoperabilität von Fremdsystemen, jedenfalls im Wirkungsbereich der Erweiterung, auf den Hersteller über.

Vor diesem Hintergrund sollte in jedem Fall geprüft werden, ob die mit einer herstellerspezifischen Erweiterung eines Standards versprochenen Verbesserungen auch mit einer langfristigen Perspektive vereinbar sind. Die Verwendung der seit langer Zeit existierenden und bewährten Referenzimplementationen können möglicherweise nicht mit jedem Feature aufwarten, sie bieten aber die Gewähr für dauerhafte Interoperabilität mit allen netzwerkfähigen Systemen.

3.5.3.1 Domain Name System (DNS)

Die Referenzimplementation des in einer ganzen Reihe von RFC-Dokumenten definierten Standards für das Domain Name System ist BIND (Berkeley Internet Name Domain), das vom Internet Software Konsortium herstellerunabhängig weiterentwickelt und gepflegt wird. Die aktuelle Version ist 9.3.x, die Versionslinie 8.4.x macht einen großen Teil der installierten Basis von DNS-Servern aus und

wird vom ISC weiter gepflegt. Die Versionen 4.9.8 und älter sollten nicht mehr eingesetzt werden.

Bind9 unterstützt unter anderem dynamisches DNS (DDNS), DNSSEC und Ipv6.

Die Anbindung von BIND 9 an fremde Datenquellen für die Zoneninformationen ist einerseits über ein umfangreiches BackEnd Database Interface möglich, andererseits gibt es ein zusätzliches vereinfachtes Interface (SDB) mit dem beispielsweise ein nur-lesender Zugriff auf LDAP oder SQL Datenbanken realisiert werden kann. Diese Anbindungen selbst sind jedoch nicht Bestandteil des BIND Softwarepakets. So existieren beispielsweise für die LDAP-Anbindung sowohl SDB Implementation als auch vordefinierte Objektklassen, mit denen eine solche Anbindung realisiert werden kann.

Der ISC bind kann auch mit Windows NT / W2k betrieben werden. Insbesondere unterstützt BIND 9 auch die dynamische Aktualisierung von Service-Records und kann damit entsprechende Dienste für W2K Server leisten.

3.5.3.2 Dynamic Host Configuration Protocol (DHCP)

Die Referenzimplementation des DHCP wird ebenfalls vom ISC weiterentwickelt und gepflegt. Das Protokoll und die Software haben folgende Aufgaben bzw. Möglichkeiten:

- Automatische Zuweisung von IP-Adresse und Rechnernamen an Clients. DHCP erlaubt sowohl die Zuweisung fester IP-Adressen (Anhand der MAC Adresse) als auch die dynamische Zuweisung einer freien Adresse aus einem festgelegten Adressbereich.
- Automatische Übermittlung von Informationen über die Netzwerkinfrastruktur. Zum Beispiel kann über DHCP der Domänenname und der Nameserver, die Default-Route und die Netzmaske zentral verwaltet an alle Clients verteilt werden.
- Darüber hinaus lassen sich eine große Zahl fest definierter optionaler Felder sowie frei definierbare Informationen zur Host-Konfiguration durch den dhcpd ausliefern. Unter anderem können auch sämtliche von Windows-Clients verwertbaren Optionen durch den ISC dhcpd übermittelt werden.
- Zusätzlich kann der dhcpd auch die Rolle eines bootpd übernehmen und so einem Client alle für das Booten über Netz erforderlichen Informationen übermitteln.

Der ISC dhcpd ermöglicht bezüglich aller auszuliefernden Informationen sowohl die Verwaltung von individuellen Clients als auch die zusammenfassende Konfiguration für Klassen und Subnetze. In der Konfiguration des ISC dhcpd ist außerdem die bedingte Zuweisung von Host-Konfigurationsdaten durch IF-Anweisungen möglich.

Der dhcpd kann in einer Failover-Konfiguration sowohl für Load-Balancing als auch zur HV betrieben werden. Die dynamisch verwalteten IP-Bereiche werden dann zwischen den sich gegenseitig ersetzenden Servern koordiniert.

Die Konfiguration des ISC dhcpd geschieht im traditionellen UNIX-Stil durch eine ASCII Konfigurationsdatei. Es existiert ein Patch, mit dem die Konfiguration des ISC-DHCP-Servers dynamisch aus einem LDAP-Repository bezogen werden kann. Die Implementation folgt dem IETF Draft zum LDAP Schema für DHCP.

3.5.3.3 Windows Internet Name Service (WINS)

Die Namensauflösung für Windows-Dienste und -Rechner wird nach einer OSS-Migration durch den nmbd vom Samba-Paket übernommen. Dabei können einerseits die bei Windows üblichen broadcastbasierten Browserdienste sowohl als Client als auch als lokaler oder domänenweiter Master Browser geleistet werden. Andererseits kann der nmbd aber auch als WINS die Koordinierung der Browser über die Grenzen von Netzsegmenten hinweg leisten, die üblicherweise mit Routern verbunden sind, die keine Broadcasts durchlassen.

3.5.3.4 Network Time Protocol (NTP)

Für viele Netzwerkanwendungen ist ein hoher Grad an Synchronisation erforderlich. Unter Verwendung des Network Time Protocol lassen sich die Uhren der Rechner im lokalen Netz im Bereich von Mikrosekunden synchronisieren. Bei einer dauerhaften Internetverbindung kann die Referenzzeit im Bereich von Millisekunden mit dem amtlichen Normal synchron gehalten werden. Alternativ lassen sich auch (unter anderem) DCF77 und GPS als Bezugsquellen für das Zeitnormal verwenden.

Die Referenzimplementation des Standards wird vom Network Time Protocol Project weiterentwickelt und gepflegt. Die Software kann auch unter Windows NT eingesetzt werden.

3.5.4 Fortführende Migration – Netzwerkdienste unter Windows 2000

In den folgenden Absätzen werden kurz die Neuerungen hinsichtlich der oben genannten Netzwerkdienste beschrieben, die mit der Einführung von Windows 2000 einhergehen.

3.5.4.1 WINS

Hinsichtlich **WINS** bietet Windows 2000 keine architektonischen Neuerungen. In Windows 2000 wird lediglich das Management der WINS Datenbank verbessert.

3.5.4.2 DNS

Die größten Änderungen durch die Einführung von Windows 2000 hat der DNS Dienst erfahren. Der Hauptgrund dafür ist, dass Windows 2000 Active Directory als primäre Namensauflösung DNS benutzt bzw. ohne DNS nicht funktionieren würde. Active Directory verwendet DNS unter anderem zur Auffindung der Dienste hinsichtlich Anmeldung und Suche (LDAP Service, Global Catalog Service und

Kerberos KDC). Für die Eintragung von Diensten muss das DNS so genannte SRV Records gem. RFC 2052 unterstützen. Da das bisherige DNS statisch funktionierte (Einträge mussten manuell vorgenommen werden), ist in Windows 2000 auch im Hinblick auf den angestrebten, zukünftigen Wegfall von WINS eine dynamische Registrierung implementiert worden: Rechner können ihre A und SRV Records dynamisch eintragen. Die Implementierung folgt dabei dem RFC 2136 (Dynamic Update). Computer mit Windows 2000 und höher können sich selbst dynamisch registrieren (Realisierung im DHCP Client). Windows NT und Windows 9x können das nicht, vielmehr benötigen sie die Hilfe eines Windows 2000 DHCP Dienstes. Das dynamische Registrieren impliziert eine architektonische Änderung der bisherigen DNS Implementierung, in der nur ein DNS Server (der primäre) die Zoneninhalte schreiben kann. Microsoft realisiert ein Multi-Master-Prinzip, indem es DNS ins Active Directory integriert. Die DNS Einträge sind somit Objekte der Datenbank des Active Directory und werden auf diese Weise repliziert. Eine dynamische Registrierung ohne AD-Integration existiert nicht. Die dynamische Registrierung kann durch Sicherheitsmechanismen reglementiert werden, so dass sich nur jene Computer registrieren können, die sich auch authentifizieren können (so z.B. Windows 2000 Clients der zugehörigen Domäne). Windows 2000 unterstützt das so genannte „Secure Update“ gemäß GSS-API laut RFC 2078; die RFCs 2535 (Domain Name System Security Extensions) oder 2137 (Secure Domain Name System Dynamic Update) sind nicht realisiert.

3.5.4.3 DHCP

Hinsichtlich DHCP bietet Windows 2000 einige nennenswerte Neuerungen. Unter Windows 2000 werden die aktuellen RFCs 2131 (Dynamic Host Configuration Protocol, ehemals RFC 1541) und 2132 (DHCP Options and BOOTP Vendor Extensions) unterstützt. Neben dem verbesserten Management werden nun Multicast Scopes, benutzer- und herstellerspezifische DHCP Optionen sowie dynamisches BOOTP unterstützt.

Eine weitere Neuerung ist die Integration von DHCP und DNS innerhalb eines Windows 2000 Netzwerkes. Clients mit Windows NT 4 oder älter unterstützen keine dynamische Registrierung ihrer DNS-Namen im Windows 2000 dynamischen DNS. Sofern diese Clients ihre IP Konfiguration von einem Windows 2000 DHCP Server beziehen, kann der DHCP Server die Registrierung im DNS übernehmen.

Der DHCP-Client von Windows 2000 kann, wenn sich kein DHCP Server in seinem Subnetz befindet, seine IP Konfiguration selbst erstellen. Hierbei werden IP Adressen des Class B Netzes 169.254.0.0 mit der Subnetzmaske 255.255.0.0 verwendet.

3.6 System-Überwachungs- und –Management-Dienste

3.6.1 Überblick

In diesem Kontext ist vorab zu bemerken, dass aufgrund der nur partiell verfügbaren und recht einfachen Systemmanagementwerkzeuge unter Windows NT an vielen Stellen umfassende Werkzeuge von Drittherstellern im Einsatz sind, die z.T. auch für Linux-Systeme verfügbar sind.

Unter Linux gibt es neben vielen Bordmitteln wie cron/at noch weitere COLS-Produkte sowie OSS-Lösungen für die Systemadministration. So steht z.B. Nagios für die Visualisierung und Dienste-Überwachung zur Verfügung. Ein komplexes hochintegriertes System, mit dem alle Systemmanagementaufgaben erledigt werden können, steht derzeit nicht als OSS-Lösung zur Verfügung.

Microsoft hat seine Werkzeugkiste mit der Fortführung seiner Produktlinie ebenfalls erweitert. Hier sind der Microsoft Operations Manager und das Application Center zu nennen.

3.6.2 Ausgangslage Windows

3.6.2.1 Allgemein

Unter Windows NT stehen nur partiell recht einfache Systemmanagementwerkzeuge zur Verfügung. Daher werden hier in weiten Bereichen Systemmanagementlösungen von Drittherstellern eingesetzt. Hierbei handelt es sich entweder um integrierte Gesamtlösungen, die sehr modular aufgebaut aber auch sehr stark aufeinander abgestimmt sind. Dazu zählen u.a. Produkte wie IBMs Tivoli oder HPs OpenView. Daneben gibt es viele Einzellösungen für die Softwareverteilung, das Netzwerkmanagement, das Monitoring von Servern und Netzwerk und viele andere. Die Betrachtung der Ablösung bzw. Fortführung der Lösungen von Drittherstellern ist nicht Bestandteil dieses Leitfadens und wird daher nicht näher untersucht.

Eine Ausnahme bei Microsoft stellt der Systems Management Server dar, der in erster Linie Aufgaben der Softwareverteilung unterstützt. Daher wird dieser im Rahmen der Beschreibung der Ausgangslage umfassender betrachtet.

3.6.2.2 Systems Management Server unter Windows NT 4

Der Systems Management Server (SMS) wurde zeitnah mit dem Erscheinen von Windows NT 4 auf den Markt gebracht. Als Endversion dieser Generation ist SMS in der Version 1.2 anzusehen. Im Jahr 1999 erschien die Version 2.0. Der Funktionsumfang dieser Version wird im Folgenden beschrieben.

SMS integriert mehrere Basisfunktionalitäten, die andere Hersteller ebenfalls vergleichbar in einem integrierten Produkt abdecken. Diese sind:

- Inventarisierung (inventory)
- Fernsteuerung (remote control)
- und Softwareverteilung (software distribution).

Für den Einsatz der Serversoftware wird Windows NT Server 4.0, Service Pack 4 oder höher und Microsoft SQL Server 6.5, Service Pack 4 oder höher benötigt.

SMS 2.0 kann in Großumgebungen mit über 100.000 Clients eingesetzt werden. Da es sich in die Windows Domänenstruktur einbetten lässt, stehen granulare Sicherheitsabstufungen zur Verfügung. SMS unterstützt auch Novell Netware NDS und Bindery-Umgebungen.

SMS 2.0 beinhaltet eine elektronische **Softwareverteilung**, die weitestgehend automatisch Software installiert und auch deinstalliert, ohne dass im Idealfall Arbeiten vor Ort anfallen oder benutzerseitige Fehler entstehen. Die Softwareverteilung kann regelbasiert erfolgen: Durch Hinzufügen bzw. Entfernen von Computern, Benutzern oder Benutzergruppen aus Auflistungen gemäß definierter Kriterien legen die Administratoren die Softwarekonfiguration fest. SMS protokolliert den Status von Softwareinstallationen und Betriebssystemaktualisierungen, so dass die Systemadministratoren darüber informiert sind, ob die Software ordnungsgemäß installiert wurde. SMS installiert unbeaufsichtigt Software ohne benutzerseitigen Eingriff, wobei diese mit Administratorrechten installiert werden kann, auch wenn ein Benutzer mit weniger umfangreichen Rechten am Computer angemeldet ist. NT-basierte Computer müssen dabei nicht angemeldet sein, so dass sich dieses Feature für die Verteilung außerhalb der regulären Geschäftszeit eignet. SMS ermöglicht eine zeitgesteuerte Softwareverteilung an eine beliebige Kombination von Benutzern, Benutzergruppen, TCP/IP-Netzwerksegmenten und Computern. SMS 2.0 ermittelt Verteilungsziele dynamisch auf der Basis von Regeln für Gruppenrichtlinien und kann diese Regeln auf alle Standorte anwenden. Wenn einer Benutzergruppe neue Benutzer beitreten, kann ihnen basierend auf der Richtlinie dieser Gruppe automatisch die richtige Software gesendet werden. Die so genannte **strukturierte Paketverteilung** berücksichtigt die Netzwerktopologie, um Software über langsame Verbindungen effizient zu verteilen. Standortserver fungieren in diesem Fall als Router, die die Software intelligent und strukturiert verteilen. Auf diese Weise verwendet eine Verteilung eine WAN-Verbindung immer nur einmal. SMS 2.0 kann Software mit dem **Courier Sender** mittels CD-ROM oder anderer Medien versenden. Sobald das Medium (z. B. die CD-ROM) beim Benutzer angekommen ist und der Benutzer dieses in sein System eingelegt hat, startet der automatisierte Vorgang. Für das Erstellen von Softwarepaketen wird ein Installationsprogramm mitgeliefert. Damit können die Systemadministratoren Änderungen an Installationspaketen durchführen sowie Skripte schreiben, um Pakete für windowsbasierte Anwendungen zu erstellen. Der **SMS Installer** beinhaltet zusätzlich zu Wrappertechnologien für die Softwareverteilung auch eine Installationsmitschnittfunktion. Der Installer verwendet eine Momentaufnahmetechnologie.

SMS 2.0 kann eine **Inventarisierung** von Hardware und Software durchführen. In einer **CIM-basierten Hardwareinventur** sammelt SMS 2.0 Daten in einem CIM-Format (Common Information Model), das SMS Zugang auf viele verschiedene Quellen, darunter auch Microsoft Win32, SNMP und DMI, ermöglicht. SMS

sammelt umfassende Inventardaten, die mit Hilfe von Optionen gefiltert werden können. Die **Softwareinventur** sammelt genaue Informationen über jede einzelne Anwendung auf jedem Computer. SMS 2.0 sucht nicht in einer vordefinierten Datenbank, sondern in jeder ausführbaren Datei auf einem Clientcomputer nach versionsbezogenen Ressourceninformationen. Die Inventurdaten können als Datenbasis für die regelbasierte Softwareverteilung herangezogen werden.

Die Fernsteuerung (Remote Control) ermöglicht es, dass Anwendungen remote ausgeführt, mit Endbenutzern per Chat-Fenster kommuniziert sowie Computer neu gestartet werden können. Darüber hinaus kann die Bildschirm-, Tastatur- und Maussteuerung übernommen werden.

SMS 2.0 kann hinsichtlich **Netzwerkmanagement** folgendes leisten: Mit Hilfe von SMS können Netzwerktopologie, Clients sowie die verwendeten Betriebssysteme angezeigt und visualisiert werden. SMS erstellt eine Übersichtskarte der Netzwerkserver und -geräte, um Systemadministratoren bei der Netzwerkverwaltung und Fehlerbehebung zu unterstützen. Durch eine Überwachung des Datenverkehrs können Netzwerkprobleme, wie beispielsweise nicht benötigte Protokolle, doppelt vergebene IP-Adressen sowie versuchte unzulässige Internetzugriffe entdeckt werden. Der **Netzwerkmonitor** kann gefundene Ergebnisse automatisch interpretieren.

SMS 2.0 bietet Tools zur Analyse, Überwachung und Steuerung von Anwendungen auf Servern und Arbeitsstationen (**Softwaremessung**). Dabei kann die Programmnutzung nach Benutzer, Gruppe, Arbeitsstation, Zeit oder Lizenzkontingente sortiert verfolgt werden. Zudem können die Nutzung bestimmter Anwendungen bestimmt, Kontingentgrenzen definiert oder auch unerlaubte Anwendungen festgelegt werden. Darüber kann auch die Einhaltung der Regeln auf jedem beliebigen Client oder Server überwacht werden. Die Softwaremessungsprogramme erkennen ebenfalls unterschiedliche Programmversionen und können feststellen, ob Client-Agenten deaktiviert wurden, um einen umfassenden Schutz vor Manipulation zu realisieren. Statistiken zur Softwarenutzung können zur Planung von Softwarelizenzierungen und zur Gebührenerfassung von Abteilungen je nach Nutzung der Anwendungen eingesetzt werden (**Lizenzmanagement**).

Die **Serverüberwachung** erfolgt mittels HealthMon. HealthMon ermittelt Leistungsdaten zu Prozessen in Windows NT Server und Microsoft BackOffice Server. In der HealthMon-Konsole können kritische Schwellwerte oder Schwellwerte für Warnungen festgelegt werden, um ausnahmebasierte Statusinformationen in Echtzeit zu erhalten, die nach Ressourcen auf Systemebene oder nach Microsoft Serveranwendungen und -Prozessen gruppiert werden können.

3.6.3 Ablösende Migration – Linux

Das Systemmanagement für OSS-Betriebssysteme basiert auf der Grundfunktionalität des Multiuser-Netzwerkbetriebssystems. Ein Administrator kann auf jedem Linux/BSD-Rechner, sei es Client oder Server, von seinem entfernten Arbeitsplatz aus wie auf einem lokalen Rechner arbeiten. Die grafische Benutzeroberflä-

che ist durch die systematische Trennung von Server (mit Display, Tastatur und Maus) und Clientsoftware, die über eine Netzwerkverbindung lokal oder aus der Ferne seine Fenster und Zeichen auf dem Display darstellt und Eingaben vom Server entgegennimmt, unter anderem auch hervorragend für die Fernbedienung von Rechnern geeignet. Hinzu kommen die Secure Shell (ssh) und eine reichhaltige Werkzeugkiste mit cron/at zur Zeitablaufsteuerung und mächtigen Kommandozeileninterpretern, Utilities und interpretierten Programmiersprachen zur weitgehenden Automatisierung von Routinearbeiten. Für die Fernsteuerung von OSS-Systemen ist keine weitere Softwareunterstützung erforderlich.

Für das zentralisierte Systemmanagement in heterogenen Netzen stehen auch unter den OSS-Systemen zusätzliche Komponenten zur Verfügung. Am oberen Ende der Skala lässt sich Linux in das Systemmanagement mit Tivoli oder OpenView integrieren. Zwischen diesen selbst nicht zur OSS zählenden Lösungen und dem einfachen Management mit den Betriebssystemwerkzeugen gibt es eine Vielzahl von Möglichkeiten, mit denen jeweils bestimmte Aufgaben des Systemmanagement automatisiert oder unterstützt werden können.

3.6.3.1 Softwaremanagement

Für die Inventarisierung, Verteilung und Aktualisierung sowie das Konfigurationsmanagement für Softwarekomponenten gibt es eine große Vielzahl von Anbietern und Lösungen. Den größten Anteil nehmen dabei kommerzielle Lösungen mit einer zum Teil sehr großen Funktionaltätsbandbreite ein. Hierbei kann zwischen Lösungen unterscheiden werden, die Bestandteil von großen, umfassenden und integrierten Managementlösungen sind, i.d.R. aber auch alleine installiert und genutzt werden können. Hierzu zählen z.B. Radia von Novadigm als Teil von HP OpenView oder der Tivoli Configuration Manager von IBM. Daneben gibt es „allein stehende“ Softwareverteilungstools, wie zum Beispiel ASDIS oder NetInstall. Im Open Source Bereich gibt es inzwischen neben den Paketmanagementsystemen der einzelnen Linuxdistributionen auch einige produktionsfertige integrierte Lösungen wie zum Beispiel Open PC Server Integration (opsi) und m23. Wobei bei den Open Source Lösungen der Umfang an Funktionalitäten und die Komplexität der Systeme bei weitem nicht mit denen der kommerziellen Lösungen zu vergleichen sind, aber die wesentlichen Funktionalitäten abdecken können.

Unterstützte Betriebssysteme

Wenn man eine ablösende Migration betrachtet, steht natürlich die Unterstützung der Verteilung von Software auf Linuxbetriebssysteme im Fokus der Betrachtungen. Hier hat sich seit der Veröffentlichung der ersten Ausgabe des Migrationsleitfadens schon einiges verändert und viele der Hersteller sind derzeit noch dabei, ihre Lösungen auf die Unterstützung von Linuxsystemen zu erweitern. Die Unterstützung von Linux beschränkt sich bei den meisten Herstellern auf die Unterstützung der beiden Distributionen von Red Hat und Novell/Suse. Hierzu gehören Produkte der Tivoli Configuration Manager, Radia von Novadigm als Teil von HP OpenView oder auch Empirum von Matrix42. Da es sich bei diesen Produk-

ten i.d.R. um Produkte handelt, die schon seit längerem auf dem Markt vertreten sind, dürfte klar sein, dass diese auch die meisten Windowsversionen mit Software versorgen können. Dies gilt auch und insbesondere für die kommerziellen Produkte, zu denen die Hersteller keine Aussagen über die unterstützten Distributionen machen sondern hinsichtlich der Softwareverteilung „nur“ angeben, welche Paketformate (wie z.B. RPM und DEB) sie unterstützen. Da es sich bei den meisten Produkten um Client-Server-Lösungen handelt, hängt die wirkliche Verfügbarkeit für eine bestimmte Distribution immer davon ab, in wie weit der Client auf der jeweiligen Distribution installiert werden kann und dort lauffähig ist. Bezogen auf die erweiterten Funktionalitäten, wie Erstinstallation inkl. Hardwareerkennung und Partitionierung, Inventarisierung und Remote Control sagt die Möglichkeit, z.B. RPM-Pakete zu verteilen, nicht sehr viel aus.

Ein wesentlicher Aspekt des Leitfadens und einer ablösenden Migration sind die Möglichkeiten auf Open Source Lösungen umsteigen zu können. An reinen Open Source Lösungen, die als produktionsfähige integrierte Lösungen zur Verfügung stehen, können zumindest zwei aufgeführt werden, auf die weiter unten auch noch näher eingegangen wird. Bei diesen Lösungen handelt sich zum einen um "Open PC Server Integration" (Opsi) der Firma uib[1] und zum anderen um das Open Source Projekt „m23“ [2]. Beide Lösungen stehen unter GPL. Opsi unterstützte bis vor kurzem nur Windows 2000 und XP, seit neuestem sollen auch Linuxsysteme unterstützt werden[3]. m23 dagegen ist eine Softwareverteilung nur für Debiansysteme.

Daneben lassen sich für die meisten Linuxsysteme mit den verfügbaren Open Source Werkzeugen für das Management der Softwarepakete (RPM, APT) sowohl die Inventarisierung als auch die Verteilung bzw. das Update von Software leicht zentralisieren. Insbesondere das Debian Paketmanagement ist hervorragend für ein zentrales Softwaremanagement geeignet, da es mit einer Hierarchie von zentralen Software-Repositories arbeiten kann und über ein sehr robustes Updateverhalten verfügt. Weiterhin ist das Open Carpet Projekt erwähnenswert, welches Basis für das Red Carpet Enterprise System und seit kurzem damit Bestandteil des ZENworks® Linux Management[4] ist (siehe auch Kapitel 2.3.5.3).

Kernfunktionalitäten von Softwareverteilungswerkzeugen

Die meisten der verfügbaren Werkzeuge beschränken sich nicht nur auf die reine Softwareverteilung sondern sehen sich als Clientmanagementsysteme. Diese unterstützen weit mehr Funktionen als die reine Softwareverteilung, wobei es auch bei der reinen Softwareverteilung unterschiedlichste Grade von Komplexität

1 http://www.ubi.de

2 http://m23.sourceforge.net/PostNuke-0.726/html/index.php

3 Leider war nicht festzustellen, in welchem Umfang, d.h. welche Paketformate oder Distributionen mit welchen Funktionen unterstützt werden.

4 http://www.novell.com/products/zenworks/linuxmanagement/quicklook.html

und Ausprägungen gibt. Im Kern aber umfassen fast alle diese Clientmanagementsysteme drei übergeordnete Funktionen:

- Softwareverteilung
- Inventarisierung
- Remote Control

Ziel ist es, mit Hilfe dieser Funktionalitäten die zeit- und personalaufwendige „Turnschuhadmistration“ weitgehend zu eliminieren.

Softwareverteilung

Die Softwareverteilung ist die wichtigste Funktionalität und beinhaltet in vielen Systemen:

- die Erstinstallation der Clients[1]
- die Wiederherstellung von Clients
- das Update- und Patchmanagement
- die Verteilung von Standard- und Fachanwendungen

Bei der Erstinstallation gehen die Hersteller unterschiedlich vor. Entweder arbeitet das System Image-basiert, d.h. für die unterschiedlichen Clienttypen werden Basis-Images erstellt und auf dem Server der Softwareverteilung hinterlegt. Die einzelnen Clients müssen dann den definierten Clienttypen zugeordnet werden. Oder andere Systeme erlauben eine „normale“ Installation des Basissystems, wobei Hardwareerkennung und Partitionierung unterstützt werden.

Eine wichtige Frage bildet in vielen Anforderungsdefinitionen die nach der Flexibilität der Verteilungskriterien. Hintergrund dafür sind die Lizenzkosten, die mit der Installation von Software entstehen. Software, die Lizenzkosten verursacht, sollte aus wirtschaftlichen Gründen immer nur dort zur Verfügung gestellt werden, wo sie zwingend benötigt wird. Neben den wirtschaftlichen Gründen kann es auch Sicherheitsgründe geben, die es erfordern, dass nicht jedem Mitarbeiter jede Software zur Verfügung gestellt wird. Häufig hängt dies von der Zugehörigkeit zu einer Organisationseinheit oder Arbeitsgruppe ab, kann im Einzelfall auch personenabhängig sein. Nun bieten einerseits viele der Softwareverteilungswerkzeuge die Möglichkeit, diese Gruppen (Organisationseinheiten, Arbeitsgruppen, Projektgruppen usw.) entsprechend abzubilden und die Clients, diesen Gruppen entsprechend zuzuordnen. Andererseits werden Organisationseinheiten, Arbeitsgruppen, Personen usw. und auch die Rechner meist schon im Rahmen der Benutzer- und Organisationsverwaltung gepflegt und müssten daher im Softwareverteilungswerkzeug redundant gehalten werden. Hier wäre es wünschenswert, wenn die Softwareverteilungstools entsprechende Schnittstellen zu den anderen Systemmanagementtools zur Verfügung stellten.

[1] Für eine Softwareverteilung werden auch Server als Clients gesehen, die mit Software zu versorgen sind.

Inventarisierung

Die Inventarisierungsfunktion ermöglicht es, über die Hardwareerkennung zu jedem Client die wesentlichen Hardwareinformationen ergänzend zu den vorhandenen Softwareinformationen aufzunehmen und bereitzustellen. Von hohem Interesse sind diese Informationen für den Help-Desk. Geht beim Help-Desk eine Fehlermeldung von einem Mitarbeiter ein, dann ist es von großem Vorteil, wenn der Help-Desk-Mitarbeiter sofort sehen kann, welches Hard- und Software-Profil der Rechner des Mitarbeiters hat, der die Fehlermeldung abgegeben hat. Auch hier ist es von Vorteil, wenn entsprechende Schnittstellen für die Bereiststellung der Inventarinformationen bezogen auf einen Rechner, der wiederum einem Benutzer zugewiesen ist, im Help-Desk zur Verfügung stehen.

Remote Control

Die Remote Control Funktionalitäten erlauben die ferngesteuerte Ausführung von Applikationen für den Transfer von Dateien, zur Problemdiagnose und zur Problembehebung.

Open Source Softwareverteilungssysteme

Opsi ist ein Produkt der Firma uib[1] in Mainz und steht unter GPL. Opsi unterstützte bisher nur die Softwareverteilung auf Windows 2000 und Windows XP Systemen. Nunmehr soll auch die Installation von Linuxsystemen unterstützt werden. Praktische Erfahrungen diesbezüglich gibt es bisher nur im Rahmen von durchgeführten Tests. Opsi bewährt sich allerdings bereits seit Mitte der 90er Jahre in einer Landesverwaltung bei der Softwareverteilung in einer Umgebung von ca. 2000 Windows-PCs[2]. Opsi selbst läuft unter Linux.

Die Funktionalitäten von opsi beschränken sich auf die reine Softwareverteilung mit

- Erstinstallation
- das Update- und Patchmanagement
- die Verteilung von Standard- und Fachanwendungen.

m23

m23[3] ist ein Softwareverteilungssystem für Debian Gnu Linux Systeme, das genau wie Opsi unter GPL steht. m23 ist damit nicht für heterogene Systemumgebungen geeignet, was aber in einer homogenen Debian-Umgebung auch kein Nachteil sein muss. m23 ist wie die meisten Softwareverteilungssysteme ein Client/Server basiertes System und beinhaltet Funktionalitäten wie

[1] http://www.ubi.de

[2] Quelle: http://www.uib.de/www/download/download/opsi2-info.pdf

[3] http://m23.sourceforge.net/PostNuke-0.726/html/index.php

- Erstinstallationen, inklusive Partitionierung und Hardwareerkennung,
- Verteilung von System- und Anwendungssoftware,
- Wiederherstellung von Clients,
- Softwareupdates und
- Inventarisierung (Hardwareerkennung).

Damit deckt m23 die wesentlichen Funktionalitäten ab, die auch von den meisten kommerziellen Systemen bereitgestellt werden.

3.6.3.2 Netzwerkmanagement

Für das Management von TCP/IP Netzwerken gibt es eine große Auswahl von Programmen mit unterschiedlichen Schwerpunkten.

Auf die Visualisierung der Netztopologie und Überwachung von Diensten auch auf Servern mit anderen Betriebssystemen ist das Monitoring-Tool „Nagios“ spezialisiert. Nagios reagiert regelbasiert zum Beispiel anhand von definierbaren Schwellenwerten auf gefundene Fehler oder eintretende Ereignisse. Dabei ist eine Eskalation von Meldungen und die Einbindung verschiedener Nachrichtenkanäle (z.B. Mail oder SMS) möglich.

Nagios benutzt Plug-Ins zur aktiven oder passiven Überwachung verschiedenster Dienste und Systemparameter. Unter anderem können typische Netzwerkdienste wie Web, Mail und LDAP, verschiedene RDBMS oder Samba überwacht werden. Außerdem gibt es Plug-Ins für die Überwachung von Systemparametern wie CPU-Last, Festplattenplatz aber auch für die Daten der Hardwaresensoren (Temperatur, Stromversorgung und Lüfterdrehzahl). Es existieren Brücken zu anderen Systemen wie MRTG/RRD und zur Verwendung von SNMP für das Monitoring. Einfache Schnittstellen und Templates erlauben die schnelle Entwicklung eigener Plug-Ins.

Auf das Monitoring und die Analyse von Netzwerktraffic ist MRTG/RRD spezialisiert. MRTG nutzt das Simple Network Management Protocol um Verkehrsdaten von den verschiedensten Netzwerkkomponenten zu sammeln und zu speichern. Die Auswertung und grafische Aufbereitung kann dann entweder intern durch MRTG oder extern durch RRD erfolgen. Für MRTG stehen über 350 Templates zur direkten Anbindung verschiedenster SNMP-fähiger Netzwerkkomponenten und -dienste zur Verfügung.

Ein weiteres Tool zur Trafficanalyse und -visualisierung ist NeTraMet das ebenfalls mit SNMP arbeitet.

Scotty ist ein weiteres Tool für Visualisierung und Management von lokalen Netzen, das ebenfalls mit SNMP arbeitet und auch die Änderung von SNMP-zugänglichen Parametern auf den entfernten Netzkomponenten erlaubt.

Auf die Suche nach auffälligen Mustern im Netzwerktraffic zur Erkennung von Einbruchsversuchen oder anderen Missbrauchsvorfällen ist Snort spezialisiert.

Als „Lightweight Intrusion Detection System“ ist es eine wertvolle Komponente für das Systemmanagement im Netzwerk.

Weiterhin ist auch das Programm Prelude[1] zu erwähnen, welches eine Kombination eines Network Intrusion Detection System und Host Based Intrusion Detection System darstellt. Prelude verwendet dabei für Network Intrusion Detection System die Snort-Regeln.

3.6.3.3 Servermanagement

Für das Management von Servern gibt es unter Linux unter anderem Ulimits, Quotas und Process Accounting zur Überwachung und Beschränkung von Systemressourcen einzelner Nutzer oder Prozesse. Das Monitoring der Dienste und lokaler Systemparameter wird von dem für das Netzwerkmanagement vorgestellten Nagios geleistet.

Die OSS-Serverdienste nutzen eine gemeinsame API zur Protokollierung von Meldungen über den syslogd. Dieser Protokolldienst erlaubt eine hierarchisch organisierte Zentralüberwachung der gesamten Linux/ BSD/ UNIX Infrastruktur. Auch Windows-Server lassen sich in ein zentrales Syslog-System einbinden. Für die automatisierte Auswertung der Logfiles gibt es sowohl anwendungsspezifisch als auch generisch eine Vielzahl von Tools und Konzepten. Eine gute Übersicht liefert http://www.counterpane.com/log-analysis.html

Für die beim Servermanagement gelegentlich notwendige Fehlersuche gibt es über die regulären Protokolldienste hinaus gute Analysemöglichkeiten mit Systemwerkzeugen wie strace, lsof, fuser und netstat.

3.6.3.4 Komplexere Systeme

Im Bereich Systemmanagement gibt es neben dem Simple Network Management Protocol auch das Common Information Model (CIM) mit dem darauf basierenden Web Based Enterprise Management (WBEM) für weiter reichende Ansätze zum standardisierten Systemmanagement in heterogenen Netzen. CIM/ WBEM sind wie SNMP in offenen Standards beschrieben und in Referenzimplementationen als Open Source Software verfügbar. Allerdings werden diese Komponenten zurzeit eher im Rahmen kommerzieller Produkte verwendet, die Praxistauglichkeit der reinen Open Source Lösungen muss sich in diesem Bereich erst noch erweisen.

3.6.3.5 Fazit

Beim Systemmanagement folgen die OSS-Betriebssysteme ihrer Herkunft entsprechend dem UNIX-Weg. Als Mehrbenutzer- und Netzwerksysteme sind bei den OSS-Systemen die Funktionen für das zentrale Systemmanagement sehr vielfältig und in einigen Bereichen das Vorbild und nicht die ersetzende Alternative zu einer Windows-Lösung. Für Administratoren und Betriebsorganisation sind bei einer Migration auch konzeptuelle Änderungen zu erwarten, die insbesondere

[1] siehe auch http://www.prelude-ids.org

bezüglich der Sicherheit große Fortschritte ermöglichen. Die Sicherheit und Zuverlässigkeit, die den Linux-Systemen allgemein zugeschrieben wird, ist nicht zuletzt das Resultat des Systemmanagement.

Für die Personen, die mit diesem Systemmanagement betraut sind, bedeutet ein Migrationsprojekt deutliche Veränderungen. Sowohl die Möglichkeiten zur Analyse als auch die Optionen zur Anpassung und Korrektur der OSS-Systeme geben den Systemmanagern viel mehr Freiheitsgrade als sie bei einem geschlossenen Windows-System zu finden sind. Diese Freiheit kann dazu genutzt werden, sich von Herstellern und externen Dienstleistern zu emanzipieren und gleichzeitig die Qualifikation der eigenen Mitarbeiter zu erhöhen. Die Transparenz der offenen OSS-Systeme erleichtert das grundsätzliche und tief greifende Verständnis von Funktion und Abhängigkeiten der verschiedenen Komponenten in einer modernen IT-Infrastruktur. Wer allerdings weiterhin auf integrierte Lösungen zurückgreifen will, muss entweder auf die nicht ganz billigen Systeme, wie sie von HP, IBM usw. angeboten werden, zurückgreifen oder auf Einzelsysteme, wie z.B. zum Softwaremanagement oder zum Netzwerkmonitoring setzen, die der Aufgabenstellung angemessen sind und die über offene Standard-Schnittstellen verfügen.

3.6.4 Fortführende Migration

3.6.4.1 Systems Management Server 2003

Der Systems Management Server 2003 (SMS) ist die Nachfolgeversion des Systems Management Server 2.0. SMS 2003 beinhaltet im Wesentlichen genau die Funktionalitäten wie der SMS 2.0, die aber auf fast allen Ebenen verbessert wurden.

Wesentliche Änderungen gegenüber der Version 2.0 sind[1]:

- Verbesserung der Skalierbarkeit und Performance
  Mit einem SMS können bis zu 25.000 Clients verwaltet werden.
- Softwareverteilung auch für mobile Geräte
- Active Directory Integration
- Erweiterung des SMS 2.0 Software Update Services auf das Security Patch Management

SMS unterstützt folgende Client-Betriebssysteme[2]:

- SPVirtual PC 2004 or Virtual Server 2005*SP
- Windows Server 2003 family
- Windows 2000 family

---

1 Ergänzende Hinweise unter:
http://www.microsoft.com/smserver/evaluation/features/default.asp#patch

2 Quelle:
http://www.microsoft.com/technet/prodtechnol/sms/sms2003/deploy/spgsms03/spsms06.mspx

- Microsoft Windows® XP Professional
- Windows NT 4.0 Service Pack 6 (with Internet Explorer 5 or later)
- Windows NT 4.0 Service Pack 5 and earlier
- Microsoft Windows® Millennium Edition
- Windows 98 (with Internet Explorer 5 or later)
- Windows 98
- Microsoft Windows® 95

Darüber hinaus gibt es ein Add-On namens Vintela Management Extensions[1] (VMX) mit dessen Hilfe auch Linux-, Unix- und Mac-Systeme unterstützt werden können. Das Add-On unterstützt Funktionen wie:

- Softwareverteilung
- Inventarisierung (Hardware und Software)
- Remote Control
- Reporting

Damit eignet sich SMS durchaus auch für den Einsatz in heterogenen Systemlandschaften. Welche Distributionen und Versionen mit welchen Funktionen im Detail unterstützt werden, muss mit dem Hersteller geprüft werden.

3.6.4.2 Microsoft Operations Manager 2005

Microsoft Operations Manager (MOM) basiert auf einer Entwicklung der Firma NetIQ und unterstützt die Administration von Windows 2000 und 2003 basierenden Serversystemen hinsichtlich der Ereignis- sowie Leistungsüberwachung und -verwaltung.

Microsoft Operations Manager liegt seit kurzem in der Version MOM 2005 vor und umfasst die folgenden Funktionalitäten:

MOM sammelt eine Vielzahl von System- und Anwendungsereignissen aus windowsbasierten Systemen ein, die in einer verteilten IT-Umgebung entstehen, und fasst diese in einem zentralen Ereignisrepository zusammen. Auf diese Weise entsteht eine verteilte **Ereignisverwaltung**. Administratoren können die gesammelten Ereignisse als Gesamtüberblick über die Verfügbarkeit von Servern und Diensten nutzen. Innerhalb von MOM können Regeln erstellt werden. Mit diesen entwickelten Regeln kann das System automatisch auf eingehende Nachrichtendatenströme reagieren. Dies geschieht entweder durch einen vordefinierten Vorgang, der auf einem speziellen Fehlerszenario basiert, oder durch ein aussagekräftiges Ereignis. Mit Hilfe dieser Regeln kann MOM auf bestimmte Ereignismuster reagieren und Vorgänge bzw. Administratorwarnmeldungen auslösen. Jede MOM-Regel kann so konfiguriert werden, dass sie spezielle **Warnungen**

[1] http://www.vintela.com/products/vmx/

mit jeweils zugeordneten Sicherheitsstufen generiert. Eine Warnung kann über ein einzelnes Ereignis oder über mehrere Ereignisse aus zahlreichen Quellen erfolgen. Ein Administrator kann jederzeit den Warnungsverlauf und entsprechende Ereignisse zurückverfolgen. Darüber hinaus können Warnungen E-Mail-Nachrichten sowie Seiten und SNMP-Traps (Simple Network Management Protocol) auslösen. Mit MOM kann eine **Leistungsüberwachung** der angeschlossenen Systeme eingeführt werden. Hierzu können Leistungsschwellenwerte festgelegt und kontrolliert werden. Durch Anpassen oder Hinzufügen von Regeln kann zu späteren Referenzzwecken oder zur Kapazitätsplanung die Entwicklung der System- und Anwendungsleistung überwacht werden. Darüber hinaus können lokale und aggregierte Schwellenwerte festgelegt werden, die als Reaktions-veränderungen in der System- oder Anwendungsleistung Warnungen und Vorgänge erzeugen, die eine Aktion des Administrators erforderlich machen.

Das Portfolio der zu verwaltenden Dienste kann durch **Management Packs** erweitert werden. Management Packs enthalten vorkonfigurierte MOM-Regeln. Jedes Paket stellt Regeln für bestimmte Anwendungen oder Dienste bereit. In MOM ist standardmäßig ein Management Pack enthalten, mit dem alle wichtigen Windows-Dienste, darunter auch der Verzeichnisdienst Active Directory sowie Internetinformationsdienste (Internet Information Services, IIS), verwaltet werden können. Es sind weitere Management Packs von Microsoft und Drittherstellern erhältlich. Microsoft bietet u.a. für folgende Produkte Management Packs an[1]:

- Exchange 5.5/2000/2003
- Internet Information Server (IIS) 4.0/5.0/6.0
- SQL Server 2000
- Commerce Server 2000
- Host Integration Server 2000
- Application Center 2000
- Proxy 2.0
- ...

MOM bietet die Möglichkeit, die gesammelten Daten in Form von Berichten aufzubereiten und darzustellen. Ein Tool zur grafischen Berichterstellung ermöglicht den Zugriff auf vorkonfigurierte Berichte und Diagramme. Die generierten Berichte ermöglichen Administratoren das Überprüfen des Status von Systemen und Diensten im Netzwerk. Mit Management Packs von Microsoft oder Drittanbietern können dem System weitere Berichte hinzugefügt werden. Insbesondere kann MOM HTML-basierte (Hypertext Markup Language) Snapshots aller entwickelten Berichte generieren. Die Snapshots können anschließend auf einen Webserver exportiert werden, so dass von Webbrowsern darauf zugegriffen werden kann.

[1] Weiteren verfügbare Management Packs findet man über http://www.microsoft.com/management/mma/catalog.aspx

Für die Installation wird Windows 2000/2003 Server benötigt. Die empfohlene Datenbankplattform ist MS SQL 2000.

3.6.4.3 Application Center

Microsoft Application Center 2000 ist ein Bereitstellungs- und Verwaltungstool für Webanwendungen mit hoher Verfügbarkeit, die auf dem Betriebssystem Microsoft Windows 2000 erstellt wurden. Mit Application Center 2000 wird die Verwaltung von Servergruppen vereinfacht.

3.7 Verzeichnisdienst

3.7.1 Überblick

Da bezüglich der Ausgangslage ein Verzeichnisdienst nicht integraler Bestandteil von Windows NT ist, geht es in den nachfolgenden Betrachtungen nicht primär um die Ablösung oder Fortführung eines bestehenden Verzeichnisdienstes. Dennoch spielt sowohl in der ablösenden als auch in der fortführenden Migration der Verzeichnisdienst eine wichtige Rolle. Mit der Migration nach Windows 2003 und insbesondere mit der Migration nach Exchange 2003 erfolgt die Einführung des Active Directory.

Bei einer Migration der bestehenden Umgebung hin zu einer Umgebung mit Verzeichnisdienst, bringt der Einsatz eines Verzeichnisdienstes, sehr viele Vorteile, insbesondere hinsichtlich der Realisierung von komfortablen Authentifizierungsdiensten.

Aufgrund dessen stellen die nachfolgenden technischen Betrachtungen eher einen Blick in die Zukunft dar und untersuchen die Besonderheiten bei einer Einführung des jeweiligen Verzeichnisdienstes bzw. die Einsatzmöglichkeiten. Einen besonderen Aspekt bildet dabei die integrative Wirkung des Active Directory (AD) und wie diese zu bewerten ist.

Im Ergebnis lässt sich festhalten, dass der AD nur in einer minimalen Ausprägung implementiert werden sollte, sofern auf dessen Einsatz nicht verzichtet werden kann. Sicherlich stehen einem damit nur ein Bruchteil der Funktionalitäten des AD zur Verfügung, die bei Implementierung einer vollen Ausprägung zum tragen kommen. Da man sich damit aber auch in gewisse Anhängigkeiten begibt empfiehlt es sich, für darüber hinaus gehende Anforderungen auf andere Produkte und Lösungen, wie z.B. ein Metadirectory zurückgreifen.

3.7.2 Grundlagen

Mit einem Verzeichnisdienst können beliebige Informationen netzwerkweit zur Verfügung gestellt werden. Ein Verzeichnisdienst besteht typischerweise aus einer Datenbank, in dem diese Informationen gespeichert und einem Netzwerkprotokoll, mit dem die Informationen abgefragt oder geändert werden können. Das zurzeit am häufigsten eingesetzte Verzeichnisdienstprotokoll ist das Lightweight Directory Access Protocol (LDAP). LDAP wurde zunächst entwickelt, um auf einfache Weise auf X.500-basierte Verzeichnisdienste zuzugreifen. Heute

wird man unter einem LDAP-Server meist die Kombination aus Datenbank und Protokollimplementierung verstanden. LDAP in der Version 3 ist im RFC 2251 definiert.

Typisch für einen Verzeichnisdienst ist die hierarchische Strukturierung der in ihm enthaltenen Informationen, ähnlich wie in einem Dateisystem. Ausgehend von einem Wurzelpunkt befinden sich die Informationen in Objekten, wobei jedes Objekt eine Anzahl von Attributen hat, deren Werte die eigentlichen Informationen darstellen. Jedes Objekt kann gleichzeitig Unterobjekte (mit Attributen haben) enthalten, die ihrerseits weitere Unterobjekte haben können.

Objekte in einem Verzeichnisdienst sind inhaltlich von anderen Objekten abgrenzbare Einheiten, wie z.B. Personen, Gruppen, Computer, Drucker oder in einem Gebäude vorhandene Konferenzräume. Welche Attribute ein Objekt haben kann und haben muss, wird durch die Objektklassen des Objekts definiert. Eine in vielen Verzeichnissen vorkommende Objektklasse trägt beispielsweise die Bezeichnung *person* und schreibt vor, dass Objekte mit dieser Klasse wenigstens die Attribute *surname* (Familienname) und *commonName* (allgemeiner Name) haben müssen. Zusätzlich erlaubt sie optional u.a. die Attribute *telephoneNumber* (Telefonnummer) und *description* (Beschreibung). Objektklassen und Attribute werden im so genannten Schema des Verzeichnisses definiert.

Durch die Möglichkeit, Objekten (auch nachträglich) mehrere Objektklassen zuzuordnen, ergeben sich eine hohe Flexibilität und die Möglichkeit, zusammenhängende Informationen an demselben Ort (nämlich in demselben Objekt) zu speichern. Eine Person kann mehrere inhaltlich zusammengehörende Eigenschaften haben, die durch unterschiedliche Objektklassen (mit unterschiedlichen und sich überschneidenden Attributen) definiert werden müssen. So kann eine Person als Benutzer von Rechnersystemen, als Telefonbucheintrag, als Eintrag in einem Adressbuch oder als Lebenspartner einer anderen Person gesehen werden. Wollte man diese Eigenschaften in einem Verzeichnis speichern, dann würden für die Eigenschaftsklassen Benutzer, Telefonbucheintrag, Adressbucheintrag und Lebenspartner entsprechende Objektklassen mit Attributen definiert werden. Damit jede dieser Objektklassen auch ohne die anderen sinnvoll benutzt werden kann, hätte jede dieser Objektklassen wahrscheinlich Attribute, die auch in den anderen benötigten Objektklassen vorkommen, wie z.B. der Name der Person. Werden die Objektklassen in einem Objekt miteinander kombiniert, dann wird das Attribut *Name* jedoch nur ein einziges Mal gespeichert.

Die Möglichkeit zur hierarchischen Strukturierung von Verzeichnissen wird im Allgemeinen genutzt, um den Aufbau einer Organisation im Verzeichnis abzubilden. Dazu werden meist spezielle Objekte verwendet, welche zur Strukturierung des Verzeichnisses dienen und künstlichen oder realen organisatorischen Einheiten entsprechen. Diese Objekte benutzten oft die Objektklasse *organizationalUnit (ou)*. Der Übersichtlichkeit halber wird der Verzeichnisdienst außerdem oft anhand des in Organisationen ohnehin schon vorhandenen DNS-Namensraumes aufgebaut. Dazu wird die Objektklasse *domainComponent (dc)* verwendet. In der

Praxis wird die Grobstrukturierung meist anhand des DNS-Namensraumes und die Feinstrukturierung mit Organisationseinheiten und anderen Containerobjekten vorgenommen.

Als Beispiel soll eine Organisation mit zwei Standorten (Oststadt und Weststadt) dienen. Die Organisation benutzt die DNS-Domäne *bsporg.de* und für die beiden Standorte die Subdomänen *oststadt.bsporg.de* und *weststadt.bsporg.de*. Als Basispunkt ihres Verzeichnisses könnte die Organisation dann ein Objekt „*bsporg.de*“ verwenden. In LDAP würde dieses Objekt als *dc=bsporg,dc=de* bezeichnet werden, um auszudrücken, dass es sich bei dem Basispunkt um ein Objekt vom Typ Domänenkomponente (*domainComponent, dc*) und mit dem Namen *bsporg* handelt, das ein Unterobjekt des Objektes *de* ist, welches ebenfalls den Typ Domänenkomponente hat.

Dieser Basispunkt würde nun zwei weitere Objekte mit den Bezeichnungen *dc=oststadt* und *dc=weststadt* aufnehmen (analog der DNS-Namen für diese Standorte). Bei diesen Bezeichnungen wird auch von den relativen Namen der Objekte gesprochen, weil durch sie nicht eindeutig bezeichnet ist, wo sie sich in der Verzeichnishierarchie befinden. Alternativ dazu können eindeutige Namen (*distinguished Names*) verwendet werden, mit denen die genaue Lage der Objekte im Verzeichnis gekennzeichnet ist. Diese Namen wären dann *dc=oststadt,dc=bsporg,dc=de* und *dc=weststadt,dc=bsporg,dc=de*.

An jedem der beiden Standorte habe die Organisation ferner drei organisatorische Einheiten, mit den Bezeichnungen Produktion, Vertrieb und Leitung. Zur Abbildung im Verzeichnis würde dazu für die Organisationseinheit Produktion am Standort Oststadt das Objekt *ou=produktion* als Unterobjekt von *dc=oststadt* angelegt (eindeutiger Name: *ou=produktion, dc=oststadt, dc=bsporg, dc=de*). Analog wäre mit den anderen Einheiten an diesem und dem anderen Standort zu verfahren. Innerhalb der Organisationseinheit Produktion wären beispielsweise Objekte für Personen, Gruppen von Personen sowie von Rechnern anzulegen. Für eine übersichtlichere Gestaltung könnten diese Objekte in Containern (im Allgemeinen bezeichnet durch Namen oder *commonName, cn*) mit den Bezeichnungen *cn=leute*, *cn=gruppen* und *cn=rechner* angeordnet werden. Schließlich würden die Einträge für die realen Objekte in diesen Containern erzeugt werden. So würde beispielsweise ein Objekt für den Mitarbeiter „Karl Schulze“, beschäftigt in der Produktion am Standort Oststadt, in dem Container *cn=leute, ou=produktion, dc=oststadt, dc=bsporg, dc=de* angelegt werden. Dieses Objekt hätte dann den Namen *cn=schulze, cn=leute, ou=produktion, dc=oststadt, dc=bsporg, dc=de*.

Durch die Nutzung möglichst vieler Anwendungen kann ein Verzeichnisdienst zum Single-Point-of-Administration einer Infrastruktur werden. Im optimalen Fall stellt er die ausschließliche Quelle der in ihm gespeicherten Informationen im Netzwerk dar. Stehen im Netzwerk einer Organisation beispielsweise Windows- und UNIX-basierte Server, eine Intranetanwendung, ein Web-Proxy mit Authentifizierung zur Verfügung, so lassen sich Benutzerkonten und die Rechte der Be-

nutzer an den unterschiedlichen Systemen jeweils separat auf den einzelnen Systemen konfigurieren. Mit der Einführung eines Verzeichnisdienstes ist es möglich, die Benutzerkonten und die dazugehörigen Berechtigungen nur noch zentral im Verzeichnisdienst speichern und alle Systeme darauf zugreifen zu lassen. Gleichzeitig können Adressbuchanwendungen, wie sie beispielsweise in E-Mail-Software eingebaut sind, auf das Verzeichnis zugreifen und so die E-Mail-Adressen der Mitglieder der betreffenden Organisation bereit stellen, ohne dass diese Daten erneut manuell eingegeben werden müssten.

Verzeichnisdienste können auch zur Speicherung von Passwörtern genutzt werden (Passwörter sind dann typischerweise ein Attribut von Personen- oder Benutzerkontenobjekten). Auch dadurch wird das Ziel der einmaligen, zentralen Datenhaltung verfolgt. Im Verzeichnis gespeicherte Passwörter brauchen nur an einer Stelle angelegt und geändert zu werden und können dann auf allen Systemen und mit allen Anwendungen genutzt werden, die das Verzeichnis zur Authentifizierung verwenden können. Außerdem können die im Verzeichnis gespeicherten Passwörter zur Authentifizierung beim Zugriff auf Daten im Verzeichnis selbst genutzt werden.

Das Beispiel Passwortspeicherung macht deutlich, dass es für den Zugriff auf den Verzeichnisdienst ein feingranulares Rechtesystem geben muss, das definiert, welche Objekte und Attribute durch welche Benutzer gelesen oder geändert werden dürfen. So ist es durchaus sinnvoll, dass Passwörter durch ihre Besitzer und Administratoren geändert werden können. Von ihren Besitzern müssen sie darüber hinaus zur Authentifizierung verwendet werden können. Alle anderen Personen, die auf das Verzeichnis zugreifen können, dürfen dagegen nicht in der Lage sein, die Passwörter überhaupt zu lesen, selbst wenn sie sich im Verzeichnis in verschlüsselter Form befinden. Gleichzeitig könnte es anderen Benutzern aber erlaubt sein, die E-Mail-Adressen von Benutzerobjekten zu lesen. In einem solchen Fall müssten unterschiedliche Attribute (Passwort und E-Mail-Adresse) desselben Objekts (Person oder Benutzer) mit unterschiedlichen Berechtigungen ausgestattet sein. Die meisten Verzeichnisdienste implementieren deswegen ein System von Access Control Lists (ACLs), das ebenfalls mit den ACLs auf Dateisystemebene zu vergleichen ist.

Trotz der weit verbreiteten Praxis, Verzeichnisdienste zur Authentifizierung zu verwenden, muss dies als fragwürdige Strategie angesehen werden. Das Konzept erlaubt keine sichere Methode zur Implementierung von Single Sign On, da an jedem System und jeder Anwendung erneut eine Authentifizierung stattfinden muss (wenngleich auch mit demselben Passwort). Außerdem sind die meisten Verzeichnisdienste nicht mit dem Ziel geschrieben worden, einen sicheren Authentifizierungsmechanismus bereit zu stellen, sondern um häufig benötigte Informationen zentral zu speichern und schnell an Clients liefern zu können. Stattdessen empfiehlt sich der Einsatz von Kerberos.

Bei der Verwendung von Kerberos werden nicht wie sonst in der Regel üblich, Benutzernamen und Passwort an jeden Server geschickt, dessen Dienste von

einem Benutzer in Anspruch genommen werden sollen. Vielmehr erfolgt eine einmalige Anmeldung an einem Key Distribution Center (KDC, gelegentlich auch als Kerberos Domänencontroller bezeichnet). Der Benutzer erhält nach erfolgter Anmeldung ein Ticket, das eine definierte Gültigkeitsdauer hat und mit dem er sich dann gegenüber allen weiteren Diensten authentifizieren kann. Nach Ablauf der Gültigkeit des Tickets muss sich der Benutzer erneut authentifizieren. Durch den Einsatz von Kerberos muss die Passwortdatenbank nur noch auf besonders vertrauenswürdigen Systemen (den Kerberos-Servern) vorhanden sein. Andere Systeme brauchen keinen Zugriff mehr auf die Passwortdatenbank. Mit Hilfe von Kerberos-Tickets kann außerdem Single Sign On implementiert werden, weil Tickets zum Zugriff auf alle im Netzwerk bereitgestellten Dienste verwendet werden können (sofern die entsprechenden Applikationen Kerberos unterstützen).

Sobald ein Verzeichnisdienst zur zentralen Informationsdatenbank einer Organisation wird, wird er zu einer besonders wichtigen Komponente des Netzwerks, die eine sehr hohe Verfügbarkeit haben muss. Verzeichnisdienste unterstützen deswegen in der Regel Replikationsverfahren, mit denen das ganze Verzeichnis und Änderungen von einem Server mit Verzeichnisdienst auf andere übertragen werden können. Dadurch wird auch eine Möglichkeit zur Lastverteilung geboten, weil nicht alle Clients auf den gleichen Verzeichnisserver zugreifen müssen.

Bei der Replikation sind zwei Verfahren zu unterscheiden, die Master-Slave-Replikation und die Multi-Master-Replikation. Beim Master-Slave-Verfahren können Änderungen nur auf einem zentralen Master-Server des Verzeichnisses vorgenommen werden, der die Änderungen dann an die übrigen (Slave-)Server repliziert. Bei Änderungen von Verzeichnisinhalten ergibt sich dadurch ein gewisser Engpass, weil sie nur auf dem zentralen Server vorgenommen werden können. Fällt der Master-Server aus, können solange keine Änderungen vorgenommen werden, bis das System zur Verwendung eines anderen Servers als Master umkonfiguriert oder der ursprüngliche Master-Server wieder hergestellt worden ist. Die Multi-Master-Replikation erlaubt die Änderung von Verzeichnisinhalten auf mehreren Servern, wodurch die oben genannten Probleme gelöst werden. Allerdings können sich bei der Multi-Master-Replikation Konsistenzprobleme ergeben, wenn miteinander in Konflikt stehende Änderungen gleichzeitig an unterschiedlichen Servern vorgenommen werden.

3.7.3 Active Directory Service (ADS)

Ziel dieses Abschnittes ist es, einen möglichst umfassenden Überblick über die Technologie „Active Directory Service“ zu vermitteln. Es wird daher auf die Kernfunktionalitäten

- Directory Service
- LDAP
- Kerberos V5
- Einsatz von Gruppenrichtlinien zum managen von Clients

- Delegation von Berechtigungen
- Zertifikatsverwaltung

eingegangen.

Darüber hinaus werden

- das Einsatzgebiet
- die Architektur
- und die strategische Bedeutung

beschrieben.

Ferner soll erörtert werden, worin der Unterschied von einem Active Directory in minimaler zu dem einer maximalen Ausprägung besteht.

3.7.3.1 Nachfolger vom Windows NT 4 Anmeldedienst

Hinsichtlich der Anmeldedienste von Windows NT kann das Active Directory (AD) als korrespondierender Nachfolgedienst bezeichnet werden.

Dieser Umstand wird dadurch untermauert, dass der Aufruf der Installationsroutine von Windows 2000 auf einem Windows NT PDC unmittelbar zum Aufbau eines Active Directory führt. Es wäre an dieser Stelle jedoch falsch zu meinen, dass der Aufbau eines Active Directory lediglich im Aufruf einer Installationsroutine auf einem einzelnen Server bestehen würde. Für den Aufbau eines AD bedarf es jedoch einer gründlichen Konzeption und einer sorgfältigen Migrationsplanung.

Kerntechnologie der Anmeldedienste im Active Directory bleibt wie unter Windows NT die Struktureinheit Domäne. Sie bleibt die Verwaltungseinheit, die die Computer- und Benutzerkonten mittels einer gemeinsam genutzten Datenbank in einem gemeinsamen Sicherheitskontext zusammenfasst. Die Domänengrenze ist die Grenze des Sicherheitskontextes und der Replikation der Benutzerdatenbank.

Der NetBIOS-Namensraum bleibt erhalten. Des Weiteren können wie unter Windows NT Computer auf der Basis

- Windows NT 4.0
- Windows 2000
- Windows XP

Mitglieder der Domäne sein.

Sollen Systeme wie Windows NT und 9x unterstützt werden, ist es weiterhin notwendig, eine fehlerfreie NetBIOS Namensauflösung (z.B. durch WINS) zu gewährleisten. Ob der Einsatz einer NetBIOS Namensauflösung erforderlich ist, wird nicht nur allein durch das Betriebssystem bestimmt sondern in erster Linie

durch das Gesamtsystem. So kann es z.B. sein, das auf dem Client Windows XP eingesetzt wird, der kein NetBIOS mehr benötigt, aber Applikationen auf dem Windows XP eingesetzt werden, die diese Namensauflösung sehr wohl noch erforderlich machen. Dieser Umstand ist bei jeder Migration zu beachten und im Einzelfalle zu prüfen.

Kennzeichnend für den zu vollziehenden Architekturwechsel ist die Implementierung eines Active Directory. Dieser bedarf zwingend einer DNS Infrastruktur, die nicht nur die Wahl eines Namensraumes sondern auch die Verwendung geeigneter DNS Server notwendig macht. Dies impliziert natürlich eine existierende TCP/IP Netzwerkumgebung.

Die Migrationsplanung bzw. eine Auswahl der möglichen Szenarien werden in einem der folgenden Abschnitte beschrieben.

3.7.3.2 Authentifizierungsmechanismus Kerberos

Unter Windows 2003 Active Directory wird weiterhin der Authentifizierungsmechanismus NTLM unterstützt. Dies ist allein deshalb schon notwendig, um die Anmeldung von Systemen wie Windows NT oder 9x zu ermöglichen.

Die Authentifizierung erfolgt mittels Kerberos**.**

Clientsysteme wie Windows 2000 oder XP nutzen standardmäßig das Kerberos Protokoll um sich bei der AD Domäne zu authentifizieren. Der Administrator kann hierbei unterscheiden ob nur Kerberos erlaubt ist, oder aber ob NTLM weiterhin für ältere oder Nicht Microsoft Betriebssysteme angeboten werden soll. Systeme wie Windows NT oder 9x können auch nicht durch Nachrüstung zu Kerberos überwechseln. Windows 2003 DCs kommunizieren ausschließlich über das Kerberos Protokoll.

In Windows 2003 ist Kerberos in der Version 5 mit Erweiterungen für die Authentifizierung via öffentlicher Schlüssel (public key) implementiert worden. Die Implementierung folgt Spezifikationen in den RFCs 1510 und 1964. Das Kerberos Key Distribution Center (KDC) ist auf jedem DC des Active Directory integriert und verwendet die Benutzerdatenbank des AD.

Für das Kerberos Protokoll ist es notwendig, dass die Systemzeiten der beteiligten Computer nur geringe Abweichungen aufweisen, da die Authentifizierung des Computers über ein so genanntes Ticket gesteuert wird, dessen Gültigkeitsdauer auf 5 Minuten begrenzt ist. Zu diesem Zweck ist in Windows 2003 ein automatischer hierarchischer Zeitabgleich zwischen den Computern, die Mitglied des AD sind, implementiert worden.

Kerberos ist flexibler, effizienter und sicherer als die NTLM Authentifizierung. Bei NTLM muss ein Applikationsserver immer den Domain Controller kontaktieren, um einen Client zu authentifizieren. Erst danach erfolgt der Zugriff auf die jeweiligen Ressourcen. Mit dem Kerberos Protokoll kann der Applikationsserver die Anmeldeinformationen untersuchen, die ihm der Client präsentiert (Ticket). Unter NTLM können Server die Identität der Clients prüfen, mit Kerberos kann der

Client auch die Identität des Servers prüfen (mutual authentication). Windows Dienste müssen den Client nachahmen (impersonate), um den Zugriff auf Ressourcen zu realisieren. NTLM und Kerberos können dem Dienst die Informationen liefern, um den Client lokal nachzuahmen. Bei verteilten Applikationen mit Front- und BackEnd auf verschiedenen Rechnern scheitert NTLM, Kerberos hingegen bietet einen Proxy Mechanismus (delegated authentication). Kerberos kann transitive, bidirektionale Vertrauensstellungen zwischen Domänen realisieren.

Das Kerberos-Protokoll setzt sich aus drei Teilprotokollen zusammen. Das Teilprotokoll, über welches das Schlüsselverteilungscenter (Key Distribution Center, KDC) dem Client einen Anmeldesitzungsschlüssel und ein TGT (Ticket Granting Ticket) erteilt, wird als Authentifizierungsdienst (Authentication Service Exchange, AS Exchange) bezeichnet. Das Teilprotokoll, über welches das KDC einen Dienstsitzungsschlüssel und ein Ticket für den Dienst erteilt, wird als Ticketdienst (Ticket Granting Service, TGS Exchange) bezeichnet. Das Teilprotokoll, über das der Client das Ticket für den Zugang zu einem Dienst sendet, wird als Client/Server-Dienst (CS Exchange) bezeichnet.

3.7.3.3 Neuerungen hinsichtlich der Strukturierung

Wie bereits erwähnt, bleibt die Struktureinheit Domäne als Grenze der Sicherheitszone auch in einem Active Directory erhalten.

Im Active Directory ist die Domäne als ein Baustein einer Gesamtstruktur (forest) und der dazu gehörenden Baumstrukturen (tree) zu betrachten, die in einem DNS Namensraum hierarchisch gegliedert sind. Die einzelnen Domänen sind über so genannte bidirektionale Transitive Kerberos-Trusts (Vertrauensstelllungen) miteinander verbunden. (Die aus Windows NT bekannten Vertrauensstellungen via NTLM können weiterhin eingesetzt werden.)

Wird von einem Active Directory gesprochen, ist damit immer die Gesamtstruktur gemeint und nicht einzelne Bäume oder Domänen.

Die folgende Abbildung zeigt eine Windows NT Domänenstruktur, in der zwei Account-Domänen und fünf Ressourcendomänen durch Vertrauensstellungen miteinander verwoben sind.

Microsoft stellt Active Directory Domänen dreieckig, Windows NT Domänen mit Ellipsen dar. Diese Konvention wird für diesen Leitfaden übernommen. Somit ergibt sich folgendes Bild:

Bild 11: Beispiel NT-Domänenstruktur

In einem Active Directory wäre dementsprechend die folgende Gesamtstruktur (Bild 12) denkbar, die ebenfalls sieben Domänen umfasst: die Gesamtstruktur umfasst zwei Bäume, in denen die Domänen hierarchisch strukturiert sind und über Kerberos transitiv (A vertraut B und B vertraut C, dann vertraut A auch C) und bidirektional (A vertraut B, dann vertraut B auch A) miteinander verbunden sind.

Bild 12: Beispiel Windows 2000

Das Active Directory wird von Domain Controllern (DC) bereitgestellt. Die Unterscheidung zwischen PDC und BDC wird nicht weiter fortgeführt. Dies trägt der architektonischen Neuerung Rechnung, dass Windows 2000/2003 Domain Controller sich einem Multi-Master-Prinzip der Replikation unterwerfen: sämtliche Änderungen innerhalb des AD können auf einem beliebigen DC durchgeführt (geschrieben) werden. Bei dem Multi-Master Prinzip sind nicht alle Rollen innerhalb der Domäne auf allen DC verteilt. Zu diesem Zweck gibt es Domain Controller mit einer speziellen Rolle. Die so genannten FSMO-Owner (Flexible Single Master Operation).

Es handelt sich hierbei um

- PDC-Emulator
- Infrastructure Master
- RID Master
- Schema Master
- Domain Naming Master.

Diese Funktionen können auf speziell ausgewählten Domain Controllern platziert werden.

Die Funktionen

- Schema Master (zuständig für das Schema des Verzeichnisses)
- Domain Naming Master (zuständig bei Änderungen im Namensraum)

sind einmalige Rollen innerhalb einer Gesamtstruktur (forest).

Die Funktionen

- PDC-Emulator
- Infrastructure Master (zuständig für Aktualisierungen von SIDs und Distinguished Names über Domänengrenzen hinweg)
- RID Master (zuständig für die Vergabe von RID Pools an andere DCs)

sind eindeutig in jeder Domäne.

Der PDC-Emulator übernimmt wichtige Funktionen wie:

- Kennwortaktualisierungen für Down-Level Clients (NT 4.0, 9x) und Partner der Windows NT Backup Domain Controller
- Quelle der Netzwerk-Uhrzeit (nur PDC der Stammdomäne)
- den Domänen Hauptsuchdienst (NetBIOS)

Eine Gesamtstruktur kann zusätzlich durch Standorte (Sites) strukturiert werden. Die Sitestruktur sollte hierbei der physischen Netzwerkstruktur folgen und diese widerspiegeln und mit den verfügbaren Bandbreiten zwischen den Lokationen (Hamburg, Berlin, Bonn etc.) korrespondieren. Primärer Zweck dieser Strukturierung ist die Steuerung der Replikation zwischen den Domain Controllern. Somit können die Replikationszeiten bei Bedarf der tatsächlich vorhandenen physischen Netzwerkstruktur angepasst werden.

Die Standorttopologie kann unabhängig von der Domänenstruktur gewählt werden. Die folgende Abbildung stellt eine beispielhafte Topologie dar.

Bild 13: Beispiel Standort- und Domänenstruktur

Eine weitere Neuerung hinsichtlich Strukturierung ist die so genannte OU-Struktur (OU steht für Organizational Unit, Organisationseinheit), diese wird im Abschnitt zum Thema Verzeichnisdienst beschrieben.

3.7.3.4 DNS Namensraum und Infrastruktur

Windows 2003 Active Directory Service benötigt zwingend eine DNS Infrastruktur, wobei hier entweder die bereits vorhandene DNS Infrastruktur der jeweiligen Behörden genutzt werden kann oder aber eine separate DNS Struktur parallel aufgebaut werden kann. Für eine genaue Betrachtung müssen jedoch zu Beginn des jeweiligen Migrationsprojektes die folgenden Fragen beantwortet werden:

- Welchen DNS Namensraum soll das AD erhalten?
  - Intern oder extern?
- Wie soll sich dieser Namensraum in den bestehenden DNS Namensraum einfügen?
  - Als Subdomain oder eigenständige Zone?
- Von wem wird der bestehende Namensraum verwaltet?
- Auf welcher Plattform (Betriebssystem: Windows 2003 oder Unix) soll das DNS bereitgestellt werden?
- Welche Korrespondenz zum NetBIOS Namensraum ist zu berücksichtigen?

Die Beantwortung dieser Fragen gestaltet sich oftmals nicht nur aufgrund technischer Umstände sondern wegen „politischer“ Hintergründe als besonders kompliziert.

Wahl der Plattform

Die DNS Infrastruktur für ein AD bedarf gewisser Eigenschaften, damit die Namensauflösung und Registrierung von Einträgen reibungslos funktioniert.

Grundsätzlich erfüllt Windows 2003 mit seiner eigenen DNS Implementierung diese Eigenschaften vollständig. Windows 2003 DNS hat unter anderem folgende Features:

- Service Records (RFC 2052)
- Dynamisches DNS (RFC 2136)
- Sicheres Dynamisches Update
- Multimaster-Methode durch Integration ins Active Directory
- Integration von WINS

Zwingend erforderlich ist die Unterstützung von RFC 2052, denn nur so können Einträge für Dienste im DNS vorgenommen werden. RFC 2052 wird von Unix-basierten Servern ab BIND 8.1.2 unterstützt.

NetBIOS Namensraum

Hinsichtlich des NetBIOS Namensraumes sind folgende Aspekte zu beachten:

- der NetBIOS Name einer Windows 2003 Domäne (z.B. RES1) kann prinzipiell vom untersten Namen des DNS Suffixes abweichen (z.B. RES001 von res001.behoerde.de). Von einer solchen Namenswahl ist aber grundsätzlich abzuraten.
- der NetBIOS Namensraum ist insbesondere dann ohne Freiheitsgrade, wenn bestehende NT Domänen aktualisiert (siehe Inplace Migration) werden sollen.

DNS Namensraum

Für die folgenden Betrachtungen wird davon ausgegangen, dass in der bestehenden Infrastruktur bereits eine DNS Umgebung existiert, die auf Basis von Unix Server bereitgestellt wird. Dies ist eine relativ allgemeine Ausgangssituation. Der Name der Domain sei hier mit „BEHOERDE.DE“ angenommen, der bestehende Namensraum BEHOERDE.DE werde nur intern verwendet. Des Weiteren wird angenommen, dass in der DNS Infrastruktur eine interne Root-Domäne („Punkt“) bzw. Zone existiert. Die folgende Abbildung skizziert die Ausgangssituation.

Ausgangssituation

Bild 14: Ausgangssituation

Die folgenden Absätze beschreiben mögliche Lösungsansätze zur Bildung eines Namensraums in Hinblick auf Windows 2000 Active Directory. Hiermit soll die Komplexität der Migration nach ADS und die damit verbundene Langfristigkeit und Bindung an ADS verdeutlicht werden.

Stammdomäne: W2K.BEHOERDE.DE

Der bestehende interne DNS Namensraum wird dazu genutzt, eine weitere Subdomäne W2K (als Stammdomäne = erste Active Directory Domäne) aufzunehmen.

Bild 15: Stammdomäne: W2K.BEHOERDE.DE

Die Vorteile dieser Stammdomäne sind:

- es wird kein neuer Namensbaum geschaffen
- bestehende Root Server werden beibehalten
- die Plattform der DNS Dienste kann frei gewählt werden
- interner und externer Namensraum bleiben getrennt

Die Nachteile dieser Lösung sind:

- der User Principal Name des Anwenders ist relativ lang (Benutzername @w2k.behoerde.de) bzw. beinhaltet eine 2nd Level Domain
- bei Vergrößerung der Gesamtstruktur (z.B. plus DNS-Baum ZUSATZ.DE) ist einer der Bäume keine 2nd Level Domain (technisch unproblematisch)
- Ein Teil der Namensauflösung hängt maßgeblich von der bisherigen Infrastruktur ab

Stammdomäne: BEHOERDE.DE

Der bestehende DNS Namensraum wird dazu genutzt, den Namen der Stammdomäne zu bestimmen.

Bild 16: Stammdomäne: BEHOERDE.DE

Die Vorteile dieser Stammdomäne sind:

- es wird kein neuer Namensbaum geschaffen
- bestehende Root Server werden beibehalten
- der User Principal Name des Anwenders ist relativ kurz (Benutzername@behoerde.de)
- bei Vergrößerung der Gesamtstruktur (z.B. plus DNS-Baum ZUSATZ.DE) sind beide Bäume 2nd Level Domain
- interner und externer Namensraum bleiben getrennt

Die Nachteile dieser Lösung sind:

- die Plattform der DNS Dienste kann nicht gewählt werden
- die Namensauflösung hängt ausschließlich von der bisherigen Infrastruktur ab

Stammdomäne: NEU.DE

Dieser Ansatz ist unabhängig vom bisherigen Namensraum und kreiert einen neuen internen DNS Namensbaum. Dieser gewählte Name NEU.DE ist weltweit einzigartig, ist also offiziell registriert.

Bild 17: Stammdomäne: NEU.DE

Die Vorteile dieser Stammdomäne sind:

- es wird ein neuer Namensbaum geschaffen, so dass keine Altlasten übernommen werden
- bestehende Root Server können beibehalten werden
- die Plattform der DNS Dienste kann gewählt werden
- der User Principal Name des Anwenders ist relativ kurz (Benutzername@neu.de)
- bei Vergrößerung der Gesamtstruktur (z.B. plus DNS-Baum ZUSATZ.DE) sind beide Bäume 2nd Level Domain
- die Namensauflösung hängt in geringem Maße von der bisherigen Infrastruktur ab
- interner und externer Namensraum können getrennt bleiben, je nach späterer Anforderung

Die Nachteile dieser Lösung sind:

- es wird ein neuer Namensbaum geschaffen, so dass neue Strukturen und zusätzliche Richtlinien entstehen
- die Komplexität hinsichtlich DNS nimmt zu und somit auch der Verwaltungsaufwand

Stamm- und Strukturdomäne: NEU.DE/ INTRA.NEU.DE

Dieser Ansatz ist unabhängig vom bisherigen Namensraum und kreiert einen neuen DNS Namensbaum. Neben der 2nd Level Domain NEU.DE wird noch eine zusätzliche Subdomain geschaffen.

Die 2nd Level Domain NEU.DE dient ausschließlich als Stammdomäne der Gesamtstruktur, als so genannte Strukturdomäne. Benutzerkonten werden nur in der Subdomäne INTRA angelegt.

Bild 18: Stamm- und Strukturdomäne: NEU.DE/ INTRA.NEU.DE

Die Vorteile der Strukturdomänen sind:

- es wird ein neuer Namensbaum geschaffen, so dass keine Altlasten übernommen werden
- bestehende Root Server können beibehalten werden
- die Plattform der DNS Dienste kann gewählt werden
- bei Vergrößerung der Gesamtstruktur (z.B. plus DNS-Baum ZUSATZ.DE) sind beide Bäume 2nd Level Domain
- bei Vergrößerung der Domänenanzahl können die neuen Domänen parallel zur Domäne INTRA verankert werden
- die Namensauflösung hängt in geringem Maße von der bisherigen Infrastruktur ab
- interner und externer Namensraum können getrennt bleiben, je nach Anforderung

Die Nachteile dieser Lösung sind:

- es werden zwei Domänen im Active Directory installiert
- es wird ein neuer Namensbaum geschaffen, so dass neue Strukturen und zusätzliche Richtlinien beachtet entstehen
- der User Principal Name des Anwenders ist relativ lang (Benutzername @intra.neu.de)
- die Anzahl der Querverbindungen steigt und somit die Komplexität und der Verwaltungsaufwand

Stammdomäne: INTRA.BEHOERDE-ONLINE.DE

Ein bestehender **externer** DNS Namensraum wird dazu genutzt, eine weitere Domäne aufzunehmen. Der bestehende Namensraum BEHOERDE-ONLINE.DE wurde bisher nur extern verwendet. Es muss eine Domäne INTRA eingerichtet werden, die nur intern verwendet wird.

Bild 19: Stammdomäne: INTRA.BEHOERDE-ONLINE.DE

Die Vorteile dieser Stammdomäne sind:

- es wird ein neuer interner Namenszweig geschaffen, so dass keine Altlasten übernommen werden
- bestehende Root Server werden beibehalten
- die Plattform der DNS Dienste kann gewählt werden
- bei Vergrößerung der Gesamtstruktur (z.B. plus DNS-Baum ZUSATZ.DE) sind beide Bäume 2nd Level Domain
- die Namensauflösung hängt maßgeblich von der bisherigen Infrastruktur ab

Die Nachteile dieser Lösung sind:

- der User Principal Name des Anwenders ist relativ lang (Benutzername@intra.behoerde-online.de)
- es wird ein neuer interner Namensbaum geschaffen, so dass neue Strukturen und zusätzliche Richtlinien beachtet entstehen
- die Anzahl der Querverbindungen steigt und somit die Komplexität und der Verwaltungsaufwand
- interner und externer Namensraum sind nicht mehr unabhängig voneinander

Stammdomäne: AMT.LOCAL

Dieser Ansatz ist unabhängig vom bisherigen Namensraum und kreiert einen neuen internen DNS Namensbaum. Die gewählte Top Level Domain LOCAL wird derzeit nicht im Internet unterstützt. Dieser gewählte Name ist also nicht offiziell registrierbar. Statt LOCAL könnte auch ein nach RFC 2606 geschützter Top Level Domain Name verwendet werden, der niemals Gefahr läuft, von der Internet-Gemeinde als Top Level Domain übernommen zu werden.

Bild 20: Stammdomäne: AMT.LOCAL

Die Vorteile dieser Stammdomäne sind:

- es wird ein neuer Namensbaum geschaffen, so dass keine Altlasten übernommen werden
- bestehende Root Server können beibehalten werden
- die Plattform der DNS Dienste kann gewählt werden
- der User Principal Name des Anwenders ist relativ kurz (Benutzername@amt.local)
- bei Vergrößerung der Gesamtstruktur (z.B. plus DNS-Baum ZUSATZ.DE) sind beide Bäume 2nd Level Domain
- die Namensauflösung hängt in geringem Maße von der bisherigen Infrastruktur ab

Die Nachteile dieser Lösung sind:

- es wird ein neuer Namensbaum geschaffen, so dass neue Strukturen und zusätzliche Richtlinien beachtet entstehen
- interner und externer Namensraum bleiben dauerhaft getrennt
- die Anzahl der Querverbindungen steigt und somit die Komplexität und der Verwaltungsaufwand

Achtung

Ungleich schwieriger wird die Wahl des DNS Namensraumes, wenn die hoheitliche Verwaltung des DNS Namensraumes außerhalb der eigenen hoheitlichen Rechte liegt. Oftmals sind dann die eigenen Erwägungen einem höher angesiedelten Interesse unterzuordnen, wodurch der Entscheidungsprozess merklich verlängern werden kann.

3.7.3.5 Verzeichnisdienst und Schema

Mit Windows 2003 Active Directory wird ein Verzeichnisdienst eingeführt, der sich an den X.500 Standard anlehnt und via LDAP (Lightweight Directory Access Protocol) administriert werden kann.

Der Verzeichnisdienst verwendet einen Datenbanktyp, der ursprünglich für Microsoft Exchange (Extensible Storage Engine) entwickelt worden ist. Die Architektur der SAM Datenbank wird dadurch abgelöst. Die SAM wird jedoch für mögliche NT basierende BDCs weiter bereitgehalten, solange das Active Directory nicht in den so genannten „Native Mode“ geschaltet wird.

Im Schema des Active Directory sind ungefähr 142 (mit Erweiterungen von Exchange 2003, HIS und ISA: 419) verschiedene Klassen von Objekten definiert, denen bis zu 863 (mit E2K, HIS und ISA: 1928) Attribute zugeordnet werden können.

Das Schema kann prinzipiell erweitert werden, auch bestehende Klassen können um neue Attribute erweitert werden.

Die Aufteilung des Active Directory bzw. der Datenbank erfolgt über die Struktureinheit der Domäne. Eine Aufteilung innerhalb der Domäne im Sinne einer dezentralen Datenbank ist also nicht möglich.

Die Replikation des Active Directory bzw. der Datenbank erfolgt zwischen den Domain Controllern (DC). Sie erfolgt anhand so genannter Unique Sequence Number (USN), die bis auf Attributebene herunter verwaltet werden. Die Replikation kann somit auf Attributebene erfolgen. Ändert sich also die Eigenschaft eines Objektes, wird lediglich die Änderung der Eigenschaft und nicht das komplette Objekt repliziert.

Jeder DC im Active Directory stellt einen LDAP Dienst bereit. Es wird die LDAP Version 3 unterstützt. Mit Hilfe eines LDAP Clients kann das Active Directory durchsucht oder administriert werden. Über den Distinguished Name kann das jeweilige Objekt gelesen und geschrieben werden. Beispielhaft sei hier ein LDAP-Pfad angegeben:

LDAP://dc001.behoerde.de/cn=Hans Muster, ou=Unterabteilung, ou=Abteilung, dc=behoerde, dc=de.

Der Name dc001.behoerde.de bezeichnet einen DC (also einen LDAP Server) in DNS Nomenklatur. Die Angabe des LDAP Servers ist bei einigen LDAP Clients optional, sofern diese ein so genanntes „serverless binding“ beherrschen. Im

Prinzip kann eine beliebige LDAP Clientimplementierung, wie z.B. OpenLDAP, bzw. Programmierschnittstelle verwendet werden wie:

- ADSI (Active Directory Services Interface (in Windows 2000 integriert)
- LDIF (LDAP Data Interchange Format)
- u.a.

Problematisch gestaltet sich der Gebrauch dieser Schnittstellen insofern, als dass

- gewisse Attribute oder Objekte werden vom Active Directory hoheitlich verwaltet und können nicht geändert werden (z.B. die Attribute SID oder GUID),
- gewisse Attribute bestehen aus Binär- oder Hash-Werten, deren Ent- und Verschlüsselungsalgorithmen nicht bekannt sind (z.B. das Attribut userParameters) und nur über separate Schnittstellen außerhalb LDAP modifiziert werden können (z.B. Windows Terminal Server API),
- die Verwendung der graphischen Oberfläche (MMC) zusätzliche Prozesse neben dem reinen Schreiben der LDAP Attribute auslöst (z.B. beim Festlegen eines Home-Verzeichnisses wird dieses auf dem File Server mit den entsprechenden Rechten angelegt).

3.7.3.6 ADS als Basis

Windows Active Directory ist zwingend erforderlich für Exchange 2003. Exchange 2003 nimmt eine Erweiterung des Active Directory Schemas vor und speichert seine eigene Konfiguration im AD.

Folgende Microsoft Produkte nutzen das AD zur Speicherung ihrer Konfiguration:

- HIS Server (Host Integration Server)
- ISA Server (Internet Security and Acceleration) im Enterprise Mode

3.7.3.7 Verwaltungsinstrumente

Die Server-Version von Windows 2000 wird mit einer Reihe von graphischen Werkzeugen zur Verwaltung der in Active Directory standardmäßig abgelegten Informationen, wie Benutzer- und Gruppenkonten oder DNS-Konfiguration ausgeliefert. Unter anderem wird hierzu die Microsoft Management Console (MMC) verwendet. Darüber hinaus stehen die aus Windows NT bekannten Werkzeuge für die Kommandozeile zur Verfügung, mit denen Benutzer und Gruppen angelegt, gelöscht und bearbeitet werden können. Über diese Werkzeuge lässt sich jedoch nur ein Teil der in Active Directory gespeicherten Kontoinformationen bearbeiten.

Mit ldifde steht außerdem ein kommandozeilenbasiertes Programm zur Verfügung, mit dem sich Verzeichniseinträge aus einer LDIF- Datei (LDAP Data Interchange Format) erzeugen lassen.

Insgesamt wenden sich die mit Windows 2000 Server gelieferten Verwaltungswerkzeuge eher an erfahrene Windows-Administratoren. Sie eignen sich kaum dazu, einfache administrative Aufgaben, wie das Anlegen oder Verändern von Benutzerkonten an weniger ausgebildete Kräfte zu delegieren.

Mit ADSI (Active Directory Service Interface) existiert eine COM-basierende Schnittstelle, mit der eine Vielzahl von Aufgaben automatisiert werden kann.

3.7.3.8 Zertifikationsdienste

Windows 2003 kann eine Public Key Infrastructure (PKI) als integralen Bestandteil einbinden. Zertifikatsdienste können über Windows Server 2003 eingerichtet und auf Windows XP Clients verteilt werden.

Die PKI ist ein Netzwerkdienst, der Zertifikate erstellt und jederzeit zu dessen Verifizierung genutzt werden kann. Die Validierung von Zertifikaten erfolgt über zentrale Verzeichnisdienste, in den diese Informationen durch die Zertifikatsdienste abgelegt werden. So dass Clients diese zentrale Infrastruktur anfragen.

Grundsätzlich werden Zertifikate zu folgenden Zwecken verwendet:

- Authentisierung
- Verschlüsslung
- Signatur
- Oder Kombinationen aus diesen.

Anwendungsgebiete einer PKI können sein:

- Sichere Authentisierung für Windows Anmeldung oder VPN-Einwahl
- Verschlüsselung von Dateien oder Emails
- Signatur von Dateien oder Emails
- Sichere Kommunikation im Netzwerk (SSL, IPSec)

Die Certification Authority (CA) kann sowohl ins AD integriert als auch separat installiert werden. Wird die AD integrierte Variante gewählt, werden hiermit die Sicherheitstechnologien

- EFS (Encrypted File System)
- IPsec
- SmartCard
- Verschlüsselung und digitale Signaturen (Mail)
- u.a.

im internen Netzwerk unterstützt bzw. ermöglicht.

Die Verteilung bzw. Aktivierung der PKI wird durch Gruppenrichtlinien unterstützt. Dies bedeutet aber nicht, dass ein separates Verwaltungskonzept für den Umgang mit Schlüsseln überflüssig wird.

3.7.3.9 Smart Card

Durch den Aufbau einer internen PKI kann die Benutzer-Authentifizierung via SmartCard erfolgen. Anmeldungen via SmartCard an Windows 2000/XP Rechnern können ohne den Einsatz von Zusatzsoftware realisiert werden.

3.7.4 Ablösende Migration – Samba und OpenLDAP

3.7.4.1 Funktionale Anforderungen

Die zentrale Anforderung an einen Verzeichnisdienst besteht in der schnellen Bereitstellung von Informationen im Netzwerk. Darüber hinaus sollte er folgende Funktionen bieten:

- Möglichkeit zur Änderung der im Verzeichnis bereitgestellten Informationen
- Möglichkeit zur hierarchischen Anordnung der Objekte im Verzeichnis
- Verwendung standardkonformer und weit verbreiteter Schemata zur Gewährleistung hoher Kompatibilität mit möglichst vielen Anwendungen. Möglichkeit zur Erweiterung durch eigene Objekte und Schemata
- Möglichkeit zur Authentifizierung von Benutzern sowie Integration mit anderen Authentifizierungsdiensten (Kerberos)
- Verwaltung von Zugriffsrechten
- Verwendung offener Standards, um hohe Kompatibilität zu möglichst allen Diensten und Anwendungen zu erreichen, welche die im Verzeichnis gespeicherten Informationen nutzen können
- Unterstützung von Replikationsverfahren
- Verwendung sicherer Übertragungsprotokolle bei der Übermittlung von Informationen zwischen Client und Verzeichnisdienst sowie bei der Replikation

3.7.4.2 Betrachtete Produkte

Soll eine Windows-NT Domäne durch einen Verzeichnisdienst auf der Basis von Microsoft Windows oder Linux ersetzt werden, kommen in erster Linie die folgenden Produkte in Frage:

- Active Directory mit Windows 2000/2003 Server
- OpenLDAP und Samba (optional mit Kerberos) unter Linux

Andere Verzeichnisdienste, wie Novell Directory Services oder SunONE, werden hier nicht betrachtet, weil sie die Einführung zusätzlicher Produkte erfordern und dadurch die Komplexität Windows- bzw. linuxbasierter IT-Umgebungen weiter erhöhen.

3.7.4.3 Genereller Vergleich des Funktionsumfangs von NTDS, Active Directory und OpenLDAP

Tab. 21 Vergleich Verzeichnisdienste

Funktion	WinNT	Win2k / ADS	Linux / OpenLDAP
Client ohne Zusatzsoftware	X	X	X
Möglichkeit zum hierarchischen Aufbau des Verzeichnisses		X	X
Erweiterbarkeit durch eigene Attribute und Objektklassen		X	X
Zeichensatz für Verzeichnisdaten	Unicode	Unicode	Unicode
Zugriffsmöglichkeit auf das Verzeichnis per Standard-Protokoll (LDAP)		X	X
Sichere Zugriffsmöglichkeit per LDAP über SSL/ TLS		X	X
Unterstützung des „starttls“ Protokolls		X	X
Unterstützung für SASL			X
Authentifizierung von NT Clients	X	X	über Samba[1]
Authentifizierung von W2K Clients	X	X	über Samba[2]
Authentifizierung von Linux Clients	Über winbind	Über winbind oder LDAP	X
Möglichkeit zur Integration von Kerberos		X[3]	X
Möglichkeit zur Verwendung eines unabhängigen / übergeordneten Kerberos-Dienstes		X[4]	X
Verwaltung von Zugriffsrechten (ACLs) für Attribute und Objekte		X	X
Delegation von Verwaltungsaufgaben		X	X
Master-Slave-Replikation	X	X[5]	X
Multi-Master-Replikation		X[6]	X[7]

1 Bei der Verwendung von Samba zur Authentifizierung von Windows Clients gegen OpenLDAP wird zwischen Windows-Client und Samba-Server das NT-LAN-Manager Protokoll verwendet.

2 Bei der Verwendung von Samba zur Authentifizierung von Windows Clients gegen OpenLDAP wird zwischen Windows-Client und Samba-Server das NT-LAN-Manager Protokoll verwendet.

3 Kerberos ist fest in Active Directory integriert.

4 Active Directory erlaubt die Authentifizierung gegen einen externen Kerberos-Server, allerdings lassen sich Active-Directory-Domänen dann nicht mehr zur Authentifizierung von Windows 95/98/Me/NT-basierten Rechnern verwenden.

5 Active Directory verwendet im „Mixed Mode“ Master-Slave-Replikation zwischen Windows 2000 DC und Windows NT 4 BDC

6 Active Directory verwendet im „Native Mode“ (in dem ausschließlich Windows 2000/2003 basierte Domänencontroller verwendet werden) Multi-Master-Replikation.

7 Die Multi-Master-Replikation in OpenLDAP gilt als experimentell und ist standardmäßig nicht eingeschaltet.

3.7.4.4 Authentifizierung mit Linux / OpenLDAP und Samba

Die Themen Authentifizierung und Verzeichnisdienst sind schwerlich voneinander zu trennen. Da ein Verzeichnisdienst aber mehr Aufgaben als die Authentifizierung übernehmen kann und die Authentifizierung ein Infrastrukturdienst ist, wird zum einen die Authentifizierung im Zusammenspiel von Linux, Samba und OpenLDAP und zum anderen auch noch im Zusammenspiel mit Windows und ADS im Kapitel 3.4 „Authentisierungsdienste“ betrachtet.

3.7.4.5 Zentrale Verwaltung von Host-Informationen mit Linux und OpenLDAP

Durch die zentrale Verwaltung von Host-Informationen in einem Verzeichnis lassen sich eine Reihe von administrativen Aufgaben deutlich vereinfachen. Dazu gehören:

- Inventarisierung der vorhanden Hardware
- Erstellung und Verwaltung von DNS-Namenseinträgen
- Erstellung von Verwaltung von DHCP-Konfigurationen
- Für Windows-Clients können Maschinen-Accounts gemeinsam mit den oben genannten Informationen gespeichert werden
- Ferner ist es möglich, beliebige weitere Host-spezifische Informationen in einem Verzeichnis zu speichern, wie beispielsweise Informationsprofile zur automatischen Installation eines Clients.

Darüber hinaus müssen diese Informationen nicht manuell oder über andere Verfahren auf mehrere Rechner verteilt werden, sondern können per LDAP-Replikation auf die betreffenden Systeme distribuiert werden.

Unter Linux stehen mittlerweile eine Reihe von Programmen zur Verfügung, mit denen Host-Informationen direkt aus einem LDAP-Verzeichnis gelesen werden können:

- Für den Standard DHCP-Server (ISC DHCPD) gibt es einen Patch, mit dem die DHCP-Konfiguration aus einem LDAP-Verzeichnis gelesen werden kann
- http://home.ntelos.net/~masneyb/dhcp-3.0.1rc11-ldap-patch
- Für BIND 9 gibt es ebenfalls einen Patch, mit dem Zonendateien durch LDAP ersetzt werden
- http://www.venaas.no/dns/bind/bind-sdb/
- Samba kann Informationen für Maschinen-Accounts direkt aus dem LDAP-Verzeichnis beziehen

Darüber hinaus gibt es eine Reihe proprietärer und freier Softwareprodukte, mit denen die BIND- und DHCP-Konfiguration transparent aus dem LDAP-Verzeichnis erzeugt werden kann.

3.7.4.6 Integration anderer Anwendungen

Neben der Verwendung von Verzeichnisdiensten zur zentralen Speicherung von Benutzer-, Gruppen- und Host-Informationen, steigt der Nutzen von Anwendungen durch den Zugriff möglichst vieler anderer Applikationen. Auf eine vollständige Liste LDAP-kompatibler Anwendungen wird an dieser Stelle verzichtet. Wichtig ist jedoch der Hinweis, dass immer mehr Applikationen LDAP-Unterstützung aufweisen, nicht zuletzt die Microsoft E-Mail-Programme Outlook und Outlook-Express oder das Office-Paket OpenOffice. Diese Anwendungen können sowohl mit OpenLDAP als auch mit Active Directory als Verzeichnisdienst arbeiten.

3.7.4.7 Administrationswerkzeuge

Zur Verwaltung der in einem Verzeichnis gespeicherten Informationen stehen unter Linux zum einen die standardmäßigen LDAP-Werkzeuge (ldapsearch, ldapadd, ldapmodify) zur Verfügung. Diese eignen sich vor allem zur Initialisierung eines Verzeichnisses, zum Datenimport, zur schnellen Suche nach Verzeichnisinhalten sowie zur automatisierten Bearbeitung eines Verzeichnisses. Zur Benutzer- und Gruppenverwaltung stehen ebenfalls einige kommandozeilenbasierte Werkzeuge bereit.

Freie graphische Werkzeuge zur verzeichnisbasierten Benutzer- und Gruppenverwaltung unter Linux befinden sich zurzeit in der Entwicklung (z.B. directory-administrator: http://diradmin.open-it.org/files.php).

Ebenso wichtig und viel flexibler sind webbasierte Werkzeuge zur Verwaltung von Benutzer-, Gruppen- und Maschinenkonten und anderen Objekten (Mailing-Listen, DNS-Einträgen usw.) innerhalb von Verzeichnisdiensten. Der Vorteil dieser Lösungen ist, dass sie mit einem Web-Browser unabhängig vom Server verwendet werden können, wobei eine sichere Datenübertragung (SSL/TLS) genutzt werden kann[1].

3.7.4.8 Laufzeitverhalten und Ressourcenverbrauch

Linux und OpenLDAP hat sich in sehr großen Umgebungen mit mehr als 70.000 Benutzern als stabil und hinreichend performant erwiesen. Samba hat sich in verschiedenen Tests und großen Installationen als sehr zuverlässig, stabil und – im Vergleich zu windowsbasierten Servern – ressourcenschonend erwiesen.

3.7.4.9 Nutzerakzeptanz

Verzeichnisdienste sind für die Endbenutzer zunächst unsichtbar und werden erst langsam mit der Anbindung von Applikationen an das Verzeichnis sichtbar. Je mehr Anwendungen das Verzeichnis nutzen, desto höher ist die Wahrschein-

[1] Beispiele sind das Webmin-Modul (http://www.webmin.com/) idxldapaccounts (http://webmin.idealx.org/).

lichkeit, dass Benutzer mit konsistenten Daten konfrontiert werden, wodurch die Akzeptanz steigen wird.

Die Migration auf die Kombination Samba/OpenLDAP kann für Benutzer und Clients transparent geschehen, so dass diese von dem Wechsel nichts mitbekommen und sich für sie keine Änderungen ergeben.

Administratoren profitieren von einem Verzeichnisdienst durch die Einführung eines Single-Point-of-Administration. Dieser kann umso besser genutzt werden, je besser die verfügbaren Verwaltungswerkzeuge an das Ausbildungsprofil und die täglichen Aufgaben der Administratoren angepasst sind.

3.7.5 Fortführende Migration – Einführung ADS

Die Migration der Anmeldedienste von Windows NT 4 nach Windows Active Directory bedarf in der Regel eines separaten Konzeptes und praktischer Tests, bevor abschließend der optimale Pfad bestimmt werden kann. Im Folgenden wird dennoch kurz erläutert, wie solch eine Migration aussehen kann, um einen Eindruck von den zu erwartenden Aufwänden und technischen Randbedingungen zu erhalten.

3.7.5.1 Reihenfolge

Die Migration von Windows NT nach Windows 2003 ist hinsichtlich der Abfolge sehr variabel gehalten. So besteht keine zwingende Notwendigkeit, zuerst die Anmeldedienste und dann die Clients zu migrieren oder umgekehrt. Es ist auch nicht erforderlich, eine Vielzahl von Windows NT Clients in einem Massen-Rollout umzustellen. Lediglich wenn die Aktualisierung einer existierenden NT Domäne (Inplace Upgrade) vorgesehen ist, dann ist zuerst der PDC dieser Domäne auf Windows 2000 zu aktualisieren.

Active Directory unterscheidet zwei Betriebsmodi: Mixed und Native Mode. In den Native Mode kann erst umgeschaltet werden, wenn keine NT BDCs in der Domäne mehr vorhanden sind. Die Umschaltung in den Native Mode ist nicht rückgängig zu machen. Der Native Mode ist aber für ein Migrationsszenario mit Restrukturierung (siehe Abschnitt „Variante 2: Aktualisierung plus Restrukturierung“ im Kapitel 3.7.5.3) notwendig.

3.7.5.2 Zielarchitektur

Das Ziel sollte eine möglicht einfach gestaltete Active Directory Struktur mit einer Domäne bzw. möglichst wenigen Domänen sein. Die Delegation der einzelnen Berechtigungen kann auch über eine geeignete OU Struktur realisiert werden. Hierfür ist nicht mehr zwingend der Aufbau von mehreren Domänen notwendig. Eine geringe Anzahl von Domänen verspricht in der Regel die geringsten Betriebsaufwände.

Bild 21: Migration durch Upgrade oder Restrukturierung

Dies entspricht den Design-Empfehlungen von Microsoft, da Microsoft hinsichtlich einer Migration von NT nach Windows 2000/2003 bereits eine große Flexibilität der Migrationspfade und ein hohes Maß an Restrukturierungsmöglichkeiten vorgesehen hat.

3.7.5.3 Übersicht der Migrationsvarianten

Es existieren folgende grundsätzlich verschiedene Migrationsvarianten:

- Reine Aktualisierung (Upgrade): Die bisherige Domänenstruktur soll beibehalten werden. Alle Domänen werden also aktualisiert.
- Aktualisierung (Upgrade) und Restrukturierung: Eine oder mehrere Domänen werden aktualisiert. Verbleibende NT Domänen werden in die Struktur eingepasst.
- Neue Domäne und Restrukturierung: Keine Domäne wird aktualisiert. Eine oder mehrere neue Domänen eines ADS dienen als Ziel einer Restrukturierung der NT Domänen.
- Parallelwelt plus Migration der Ressourcen: Keine Domäne wird aktualisiert oder restrukturiert. Es werden lediglich die Ressourcen (Daten, Drucker etc.) migriert (kopiert).

Variante 1: Reine Aktualisierung

Eine reine Aktualisierung (Inplace Upgrade alle Domänen) würde die Beibehaltung der jetzigen Domänenstruktur bedeuten. Eine spätere Restrukturierung der einzelnen Domänen ist weiterhin möglich (so genannte Intra-Forest-Restrukturierung).

Variante 2: Aktualisierung plus Restrukturierung

Die Aktualisierung oder Inplace-Migration beinhaltet die Anhebung der Account-Domäne auf Windows 2003. Im Anschluss findet die so genannte Inter-Forest-Restrukturierung (bedeutet die Auflösung der Ressourcen Domänen) statt.

Bild 22: Migration ADS – Aktualisierung plus Restrukturierung

Variante 3: Neue Domäne plus Restrukturierung

Zunächst wird eine neue Domäne bzw. ein neues AD aufgesetzt.

Bild 23: Migration ADS – Neue Domäne plus Restrukturierung

Die Benutzerkonten und die globalen Gruppen der Account-Domäne werden in die neue (Ziel-) Domäne geklont (inkl. SID-History).

Bild 24: Migration ADS – Klonen von Benutzern und Gruppen

Vorteile dieser Vorgehensweise sind:

- unterbrechungsfreie Migration für den Benutzer
- sehr gutes Fall Back
- das Neuschreiben der Rechte (ReACLing) ist verschiebbar bzw. zeitlich unkritisch

Nachteil ist:

- zusätzliches ADS inkl. Hardware für die neue Domänenstruktur muss vorhanden sein.

Variante 4: Parallelwelt und Migration der Ressourcen

Zunächst wird eine neue Domäne bzw. ein neues ADS aufgesetzt.

Bild 25: Migration ADS – Parallelwelt und Migration der Ressourcen

Die parallele Welt wird mit neuen Benutzerkonten und Gruppen gefüllt. Die bisherigen Ressourcen werden in die neue Welt kopiert.

Bild 26: Migration ADS – Füllen der parallelen Welt mit Benutzerkonten und Gruppen

Vorteile sind:

- keine zeitkritische Migration von Servern
- keine SID History

- Zugriffsrechte müssen bekannt sein und in der neuen Welt „nachgeahmt“ werden
- Datenmigration kann Datenreduktion bedeuten

Nachteile sind:

- die Migration der Daten erfordert hohen logistischen Aufwand hinsichtlich des gemeinsamen Zugriffs
- zum Zeitpunkt der Datenmigration müssen zusätzliche Hardware-Geräte vorhanden sein

3.7.5.4 Migrationsaufgaben

Die Migration (Ablösung von NT) oder auch die komplette Neueinführung von Windows 2003 Active Directory bedarf sorgfältiger Planung und der Validierung in Testumgebungen um einen reibungslosen Ablauf der Migration gewährleisten zu können.

Folgende Aufgaben sind innerhalb eines Migrationsvorhabens zu erledigen:

- Aufnahme der bestehenden Infrastruktur in schriftlicher Form
- Ermittlung der Anforderungen an eine neue Umgebung
- Ermittlung der technischen und organisatorischen Randbedingungen
- Bewertung der aktuellen Umgebung
- Konzept der zukünftigen Gesamt- und Domänenstruktur
- Festlegung des DNS Namensraumes und des NetBIOS Namensraumes
- Festlegung der Standorte und Platzierung der Domain Controller
- Erstellung eines umfassendes Namenskonzeptes
- Anbindung an andere Verzeichnisdienste
- Konzeption der OU Struktur
- Migrationskonzept für Anmeldeserver, Ressourcen, Applikationen und Arbeitsplatzsysteme

3.7.5.5 Active Directory hinsichtlich Windows 2003

Die grundsätzliche Architektur des Active Directory wurde mit dem Nachfolgeprodukt Windows 2003 beibehalten.

Einige Änderungen gegenüber Windows 2000 seien hier dennoch erwähnt:

- Es wurde neben den bisherigen Typen (schema, configuration, domain) ein zusätzlicher Partitionstyp eingeführt: die Application Partition. Dieser Partitionstyp wird nicht mehr zwingend auf alle DCs einer Domäne repliziert. Dadurch können für Anwendungen von Drittherstellern eigene Partitionen erstellt werden, in denen verstärkt dynamische Daten abgelegt werden können. Diese dynamischen Daten können dann hinsichtlich der

Replikation verbessert kontrolliert werden. Die AD integrierten DNS Daten des Active Directory werden in eine solche Partition verlagert.

- Windows 2003 wird aller Voraussicht nach die Möglichkeit bieten, separate LDAP Server aufzubauen, ohne einen DC installieren zu müssen. Diese LDAP Server (ADAM= Active Directory Application Mode) verfügen über ein eigenes Schema, unterwerfen sich aber den Anmeldediensten des AD. So wird es möglich, LDAP Dienste für Anwendungen zu bauen, ohne auf Änderungen des AD Schemas angewiesen zu sein.

3.7.5.6 Active Directory: Minimale Ausprägung

Wie bereits beschrieben, bietet ein Active Directory in seiner Gesamtheit eine Vielzahl von Technologien und Funktionalitäten, die es prinzipiell erleichtern, neue Funktionen und/oder effiziente Betriebsverfahren in IT Landschaften auszurollen. Die Abhängigkeit von Microsoftprodukten bzw. –technologien steigt in solchen Fällen an.

Sofern dies nicht gewünscht ist, kann folgendes Ziel formuliert werden: ein Windows Active Directory mit minimaler Ausprägung. Im folgenden wird kurz beschrieben, wie solch eine Konstellation aussehen kann.

Ein Active Directory mit minimaler Ausprägung hat folgende Eigenschaften bzw. unterliegt folgenden Maßnahmen:

- Auf die Bildung einer einzigen Gesamtstruktur wird verzichtet. Vertrauensstellungen zwischen Domänen werden auf die herkömmliche Art realisiert.
  Zweck: jede bisherige Windows NT Domäne kann ihr eigenes Schema in einer eigenen Gesamtstruktur verwalten.
- Werden darüber hinaus die Domänen nicht in den „Native Mode“ geschaltet, reduziert sich die „Gefahr“, die damit verbundenen, erweiterten Gruppen zu nutzen.
- Auf den Aufbau einer OU-Struktur innerhalb der Domänen wird ebenfalls verzichtet.
  Zweck: durch solch eine Struktur werden zusätzliche Funktionen möglich, auf die „dann doch“ zurückgegriffen werden könnte.
- Der Einsatz von Gruppenrichtlinien wird auf die Sicherheitseinstellungen (z.B. Kennwort (Laufzeit, Mindestlänge etc.), Privilegien (Ändern der Systemzeit, Lokale Anmeldung etc.), Überwachungseinstellungen (Auditing)) in der „Default Domain Policy“ begrenzt. Diese sind notwendig, um die Einstellungen von Windows NT adäquat zu ersetzen.
  Zweck: durch ein fehlendes Konfigurationsmanagement der Clients via Gruppenrichtlinien wird die Abhängigkeit reduziert.
- Auf den Einsatz einer AD basierenden PKI (Public Key Infrastructure), die z.B. für EFS oder IPsec erforderlich wäre, wird grundsätzlich verzichtet.

Zweck: Vermeidung zusätzlicher Abhängigkeiten, die durch die integrierte Speicherung im AD entstehen würden.

- Einsatz eines AD-basiertes DFS (Distributed File System)
  Zweck: Vermeidung einer zusätzlichen Abhängigkeit, die durch die integrierte Speicherung im AD entstehen würde.
- Sofern kein Exchange 2000 eingesetzt wird, bleiben die zusätzlichen Attribute der Benutzerobjekte ungenutzt bzw. auf die obligatorischen Attribute beschränkt.
  Zweck: das AD wird nicht als Speicher von Personendaten verwendet, dies reduziert mögliche Folgeabhängigkeiten (z.B. Drittanwendungen, die diese Daten per LDAP abfragen).
- Kontaktobjekte im AD werden nicht verwendet.
  Zweck: Die Anhäufung solcher Informationen im AD erhöht die Abhängigkeit.
- Die Veröffentlichung von Druckern oder Freigaben im Active Directory unterbleibt.
  Zweck: Anwender sollen sich nicht daran gewöhnen, Ressourcen auf diese Weise zu finden.

Hinweis: Die genannten Eigenschaften/ Maßnahmen verhindern die maximale Effizienz, dem Einsatz der neuen Technologien erreicht werden kann. Dies ist der Preis für eine erhöhte Unabhängigkeit.

Die Verwendung von Standorten innerhalb des ADS ist hingegen sinnvoll, um die Replikation zwischen den einzelnen Lokationen zu steuern.

Beim Einsatz von Exchange 2003, das domänenübergreifend in einer einzigen Exchange Organisation arbeiten soll, ist allerdings der Einsatz einer einzigen Gesamtstruktur nicht zu umgehen, da pro Exchange Organisation nur eine Gesamtstruktur von Windows Active Directory unterstützt wird.

3.8 XML (Extensible Markup Language)

3.8.1 Allgemeines

XML ist die Abkürzung von "eXtensible Markup Language" (Erweiterbare Auszeichnungssprache). Eine Auszeichnungssprache dient **zur Kennzeichnung der Strukturen (elektronischer) Dokumente in ihrer Textrepräsentation** (beispielsweise als Inhalt einer Datei). Markantestes Merkmal von XML-Dateien sind auf den ersten Blick die von spitzen Klammern eingeschlossenen XML-"Tags", die die einzelnen Struktur-Elemente markieren[1]. Das folgende Beispiel zeigt eine mögliche XML-Auszeichnung eines Briefes:

[1] Die in den Beispielen gezeigten Einrückungen sind kein Merkmal von XML, sondern dienen allein der Verdeutlichung der Dokument-Struktur.

```
<?xml version="1.0" ?>
<brief>
  <absender>
   <zeile>Andrea B. Sender</zeile>
   <zeile>Hierstrasse 11</zeile>
   <zeile>00000 Daselbstsbüttel</zeile>
  </absender>
  <empfaenger>
   <zeile>Ernst M. Pfenger</zeile>
   <zeile>Anderswoallee 187</zeile>
   <zeile>99999 Dorthausen</zeile>
  </empfaenger>
  <datum>31.02.2005</datum>
  <anrede>Lieber Ernst!</anrede>
  <brieftext>
   <absatz>Habe ich Dir schon berichtet, dass...</absatz>
  </brieftext>
  <grussformel>Bis bald, Deine Andrea</grussformel>
</brief>
```

Ein solcher Brief ist ein Dokument im alltäglichen Sinne, wie es häufig als "narratives Dokument" bezeichnet wird. XML-Dokumente können aber auch den Charakter eine Datentabelle oder Datenbank haben, wie das folgende Beispiel einer Telefonliste zeigt:

```
<?xml version="1.0" encoding="UTF-8"?>
<telBuch>
  <telBuchEintrag>
    <vollerName>Klaus Meier</vollerName>
    <telefonNr>123</telefonNr>
  </telBuchEintrag>
  <telBuchEintrag>
    <vollerName>Petra Schulz</vollerName>
    <telefonNr>456</telefonNr>
  </telBuchEintrag>
</telBuch>
```

Bereits ein erster unbefangen-phänomenologischer Blick auf diese Beispiele zeigt, dass Auszeichnungen ganz unterschiedlichen Zwecken dienen können. Im Brief geben die XML-Tags offenbar Hinweise darauf, wie der Brief zu Papier gebracht werde soll. Beispielsweise setzen sich Absender- und Empfängeranschrift aus einzelnen Zeilen zusammen, der Brieftext scheint dagegen aus beliebig umbrechbaren Fließtext-Absätzen zu bestehen. Aus welchen Teilen sich eine Anschrift zusammensetzt (Vorname, Straße, Stadt), spielt hier offenbar keine Rolle. Die Telefonliste enthält hingegen keinerlei erkennbare Hinweise auf die intendierte Darstellung, sondern kennzeichnet augenscheinlich die Semantik der im Dokument enthaltenen Daten.

Ein genauerer Blick auf die Struktur der Beispiele zeigt: die optische Ähnlichkeit, mit dem vertrauten HTML, derentwegen XML häufig als dessen "Weiterentwicklung" bezeichnet wird, trügt. So haben XML-Dokumente eine konsequent hierarchische Struktur: zu jedem öffnenden Tag, wie z.B. "<telBuch>", existiert auch ein spiegelbildlicher schließender Tag, z.B. "</telBuch>", es sei denn, es handelt sich um einen leeren Tag, der sich selbst gleich wieder schließt, z.B. "<telBuch/>". Öffnende Tags, die nie wieder geschlossen werden (wie "<hr>" in HTML) sind also nicht zulässig. Die hierarchische Struktur hat genau einen Wur-

zelknoten, im gezeigten Beispiel "<telBuch>" (analog zu "<html>"). Alles, was in einer XML-Datei steht, hat seinen eindeutigen Platz in dieser hierarchischen Struktur. Die "<p>"-Elemente in HTML können hingegen zu mehrdeutigen Strukturen führen.

Ein derart strukturiertes XML-Dokument kann nicht nur als Dateiinhalt existieren, sondern beispielsweise auch als Zeichenstrom, der zwischen zwei Anwendungsprozessen ausgetauscht wird[1]. Ein solcher Zeichenstrom enthält nach wie vor die im Beispiel gezeigten Tags. Datei wie Zeichenstrom sind Text-Repräsentationen des Dokumentes. Der Inhalt des Dokumentes kann aber auch in geeigneter Weise im Arbeitsspeicher eines Computers abgelegt werden, um dort auf irgendeine Weise verarbeitet zu werden. Eine solche Repräsentation des Dokumentes umfasst zwar noch die Daten, wie "Klaus Meier" und "123", die auszeichnenden Tags sind jedoch in aller Regel nicht mehr Teil dieser Repräsentation. Da XML eine Auszeichnungssprache ist, handelt es sich bei einer solchen internen Repräsentation des Dokumentes bei Wegfall der Auszeichnung streng genommen nicht mehr um ein XML-Dokument.

Die durch XML-Auszeichnung ausgedrückte Struktur kann aber auch auf verschiedene andere Arten beschrieben werden. Abstrahiert vom Inhalt einer XML-Datei bietet sich eine verschachtelte Sichtweise an, wie sie die folgende Abbildung zeigt, abermals anhand der Telefonliste:

Bild 27: Behälter-orientierte Struktur-Interpretation

Ebenso gut kann das gleiche Dokument als Baumstruktur verstanden werden, wie die nächste Abbildung zeigt: Eine baumorientierte Sicht macht sich das Document Object Model (DOM) zu eigen. Es ist ein Programmiermodell für die Bearbeitung hierarchisch strukturierter Dokumente, typischerweise als Anwendungs-interne Repräsentation im Arbeitsspeicher eines Computers. Da DOM auf verschiedene Weise eng mit XML verbunden ist, kann man DOM etwas salopp auch als "XML im Arbeitsspeicher" bezeichnen.

[1] Die in Kapitel 3.9.4 vorgestellten Web Services basieren typischerweise auf dem Austausch von XML-Zeichenströmen.

Bild 28: Hierarchische Strukturinterpretation

Noch ein weiteres wichtiges Merkmal von XML wird durch einen Vergleich der gezeigten Beispiele mit dem Inhalt einer beliebigen HTML-Datei deutlich. Die Tags einer HTML-Datei, wie "<html>", "<body>", "<h1>" oder "<p>", sind Teil von HTML. Die im Beispiel gezeigten Tags "<telBuch>", "<telBuchEintrag>" etc. dagegen sind jedoch nicht Teil von XML. XML schreibt im Wesentlichen lediglich die hierarchische Struktur vor. Jedes XML-Dokument, das irgendwelche Elemente in einer solchen Struktur anordnet, ist zunächst einmal syntaktisch korrekt und wird als "wohlgeformt" (well-formed) bezeichnet. Tatsächlich definiert XML als solches überhaupt keine Elemente. Während HTML die Struktur und Gestaltung von Web-Dokumenten beschreibt, ist XML als solches gewissermaßen eine Sprache ohne Worte. XML wird deshalb oft auch als **Meta-Auszeichnungssprache**[1] bezeichnet.

Eine konkrete XML-Auszeichnungssprache wird auch als **XML-Anwendung** bezeichnet. Sie definiert

- einen Wortschatz, nämlich die Elemente, die verwendet werden dürfen[2], wie eben z.B. "telBuch",
- eine Syntax, nämlich welche Daten die Elemente aufnehmen und in welcher Weise sie verschachtelt werden dürfen, z.B. dass "telBuch" eines oder mehrere "telBuchEintrag", und dass "telefonNr" nur Ziffern und bestimmte Sonderzeichen enthält, und
- eine Semantik, nämlich dass der Inhalt eines "telefonNr"-Elementes eine Telefonnummer ist.

---

[1] Unter einer Meta-Sprache wird häufig eine 'Sprache zur Beschreibung von Sprachen' verstanden. Diese Funktion haben im XML-Kontext jedoch die unten beschriebenen XML-Schemata. XML selbst kann demgegenüber als eine Art Strukturbaukasten verstanden werden.

[2] Sie beschreibt darüber hinaus die Attribute, die Tags haben dürfen oder müssen. Attribute eines Tags werden als Schlüssel-Wert-Paare im Tag notiert. Um einen Telefonbuch-Eintrag als öffentlich sichtbar zu kennzeichnen, kann z.B. die Attributierung '<telBuchEintrag oeffentlich="ja">' verwendet werden. Attribute werden im Rahmen des Leitfadens nicht näher behandelt.

XML-Anwendungen sind das Merkmal, dessentwegen XML das "X" (wie "eXtensible") im Namen führt. Tatsächlich ist eine XML-Anwendung jedoch offensichtlich keine Erweiterung von XML, sondern eine Vervollständigung oder Anreicherung.

Eine XML-Anwendung muss nicht immer explizit formuliert werden. Das gezeigte Telefonlisten-Beispiel macht dies deutlich: Elemente, intendierte Struktur und Semantik erschließen sich zumindest dem menschlichen Betrachter ohne weiteres aus dem Dokument selbst, wenn auch nicht unbedingt vollständig.

Zur formalen und maschinell verarbeitbaren Beschreibung der Elemente und ihrer möglichen Verschachtelung dienen Dokumenttyp-Definitionen (DTDs) oder XML- **Schemata** [1]. Dokumente, die die Vorschriften eines solchen Schemas einhalten, sind "gültig" (valid) und werden auch als **Anwendungsinstanz** bezeichnet. Schemata werden von verschiedenen XML-Werkzeugen verwendet. XML-**Parser** lesen XML-Dokumente als Zeichenstrom und können sie zugleich anhand eines Schemas validieren. Interaktive XML- **Editoren** nutzen Schemata, um dem Anwender beispielsweise vorschlagen zu können, welche Elemente er an einer bestimmten Position in der Struktur des Dokumentes einfügen darf.

Ein explizites XML-Schema für das vorgestellte Telefonbuch könnte beispielsweise so aussehen[2]:

---

1 "XML-Schema" wird in diesem Leitfaden als Sammelbegriff sowohl für DTDs als auch für unterschiedliche Schema-Sprachen gebraucht, da ihre Unterscheidung in diesem Rahmen nicht von Belang ist. Unterschiede zwischen den Schema-Sprachen liegen sowohl in ihren Ausdrucksmöglichkeiten als auch hinsichtlich ihrer formalen Struktur; häufig sind Schema-Sprachen selbst XML-Anwendungen. DTDs sind ein Teil von XML, während es sich bei allen anderen Schema-Sprachen um selbständige Lösungen handelt. Daher gibt es nur eine 'echte' DTD-Sprache, aber mehrere Schema-Sprachen. Die gegenwärtig wichtigsten Schema-Sprachen sind das (modulare) W3C XML Schema (http://w3c.org/XML/Schema) und (z.T. auf dessen Modulen aufbauend) RELAX NG (http://www.relaxng.org). Schemata unterstützen in der Regel die sogenanntenNamespaces, innerhalb derer Bezeichner von Elementen oder (den im Leitfaden nicht behandelten) Attributen Gültigkeit haben. Namespaces werden im Leitfaden nicht näher behandelt.

2 Das zuvor gezeigte Telefonbuch-Dokument würde in der Praxis um eine explizite Referenz auf dieses Schema ergänzt werden.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="telBuch">
   <xs:complexType>
     <xs:sequence minOccurs="0" maxOccurs="unbounded">
      <xs:element name="telBuchEintrag">
        <xs:complexType>
          <xs:sequence>
           <xs:element name="vollerName" type="xs:string"/>
           <xs:element name="telefonNr" type="xs:string"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
     </xs:sequence>
   </xs:complexType>
  </xs:element>
</xs:schema>
```

Wie erwähnt beschreiben Schemata nur das Vokabular und die Syntax einer XML-Anwendung. Vergleichbare formale Mittel und technische Unterstützung für die Definition der Semantik einer XML-Anwendung gibt es jedoch nicht.

Bild 29: Eingabeunterstützung und Konsistenzprüfung anhand des Schemas: typischer XML-Editor

Die Notwendigkeit, eine Meta-Sprache anzupassen und dadurch erst eine konkrete Auszeichnungssprache zu erzeugen, ist keine XML-spezifische Neuerung. XML erbt dieses Merkmal vielmehr von seinem Vorläufer **SGML** (Structured General Markup Language). XML ist eine aufs Wesentliche reduzierte SGML, und insofern deren Nachfolger. HTML dagegen ist eine Anwendung im beschriebenen Sinne, allerdings von SGML. Die optische Verwandtschaft zwischen XML und HTML ist insofern kein Zufall[1].

[1] XHTML ist, kurz gesagt, ein Nachbau von HTML mit den Mitteln von XML.

Häufig wird unter "XML" nicht nur XML selbst verstanden, sondern eine große und stetig wachsende Familie weiterer Spezifikationen, von denen viele ihrerseits XML-Anwendungen sind und aufeinander aufbauen. Die Zielsetzung dieser Spezifikationen variiert in großer Breite. Sie reicht von der Lösung generischer Teilprobleme, die sich bei der Verarbeitung von XML-Dokumenten ergeben, bis hin zu selbständigen XML-Anwendungen:

- XPath ist ein hierarchisches Strukturmodell für XML-Dokumente und eine Sprache, mit der einzelne Elemente oder Teilstrukturen innerhalb eines solchen Dokumentes identifiziert werden können. XPath-Ausdrücke sind den absoluten und relativen Pfaden vergleichbar, mit denen Dateien in einem Dateisystem identifiziert werden. Allerdings gehen die Ausdrucksmöglichkeiten von XPath weit darüber hinaus. XPath ist im Kontext von XSL entstanden, ist aber eine selbständige Spezifikation und findet zahlreiche andere Anwendungen,
- XSLT ("eXtensible Stylesheet Language Transformation") ermöglicht die Transformation eines XML-Dokumentes in ein anderes Dokument. Dieses Zieldokument kann seinerseits ein XML-Dokument sein, aber auch beispielsweise ein HTML-, TeX-, PDF- oder ein simples Textdokument. Die Transformation wird durch so genannte Stylesheets gesteuert. Die "eXtensible Stylesheet Language" (XSL) ist ihrerseits eine XML-Anwendung und benutzt XPath, um die Transformationsregeln zu definieren. XSLT und XSL-FO haben ihren gemeinsamen Ursprung in XSL ("eXtensible Stylesheet Language"); "XSL" und "XSLT" werden häufig synonym gebraucht.
- XSL-FO ("XSL Formatting Objects") dienen zur abstrakten Beschreibung gestalterischer Merkmale wie Schriftarten, Textauszeichnungen, Seitenränder, Einrückungen etc. Beispielsweise kann XSL-FO als Zwischenformat komplexer Transformationen verwendet werden, z.B. von einem XML- in ein PDF-Dokument.

Diese Liste zeigt nur einen kleinen Ausschnitt einer beeindruckenden und stetig wachsenden Zahl von Technologien. Weitere Informationen zum für sich genommen schon umfangreichen Kernbereich von XML finden sich auf der Website des W3C (http://www.w3.org). Ein lohnender Einstieg in die vertiefende Lektüre ist die XML-Website des O'Reilly-Verlages (http://www.xml.com). Ein Highlight ist hier die "Annotated XML Specification"[1]. Mit sowohl historischen wie technischen Anmerkungen und kleinen Beispielen gibt sie auch dem Nicht-Spezialisten unter den Lesern wenigstens eine kleine Chance, sich die ursprüngliche XML-Spezifikation zu erschließen.

[1] http://www.xml.com/axml/testaxml.htm

3.8.2 Vorteile und Schwächen

Ein großer Vorzug von XML als Dateiformat ist offensichtlich: Der Inhalt von XML-Dateien ist prinzipiell **für den menschlichen Betrachter lesbar**. Das ist keineswegs selbstverständlich. Viele gebräuchliche Dateiformate sind Abbilder der Bits und Bytes, mit denen eine Anwendung ihre Daten im Arbeitsspeicher organisiert. Diese meist als Binärformate bezeichneten Dateiformate sind zwar für die fragliche Anwendung zugänglich, für das menschliche Auge sind sie jedoch in der Regel nicht zu entschlüsseln.

Dass eine XML-Repräsentation von Daten unmittelbar von Menschen betrachtet und bearbeitet werden kann, ist im Alltag eher eine Ausnahme. Wie andere Formate auch werden XML-Dateien in der überwiegenden Mehrzahl der Fälle von Anwendungen erzeugt, geschrieben und gelesen, die die damit verbundenen technischen Details vor dem Nutzer verbergen. In der Regel wird dem Nutzer sogar verborgen bleiben, ob eine Anwendung Daten in XML-Dateien oder in andersartig strukturierten Dateien verarbeitet.

Als kritischer Vorzug erweist sich XML als Dateiformat dann, wenn eine Datei mit der dafür vorgesehenen Anwendung nicht bearbeitet werden kann. Die Gründe dafür können unterschiedlich sein. Beispielsweise könnte die Datei beschädigt worden sein, und die Anwendung könnte sich darauf hin weigern, die Datei zu öffnen. Oder der Dateizugriff wird notwendig, nach dem die Anwendung bereits lange außer Dienst gestellt wurde. In solchen Situationen bieten XML-Dateien die prinzipielle Möglichkeit, Dateiinhalte unmittelbar zu bearbeiten, notfalls mit einem simplen Text-Editor. Ebenso können beschädigte oder verloren gegangene Schemata anhand valider Dokumente prinzipiell rekonstruiert werden. So kann die 'Menschen-Lesbarkeit' von XML-Dateien einen im Einzelfall entscheidenden Beitrag zur Rettbarkeit von Daten und damit letztlich zur **Robustheit** von Anwendungssystemen leisten.

Allerdings führen Reparaturversuche an XML-Dateien nicht zwangsläufig zum Erfolg. Das oben vorgestellte Telefonbuch-Beispiel zeigt zwar, dass der Inhalt einer XML-Datei so selbsterklärend sein kann, dass man ihn mitunter auf Anhieb verstehen und sogar das Schema (wenn auch möglicherweise nicht vollständig) aus einem gegebenen Dokument ableiten kann. XML wird deshalb häufig als **selbstdokumentierend** bezeichnet. In der Praxis verwendete XML-Dateien sind jedoch in mehrerlei Hinsicht komplexer. Nicht nur sind die Schemata und die Dokumente selbst umfangreicher, sondern auch die Beschränkung von XML auf hierarchische Strukturen führt oft zu Komplikationen. Viele XML-Dokumente müssen Strukturen ausdrücken, von denen sich nur Teile auf den hierarchischen Strukturbaum eines XML-Dokumentes abbilden lassen. Andere Teile müssen hingegen mit prinzipiell beliebigen Mitteln im Inhalt des Dokumentes niedergelegt werden und sind dort weitaus schwieriger zu verfolgen.

Auch hat die Lesbarkeit von XML-Dateien durchaus ihren Preis. Die oben angesprochenen Binärformate erlauben mitunter das unmittelbare Hin- und Herkopieren der Daten zwischen Datei und Arbeitsspeicher[1]. Soll eine Anwendung ihre Daten in XML-Dateien ablegen, so müssen sie sie in der Regel aus einem internen Format in ein XML-Dokument übersetzen und aus diesem Dokument einen Zeichenstrom formen. Ein entsprechender Aufwand ist für das Lesen der Daten erforderlich. In der Mehrzahl der praktischen Anwendungsfälle ist dieser zusätzliche **Laufzeitaufwand** jedoch tolerierbar.

Schwerer als alle technischen Merkmale und Implikationen von XML wiegt inzwischen ein anderer Vorteil: XML ist ein **offener Standard mit einer beispiellos breiten Akzeptanz** im Markt. Entscheidungen über die externe Repräsentation von Anwendungsdaten fallen daher beinahe automatisch zugunsten von XML aus. Dies gilt nicht nur, wenn die Daten einfach nur in Dateien gesichert werden sollen, sondern erst recht auch dann, wenn die Daten vermittels dieser Dateien oder auch unmittelbar mit anderen Anwendungen ausgetauscht werden sollen. Wann immer **Interoperabilität** zwischen Anwendungen auf der Basis offener Standards hergestellt werden soll, führt an XML kaum ein Weg vorbei.

Mit der großen Akzeptanz verbunden ist eine außerordentlich breite Palette an verfügbaren Werkzeugen, von selbständigen Anwendungen wie XML-Editoren bis hin zu Schnittstellen, Bibliotheken und Frameworks für die Anwendungsentwicklung. Sie stellen Parser und XSL-Tranformatoren bereit, aber auch Werkzeuge für die wechselseitige Abbildung zwischen XML-Dokumenten und anwendungsinternen Datenrepräsentationen. Obendrein sind viele dieser Werkzeuge in dem einen oder anderen Sinne frei verfügbar. Für die individuelle Anwendungsentwicklung und -Integration bieten einsatzfertige Schnittstellen und Werkzeuge die Vorteile einer reduzierten Fertigungstiefe, einer stärkeren Konzentration auf das fachlich Wesentliche und damit eine merkliche Reduktion von Risiken und Kosten. Insofern bietet sich XML als strategische Technologieplattform an, um die in Kapitel 3.9 angesprochene Schwerpunktverlagerung von Desktop-Standardwerkzeugen hin zu individuell integrierten Prozesslösungen zu realisieren.

XML und einige nah verwandte Spezifikationen sind "Empfehlungen" (Recommendations) des World Wide Web Consortium (W3C)[2], in dem in erster Linie Hersteller und Universitäten vertreten sind. Zahlreiche andere technisch ("horizontal") orientierte XML-basierte Spezifikationen befinden sich jedoch in der Obhut ähnlicher Organisationen, wie etwa OASIS[3] oder der Web Services Interope-

---

1 Diesen Performance-Vorteil stehen unter Umständen Sicherheitsrisiken gegenüber. Die im Arbeitsspeicher gehaltenen Datenstrukturen können Rückschlüsse auf vorausgegangene Bearbeitungsschritte zulassen. Diese Informationen können ebenfalls in eine Datei gelangen, ohne dass dies dem Anwender bewusst ist. Siehe auch Maßnahme M 2.223 im IT-Grundschutzhandbuch des BSI (http://www.bsi.de/gshb).

2 http://www.w3.org

3 http://www.oasis-open.org

rability Organization (WS-I)[1]. Da, wie oben dargestellt, XML erst durch die Definition von XML-Anwendungen zu einer echten Auszeichnungssprache wird, gibt es auch eine Vielzahl von Initiativen, um fachlich ("vertikal") orientierte XML-Anwendungen zu definieren[2].

Die Vielzahl der Konsortien und die Vielfalt der Kräfte, die die Entwicklung und Anwendung von XML vorantreiben, sind bemerkenswert, ebenso wie die Modularisierung der zentralen XML-Standards. Zwar ist dieses Entwicklungsmodell recht unübersichtlich und produziert auch durchaus unübersichtliche Ergebnisse. Dennoch hat es binnen weniger Jahre eine Standard-Plattform geschaffen und eine Wirkung entfaltet, die auf der Basis eines konventionellen, Hersteller-zentrierten Prozesses kaum vorstellbar ist. Ambitionierte Projekte wie OASIS ebXML[3], eine Umgebung für unternehmensübergreifende Internet-basierte Geschäftstransaktionen, wären ohne ein kollaboratives Entwicklungsmodell vermutlich aussichtslos.

Insofern kann auch das Entwicklungsmodell, aus dem XML entstanden ist, als Vorzug von XML verstanden werden. Es sorgt für Interoperabilität, fördert die Akzeptanz, gewährt Offenheit und Gestaltbarkeit, und bietet somit ein hohes Maß an Investitionssicherheit.

Dennoch ist nicht automatisch alles rundherum offen und interoperabel, was ein XML im Namen trägt. Die Vielfalt der XML-Technologien erlaubt es beispielsweise (und zwingt in einigen Umbruch-Situationen dazu), bestimmte XML-Technologien zu verwenden, andere hingegen nicht. Microsoft InfoPath (siehe Kapitel 3.9.3.2) ist ein Beispiel dafür, wie eine Anwendung zwar verschiedenste XML-Standards einsetzt, in der Realisierung einer entscheidenden Funktionalität aber eigene Wege geht.

3.9 Backend-Integration

3.9.1 Überblick

In den meisten Organisationen fällt die überwiegende Menge aller Daten an den Schreibtischen der Mitarbeiter an und wird mit den dort verfügbaren Werkzeugen verarbeitet und gespeichert. Soweit keine Fachanwendungen zum Einsatz kommen, sind dies in der Regel Office-Suiten. Statistisch oder operativ wertvolle Informationen versinken in Office-Dokumenten, aus denen sie nur schwer zu bergen sind. XML verringert die technischen Probleme dieser Bergung und kann zur Verringerung ihrer semantischen Probleme beitragen. Der Einsatz von XML-basierten Dateiformaten ist ein Migrationsthema, das in diesem Leitfaden angesprochen wird (siehe Kapitel 3.13).

---

1 http://www.ws-i.org

2 Für die öffentliche Verwaltung bietet der XML-Infopoint der KBSt (http://kbst.bund.de/E-Government/-,231/XML-Technologie.htm) eine Übersicht.

3 http://www.ebxml.org

XML-basierte Dateiformate erleichtern aber nur die Problembehebung, sie schaffen das Problem nicht aus der Welt. Daten, die in zentralen DV-Systeme benötigt werden oder dort sinnvoll erschlossen werden könnten, sollten gar nicht erst in Office-Dokumenten vergraben sondern von vornherein zentral verwaltet werden. Auf den Desktop gehören lediglich Werkzeuge für die Erfassung und den Abruf dieser Daten. Auf eine kurze Formel gebracht heißt das: Ablösung von informellen Desktop-Ritualen durch zentrale Anwendungen.

Anwendungsentwicklung ist keine typische Migrationsaufgabe, da Migrationsentscheidungen auf den Einsatz von Standardlösungen abzielen, Anwendungsentwicklungen aber individuelle und damit wesentlich aufwändigere Maßnahmen sind. XML-Technologien erleichtern jedoch auch die Anwendungsentwicklung, nicht zuletzt aufgrund der Vielfalt verfügbarer Werkzeuge und Lösungskomponenten. Die Entwicklung individueller Anwendungen wird dadurch attraktiver. Zugleich ist die neue Generation der Office-Suiten für die Integration mit XML-orientierten Backend-Anwendungen besser vorbereitet als jede vor ihr. Office-Anwendungen sind keine Alternative zu individuellen Lösungen, sondern sie werden zu deren Bestandteil. Grund genug, Migrationsentscheidungen insbesondere im Office-Bereich auch im Lichte neuer Technologien für prozessorientierte Individualentwicklungen zu bewerten. Namentlich sind dies auf der Client-Seite beispielsweise XForms nebst darauf basierenden oder vergleichbaren Produkten, sowie auf der Backend-Seite Web-Service und die zu ihrer Implementation verwendbaren Plattformen .NET und J2EE.

3.9.2 Einführung

Über die Gesamtheit der Organisationen hinweg, die Migrationsstrategien entwickeln, sind Office-Suiten sicherlich das am häufigsten eingesetzte Desktop-Werkzeug. Wie im Kapitel 3.13 dargestellt, hält XML seinen Einzug nun auch in diese Domäne, da nach OpenOffice.org/Sun StarOffice (OOo/SO) mit Office 2003 nun auch Microsoft damit beginnt, XML-Dateiformate zu unterstützen. Beide Office-Suiten lassen es dabei aber nicht bewenden, sondern bieten Funktionalitäten an, die eine stärkere Verzahnung dieser Desktop-Werkzeuge mit zentralen Datenverarbeitungssystemen ("Backoffice") erlauben. Desktop-Anwendungen dienen im Rahmen einer solchen Integration weniger als Autorenumgebung für frei gestaltete Dokumente, sondern als Dateneingabewerkzeug für zentrale DV-Prozesse.

Microsoft unterstreicht die wachsende Bedeutung dieser Funktionalität mit der Aufnahme von InfoPath als selbständigem Produkt in einige Editionen der Office-Palette. OOo/SO realisiert in der kommenden Version 2 bzw. 8 auch diese Funktionalität als Teil des Integrierten Gesamtpaketes.

Eine der Empfehlungen des Migrationsleitfadens lautet zwar, Geschäftsprozesse nicht in Office-Makros auf dem Desktop zu kodieren, sondern sie an zentraler Stelle mit Werkzeugen zu realisieren, die dieser Aufgabe angemessen sind. Genau dafür eröffnen die neuen Generationen der Office-Werkzeuge neue Möglichkeiten. Allerdings sprengt die Entwicklung und Integration solcher Backoffice-

Prozesse ganz offensichtlich den Rahmen einer Migration im engeren Sinne, und kann daher im Migrationsleitfaden nicht abgehandelt werden.

Mit den neuen Komponenten und Leistungsmerkmalen einer Office-Suite entscheidet aber auch ihre Auswahl mit über die weiterführenden Gestaltungsmöglichkeiten. Dieses Kapitel wirft daher ein kurzes Schlaglicht auf die neuen Möglichkeiten auf dem Desktop und auf einige Technologien, mit denen die korrespondierenden Backend-Lösungen realisiert werden können.

Automatisch ins Blickfeld geraten dabei Fragen der Anwendungsarchitektur. Im Rahmen dieses Kapitels werden diese Fragen gerade so weit vertieft, wie es zur Verdeutlichung der technologischen Perspektiven sinnvoll scheint. Der größere Zusammenhang, in dem diese Fragen im Einzelfall zugespitzt werden müssen, kann ihm Rahmen dieses Kapitels nicht aufgezeigt werden. Weiterführende Informationen bietet stattdessen beispielsweise das E-Government-Handbuch[1].

3.9.3 Dokumente, Daten und XML

Die Notwendigkeit eines intensiveren Ineinandergreifens von Desktop- und Backoffice-IT ergibt sich in erster Linie in Organisationen, die prozessorientiert arbeiten, und deren Erfolg sich etwa an der Zuverlässigkeit, Geschwindigkeit oder Effizienz orientiert, mit der sie diese Prozesse durchführen. Dieser Abschnitt skizziert die Motivation solcher Organisationen für den Einsatz von XML-Technologien, wie sie in diesem Kapitel vorgestellt werden. Zu diesem Zweck ordnet er zwei häufig synonym gebrauchte Begriffe neu ein, nämlich "Daten" und "Dokumente".

Prozesse können unmittelbar den Daseinszweck der Organisation unterstützen, z.B. den Handel mit Waren oder die Durchführung von Antragsverfahren. Stattdessen oder zugleich können sie aber auch der Steuerung der Organisation dienen, indem sie beispielsweise Informationen über die zuvor genannten Prozesse agreggieren und statistisch aufbereiten.

Prozesse können als variable, letztlich aber vordefinierte Abfolge von einzelnen Schritten beschrieben werden. Jeder Schritt kann Ergebnisse vorausgegangener Schritte verwenden, Informationen aus der Umgebung des Prozesses hinzu ziehen, Ergebnisse für folgende Schritte oder für die Verwendung außerhalb des Prozesses bereit stellen und Entscheidungen über den weiteren Prozessverlauf treffen. Ein Prozess existiert einerseits als abstrakte Prozessdefinition, und wird andererseits auf konkrete Prozessfälle angewendet.

In der öffentlichen Verwaltung kann ein solcher Prozess beispielsweise ein mehrstufiges Antragsverfahren sein. Der Verlauf eines Falles kann durch einzelne Daten beschrieben werden. Diese Daten sind zunächst auf dieser Betrachtungsebene ein informelles Konzept; es liegt im Zusammenhang dieses Kapitels aber nahe, gleich an Datenstrukturen in einem technischen DV-System zu denken.

[1] http://www.bsi.bund.de/fachthem/egov/3.htm

Inhaltlich kann es sich bei diesen Daten um Merkmale des Falles handeln, wie z.B. das Aktenzeichen oder (nach dessen Abschluss) das Ergebnis des Verfahrens. Es kann sich aber auch um Merkmale des einzelnen Schrittes handeln, beispielsweise Ausführungszeitpunkt und Identität des Bearbeiters.

Ist in der Prozessdefinition ein Bescheid oder eine Rückfrage beim Antragsteller vorgesehen, dann erhält dieser möglicherweise ein Dokument mit entsprechendem Inhalt. Technisch ist dabei an ein Schreiben oder an eine E-Mail zu denken. Inhaltlich bündelt das Dokument Fall-Daten wie das Aktenzeichen mit Schritt-Daten wie dem Kalenderdatum des Verfahrensschrittes, der das Dokument erzeugt hat. Hinzu kommen möglicherweise Daten von außerhalb des Prozessfalles, wie beispielsweise die Telefonnummer und die Sprechzeiten des Bearbeiters sowie eine Rechtsbehelfsbelehrung. In Reaktion darauf verfasst der Antragsteller möglicherweise seinerseits ein Dokument, in dem er die besonderen Umstände darlegt, die im Verfahren berücksichtigt werden sollten. In einem folgenden Schritt wird diese Darlegung ein Datum des Verfahrensfalles (oder Schrittes).

Die beiden Dokumente in diesem Beispiel haben unterschiedliche Funktionen. Das erste Dokument dient dazu, dem Antragsteller den Stand des Verfahrens mitzuteilen und ihm möglicherweise die Mitgestaltung folgender Schritte zu ermöglichen. Ausgehend von diesem Zweck stellt es eine Art Schnappschuss von Daten aus unterschiedlichen, voneinander möglicherweise unabhängigen Quellen zusammen. Es enthält also keinerlei Daten, die nicht bereits zuvor existierten. Das zweite Dokument enthält im Gegensatz dazu mit der Darlegung des Antragstellers etwas gänzlich Neues, und seine Aufgabe ist es, dieses Datum in den Prozessfall einzuführen.

Abstrahierend von diesem Beispiel können Dokumente als Ein- und Ausgabekanäle von Prozessfällen bezeichnet werden, die zur Einbindung solcher Prozessteilnehmer in den Prozessfall dienen, die sich außerhalb der (organisatorischen bzw. technischen) Strukturen befinden, in denen der Prozess ausgeführt wird.

Ein Dokument hat im Prozesskontext nur eine Daten-Transportfunktion, und diese auch nur zu einem bestimmten Zeitpunkt. Ein dauerhafter, autoritativer Ablageort für Daten sind Dokumente in diesem Sinne jedoch nicht. Jedes Dokument muss daher gewissermaßen be- und entladen werden, um seine Funktion im Prozesskontext zu erfüllen. Somit verursacht jedes Dokument Aufwände. Aus Effizienzgründen sollte der Einsatz von Dokumenten in Prozessen daher so weit wie möglich vermieden werden. Wo er unvermeidlich ist, sollte der Be- und Entladevorgang so weit als möglich automatisiert werden.

Vermeiden lässt sich der Einsatz von Dokumenten durch eine unmittelbare, synchrone Integration der Prozessbeteiligten, beispielsweise durch die Bereitstellung des Prozesses als Online-Anwendung.

Automatisieren lässt sich der Be- und Entladevorgang auf verschiedene Weise. Wünschenswert mit Blick auf die Entladung sind Verfahren, die eine einfache und zweifelsfreie Identifikation der Daten in Dokument ermöglichen, die Spielräume

der Interpretation der Daten möglichst einschränken und die (formale oder sogar inhaltliche) Validität der Daten gewährleisten.

Nicht jede technisch machbare Lösung erfüllt diese Wunschliste. Kann der Antragsteller im oben beschriebenen Verfahren seine Stellungnahme als E-Mail schicken, dann könnte eine robust gestaltete E-Government-Anwendung einigen Aufwand treiben, um beispielsweise das Aktenzeichen aus der E-Mail zu gewinnen. Sicherlich ist der Antragsteller gehalten, das Aktenzeichen in einer bestimmten Weise in den Betreff der Mail zu schreiben. Was aber, wenn er sich nicht daran hält? Um die Mail trotzdem verarbeiten zu können, könnte die Anwendung Betreff und Text der Mail nach bestimmten Mustern durchsuchen, und die so gefundenen potentiellen Aktenzeichen anhand der in Frage kommenden Prozessfälle validieren. Dazu muss die Anwendung in der Lage sein, mehrteilige Mails in ihrer Bestandteile zu zerlegen und ggf. zu dekodieren. Im Ergebnis ist dieses Verfahren nicht einfach. Auch ist die Validität der Daten nicht einmal formal gewährleistet, Identifikation und Interpretation der Daten brauchen dementsprechend eine Portion Glück.

Im Vergleich werden die Vorzüge deutlich, die die in Kapitel 3.8 vorgestellten zentralen XML-Technologien bieten. XML-Schemata definieren ein gewisses Maß an zumindest formaler Datenkonsistenz, Namespaces erlauben die Einbettung von Dokumenten des einen Typs in Dokumente des anderen Typs, und XPath bietet weit reichende Möglichkeiten für die Identifikation bestimmter Daten inmitten eines ansonsten völlig unbekannten Dokumentes. Und das alles mit Standard-Werkzeugen. Bemerkenswert ist jedoch, dass XML-Dokumente zwar Dokumente heißen und die beschriebenen Gestaltungsfreiheiten bieten, tatsächlich aber stets wohlstrukturierte Daten sind. Insofern sind XML-Dokumente gemessen an der oben beschriebenen Verwendung von "Dokumenten" und "Daten" ein grandioser Hybrid.

Web Services (siehe Kapitel 3.9.4) nehmen XML-Dokumente entgegen, denen sie u.a. die Parameter einer auszuführenden Funktion entnehmen. Das Ergebnis dieser Funktion kleiden sie ihrerseits wieder in ein XML-Dokument und senden es zurück.

Aber wie kann das Beladen bzw. Erzeugen eines XML-Dokumentes geschehen, wenn der bereits mehrfach angesprochene Antragsteller seine Stellungnahme formulieren will? XML-Editoren unterstützen den Benutzer in einer Weise, die die formale Korrektheit der XML-Dokumente im Sinne des assoziierten XML-Schemas mehr oder weniger erzwingt. Damit ist allerdings nicht gewährleistet, dass das Dokument inhaltlich in sich stimmig ist. Überdies kann dem Antragsteller der unmittelbare Umgang mit den rohen XML-Strukturen kaum zugemutet werden. Er benötigt daher ein Werkzeug zum Bearbeiten von XML-Dokumenten, das die Komplexitäten von XML vor ihm verbirgt und ihm eine freundlichere Sicht auf das Dokument bietet, die sich an seinem Verständnis des Dokumenteninhaltes orientiert. Dazu sollte das Werkzeug auch nicht nur XML-Schemata berück-

sichtigen, sondern auch die inhaltlichen Regeln und Gültigkeitsbedingungen des Dokumentes verstehen und durchsetzen können.

Der offene Standard XForms und das Produkt Microsoft InfoPath können beide eingesetzt werden, um ein solches Eingabewerkzeug anwendungsbezogen bereit zu stellen. Die folgenden zwei Abschnitte beschreiben beide näher. Ein weiterer Abschnitt im Anschluss daran stellt XForms und InfoPath einander kurz gegenüber.

3.9.3.1 XForms

Der Siegeszug des World Wide Web ist in vielerlei Hinsicht eine Erfolgsgeschichte, aber sie ist auch eine Geschichte vom Preis des unverhofften Erfolges. Die Technologien des Web sollten ursprünglich als Hypertext-System für statische wissenschaftliche Dokumente dienen. Seine heutige Bedeutung hat das Web jedoch als dynamische Interaktionsplattform, mit der von praktisch überall her Flugverbindungen ermittelt, Bücher bestellt und e-Government-Leistungen in Anspruch genommen werden können. Web-Technologien haben diese Anwendungen zum einen deshalb möglich gemacht, weil sie einfach, robust und plattformunabhängig sind. Zum anderen ist für die Nutzung einer inzwischen unüberschaubaren Vielfalt von Anwendungen nichts weiter nötig als ein einziger, immer gleicher und (ursprünglich) simpler Web-Browser. Das Potential der Web-Technologien als Client-Plattform für Anwendungen blieb deshalb auch nicht lange unentdeckt.

Ganz im Sinne ihrer ursprünglichen Aufgabe war allerdings die Unterstützung der Web-Technologien für die Interaktion mit dem Anwender von Anfang an ausgesprochen sparsam, und erstaunlicherweise hat sich daran in nun bald anderthalb Jahrzehnten prinzipiell nichts geändert. Eine Vielzahl von Technologien und Produkten verfolgen seither das Ziel, Web-Anwendungen reaktionsfreudiger, benutzerfreundlicher und beherrschbarer und damit die Kargheit der Web-Technologien als Interaktionsplattform erträglicher zu machen, ohne sie allerdings zu beheben.

Das Zentrum all dieser Anstrengungen sind die in HTML realisierten Formulare. XForms treten an, diese Formulare abzulösen. Deshalb dürften XForms in den kommenden Jahren einen erheblichen Einfluss auf die Entwicklung der Architekturen von Web-Anwendungen nehmen.

Die folgenden Abschnitte charakterisieren einige wesentliche Merkmale von XForms, um dieses Potential zu verdeutlichen.

Was ist besser an XForms?

XForms sind, wie ihr Name bereits andeutet, eine weitere XML-Technologie. Da sie HTML-Formulare ablösen sollen, übernehmen sie unter anderem deren Funktion, nehmen dabei aber weitaus größere Rücksicht auf die Bedürfnisse der Anwendungsentwicklung.

Natürlich sind XForms ganz und gar XML. Das gilt auch für die Daten, die der XForms-Client, der so genannte Prozessor, an den Server zurück sendet. HTML-Formulare liefern nur simple Schlüssel-Wert-Paare. Sollen komplexe Daten übertragen werden, müssen sie 'platt gedrückt' und auf der Server-Seite mühsam wieder auseinander gefaltet werden. Ein XForms-Prozessor schickt dagegen ein XML-Dokument. Selbstverständlich können XForms die Benutzereingaben nicht nur auf beliebig komplexe Strukturen von XML-Elementen abbilden, sondern auch auf deren Attribute.

Im Quelltext von HTML-Formularen hängen Formularstruktur, initiale Formulardaten, grafische Repräsentation in einem Web-Browser und Interaktionslogik sehr eng miteinander zusammen. Um ihre Kombination variieren zu können und ein Formular mal mit den einen, mal mit den anderen Daten zu befüllen, werden die Formulare meist dynamisch generiert und statische und dynamische Formular-Anteile dabei immer wieder neu miteinander verwoben. XForms dagegen trennen drei konzeptionell voneinander unabhängige Aspekte auch technisch voneinander: Struktur, Daten und Präsentation.

- Statische Struktur und Interaktionslogik von XForms sind einem Modell zusammengefasst.
- Teil des Modells ist die Definition der Daten, die vom XForm angezeigt bzw. entgegengenommen werden sollen, in Gestalt vom Instanzen. Instanzen können sich darauf beschränken, die Struktur der Daten zu definieren, nicht jedoch die Daten selbst. An deren Stelle kann ein Verweis auf eine externe Datenquelle (natürlich XML) treten. Diese Quelle anzuzapfen und die Instanz mit den Daten zu befüllen ist dann nicht mehr das individuelle Problem der Web-Applikation, sondern ein Service des XForms-Prozessors.
- Die XML-Elemente, die die Präsentation des XForms und damit die Controls beschreiben, mit denen der Anwender interagiert, enthalten selbst keine Daten und keine Logik. Vielmehr beziehen sie sich auf das Modell und die Instanzen. Darüber hinaus identifizieren sie lediglich die abstrakte Funktion eines Controls, wie etwa dass der Anwender aus einer Reihe von vorgegebenen Optionen genau eine auswählen kann. Ob sich diese Funktion dem Benutzer als weitläufige Serie von Radio Buttons darbietet oder aber als kompakte Drop-Down-Liste, ist nicht im XForm definiert, sondern liegt in der Entscheidungsfreiheit des Prozessors. So können unterschiedliche Prozessoren ein und dasselbe XForm für unterschiedliche Umgebungen aufbereiten – nicht nur für Web-Browser, sondern beispielsweise auch für mobile Endgeräte.

XForms orientiert sich mit dieser Aufteilung vage am MVC-Programmiermodell (Model-View-Controller), das in der GUI-Programmierung getrost als Selbstverständlichkeit bezeichnet werden kann. Ein anderer Aspekt des Zuschnitts von XForms ist weitaus überraschender: während HTML-Formulare ein Bestandteil von HTML sind, sind XForms eine selbständige XML-Anwendung. Allerdings de-

finiert XForms keinen selbständigen Dokumenttyp. Vielmehr werden XForms Dokumente eines anderen Typs eingebettet. Als sinnvolle Wirtsdokumenttypen gelten gemeinhin XHTML 2 und SVG (Scalable Vector Graphics). OpenOffice.org 2 bzw. StarOffice 8 (siehe 3.13.5) bettet XForms in das OpenDocument-Format ein. Da XForms prinzipiell unverändert in beliebige unterschiedliche Wirtsdokumente einbettbar sind, können sie einen Beitrag zur Entkopplung von Anwendungslogik (niedergelegt im XForm) und Benutzeroberfläche (repräsentiert durch das Wirtsdokument) leisten.

Was ist neu an XForms?

XForms erfüllen nicht nur die Aufgaben von HTML-Formularen auf elegantere und flexiblere Weise. Sie bieten auch Leistungen, die über HTML-Formulare deutlich hinausgehen.

HTML-Formulare im engeren Sinne reichen selten aus, um die Interaktion des Anwenders mit der Web-Anwendung zu gestalten. Häufig sind dynamische Reaktionen auf Benutzereingaben notwendig. In aller Regel müssen die gänzlich untypisierten Benutzereingaben auf Typkonformität geprüft werden, also beispielsweise darauf hin, ob die Eingabe im Datumsfeld auch als Datum interpretiert werden kann. Oft müssen die Eingaben aber auch miteinander in Beziehung gesetzt werden, um eine inhaltliche Konsistenzprüfung zu realisieren oder um Controls ein- oder ausgeschaltet oder mit berechneten Werten zu befüllen. Um diese Funktionalitäten bereit zu stellen, werden HTML-Formulare häufig mit Scripten ergänzt, die vom Web-Browser ausgeführt werden. Wo das nicht ausreicht, müssen die Formulardaten an den Server gesendet und das Formular neu generiert werden. Allerdings ist Scripting die Achillesferse vieler Web-Anwendungen und unter Sicherheitsaspekten nicht unbedenklich. Darüber hinaus behindert der Neuaufbau des Formulars den Interaktionsfluss.

XForms machen einige der zusätzlich benötigten, meist durch Client-Scripts realisierten Funktionalitäten zu einem Bestandteil des Formular-Mechanismus als solchem:

- Daten in XForms sind typisiert. Zur Definition dienen XML-Schemata, sowohl existierende wie auch im XForm selbst formulierte Fragmente. Typen werden selbstverständlich den Instanz-Elementen zugewiesen (und nicht den Controls).
- An Controls sichtbare Merkmale, wie aktiv oder inaktiv zu sein, nicht leer bleiben zu dürfen oder nicht editierbar zu sein, werden ebenfalls der Instanz zugewiesen und können durch Ausdrücke definiert werden.
- Aufbauend auf anderen XML-Standards definiert XForms ein Prozessmodell und eine Vielzahl von Events. Sie können verwendet werden, um eine Reihe von vordefinierten Aktionen auszulösen. Diese Aktionen bilden teilweise häufig verwendete Scripting-Funktionalitäten nach, wie beispielsweise die Anzeige von Warnungen, die Manipulation von Datenstrukturen bzw. Controls (im Falle von XForms also der Instanzdaten) oder die Kon-

trolle des Eingabefokus. Andere Aktionen ermöglichen Eingriffe in das Event-Management. Abfolgen von vordefinierten Aktionen können zu neuen Aktionen verknüpft werden.

Meist Server-seitig realisierte Funktionalitäten wie den datenabhängigen Neuaufbau von Tabellen und Formularen, etwa zur Realisierung von Wizards, können mit XForms Client-seitig realisiert werden.

Wie viele XML-Anwendungen ziehen XForms die Deklaration ("Was ist das Ziel?") ganz klar der Prozedur ("Wann und wie wird es erreicht?") vor; zur deklarativen Verknüpfung der verschiedenen XForms-Bestandteile dient XPath, ergänzt um eine Reihe von XForms-spezifischen Funktionen. Das XForms-Programmiermodell ähnelt insofern dem typischen Umgang mit einer Tabellenkalkulation: der Anwender gibt in einer bestimmten Syntax statische Formeln in Felder ein; um den Zeitpunkt und die Durchführung der notwendigen Berechnungen muss er sich jedoch nicht kümmern, sondern kann dies getrost seinem Werkzeug überlassen. (Ähnlich den Makro-Mechanismen in großen Tabellenkalkulationen bieten allerdings auch XForms einige traditionelle imperativ-prozedurale Gestaltungsmöglichkeiten.)

Zukünftige Rolle von XForms

XForms können prinzipiell helfen, die Architektur von Web-Anwendungen drastisch zu vereinfachen. Bis zu einem gewissen Grade sollen sie Client-seitiges Scripting überflüssig machen und damit eine notorische Fehlerquelle und Cross-Browser-Stolperfalle zumindest eindämmen. Zugleich sollen sie die Interaktionsfreudigkeit von Web-Anwendungen beibehalten, in dem sie Skript-Funktionalitäten mit Standard-Mechanismen realisieren oder sie sogar erhöhen, indem sie zusätzliche Gestaltungsmöglichkeiten bieten und Server-Requests vermeiden helfen. Und bereits in der Version 1 haben XForms das Zeug dazu.

Zwei Hindernisse dürften es im Wesentlichen sein, die sich dem Erfolg von XForms in den Weg stellen könnten. Das erste ist das weitgehend deklarative Programmiermodell. Im Vergleich zur gewöhnlichen imperativen Skript-Programmierung verlangt es von Web-Entwicklern deutlich mehr Geschicklichkeit im Umgang mit relativ abstrakten Modellen. Zugleich bietet es zur Formulierung dieser Modelle teilweise radikal andere Begrifflichkeiten an.

Das zweite, weitaus ernstere mögliche Hindernis ist die Durchsetzbarkeit von XForms als Standard. Vordergründig hängt sie von der direkten Unterstützung durch marktübliche Browser ab. Um sie einschätzen zu können, muss das sehr junge Alter der Technologie in Betracht gezogen werden. Die XForms-Empfehlung des W3C in der Version 1.0 wurde am 14. Oktober 2003 veröffentlicht (also praktisch zeitgleich mit SAGA 2.0); zu diesem Zeitpunkt war ein gutes Dutzend (partieller) Implementationen bekannt[1], darunter portable Lösungen auf

[1] http://www.xml.com/pub/a/2003/09/10/xforms.html

der Basis von Java und des im Web bereits weit verbreiteten Flash 6 (DENG[1]). Am 11. August 2004 kündigte die Mozilla Foundation zusammen mit IBM und Novell eine Standard-Implementation an. Der Erfolg dieser Bemühungen bleibt aus heutiger Sicht abzuwarten, sowohl mit Blick auf die technische Funktionstüchtigkeit, die Akzeptanz bei Entwicklern und Anwendern und die Einstufung durch SAGA. Zuvor wartet allerdings das als primäre Wirtssprache vorgesehene XHTML 2 noch auf seine Verabschiedung. OpenOffice.org 2 bzw. StarOffice 8 (siehe Kapitel 3.13.5) bietet unterdessen Formulare zur Bearbeitung von XML-Dokumenten als neuen Dokumententyp an, wie erwähnt eingebettet in OpenDocument.

Allerdings könnten XForms auch einen gänzlich anderen Weg zum Erfolg einschlagen, nämlich als Modell-Technologie. Wie erwähnt können XForms in prinzipiell beliebige Wirtsdokumente eingebettet werden. Das können nicht nur die Seiten von Web-Anwendungen sein, die unmittelbar (oder mittelbar durch Plugins) im Browser interpretiert werden. XForms sind auch bereits dann ein großer Schritt nach vorn, wenn sie lediglich zur abstrakten, plattformunabhängigen Formulierung von Benutzerschnittstellen eingesetzt werden und ihre Umsetzung serverseitig erfolgt, beispielsweise in HTML (ggf. mit generierten Client-Scripts) oder WML. Auf diese Weise sind XForms auch mit den bereits vorhandenen Browsern einsetzbar. Ein prominentes XForms-Projekt fokussiert sich sogar ausdrücklich auf dieses Einsatzspektrum[2].

3.9.3.2 InfoPath

Wie die Spezifikation XForms dient auch das Produkt Microsoft InfoPath dazu, dem Benutzer eine Formular-orientierte Sicht auf XML-Dokumente zu bieten. InfoPath bietet insofern die gleichen Vorzüge, die bereits im Zusammenhang mit XForms beschrieben wurden. Während aber XForms-im engeren Sinne nur definiert, wie ein Formular beschrieben und wie diese Beschreibung interpretiert wird, ist InfoPath eine einsatzfähige, in sich geschlossene Lösung mit Entwicklungs- und Laufzeitumgebung in einem einzigen Programm.

Formularbeschreibungen verwaltet InfoPath als so genannte Form Templates. Sie bestehen aus einer ganzen Reihe von Dateien, die zu einem CAB-Archiv (*.xsn) zusammengefasst werden können. Form Templates enthalten so genannte Views. Dabei handelt es sich um XSL-Stylesheets, die die Struktur und das Aussehen des Formulars beschreiben. Ein Form Template kann mehrere Views enthalten, die das Dokument auf unterschiedliche Weise darstellen, beispielsweise um einzelne Teile eines umfangreichen Dokumentes zur Bearbeitung anzubieten, oder um unterschiedlichen inhaltlichen Blickwinkeln Rechnung zu tragen. Der Anwender kann zwischen den Views umschalten. Für die Gestaltung der Views steht ein visuelles Werkzeug zur Verfügung.

---

1 http://sourceforge.net/projects/dengmx

2 http://chiba.sourceforge.net

Wie XForms validiert InfoPath die Eingaben des Anwenders anhand des maßgeblichen XML-Schemas und erlaubt ergänzend die Formulierung von statischen Gültigkeitsbedingungen in XPath-Ausdrücken. Darüber hinaus bietet InfoPath eine bereits eingebaute Infrastruktur für dynamische Prüfungen: InfoPath interpretiert VBScript- und JScript-Fragmente sowie .NET-Komponenten und stellt ein Event-Management-System zur Verfügung, mit dessen Hilfe sie zur Ausführung gebracht werden können.

InfoPath soll zwar als Eingabewerkzeug konsequent über die Korrektheit und Plausibilität der eingegebenen Daten wachen, zugleich dem Benutzer aber den Komfort moderner Textverarbeitungen bieten. Dieser Anspruch wird nicht nur durch die vertraute automatische Korrekturfunktion eingelöst, sondern auch durch ein Rich Text-Control, mit dem eingebettete XHTML-Dokumente üppig formatiert oder mit Hyperlinks versehen werden können. Bei Bedarf können die Oberflächen-Elemente durch zusätzliche, maßgeschneiderte ActiveX-Controls ergänzt werden. Ferner wird der Anwender durch eine so genannte Task Pane mit kontextsensitiven Hinweisen bei der Arbeit unterstützt.

Die Laufzeitumgebung von InfoPath ist in der Lage, Formulardaten direkt aus Web Services zu beziehen und in Web Services zurück zu schreiben. Die Entwicklungsumgebung bietet eine interaktive Unterstützung für die Verdrahtung eines Form Templates mit Web Services. Ferner können Dokumente signiert werden.

InfoPath ist mit weiteren Microsoft-Produkten integriert. So können Benutzergruppen, die im Active Directory definiert sind, zur Selektion von Views verwendet werden. Zur Distribution von Form Templates auf die Clients kann SharePoint eingesetzt werden, und der Internet Explorer startet InfoPath, wenn er auf die entsprechenden Dokumente stößt.

3.9.3.3 XForms und InfoPath – zwei ungleiche Brüder

Ein direkter Vergleich von XForms und InfoPath ist selbstverständlich schon deshalb nicht möglich, weil XForms für sich genommen 'nur' die Spezifikation eines offenen Standards eines Konsortiums ist, InfoPath dagegen das konkret einsetzbare Produkt eines einzelnen Herstellers. Da jedoch beide offensichtlich im Kern die gleiche Funktionalität adressieren, können durchaus Gemeinsamkeiten und Unterschiede in der Herangehensweise identifiziert werden.

Tatsächlich beschreibt XForms als offener Standard einen Teilaspekt dessen, was InfoPath leistet. InfoPath macht intensiven Gebrauch von offenen Standards[1], wählt jedoch für den Aspekt, den XForms beschreibt, eine eigene Lösung[2].

---

1 http://msdn.microsoft.com/library/en-us/odc_ip2003_ta/html/odc_inXMLs.asp

2 Da diejenigen Funktionalitäten in InfoPath, die den durch XForms definierten entsprechen, nicht für den Gebrauch außerhalb von InfoPath bestimmt sind, werden sie im Rahmen des Leitfadens als Implementationsdetail verstanden und nicht näher untersucht.

Beide Technologien bieten die Möglichkeit, anwendungsspezifische XML-Editoren zu gestalten, die dem Benutzer nicht nur mehrere alternative formularhafte Sichten auf seine Daten bieten, sondern ihn auch mit Eingabehilfen und -validierungen unterstützt. Beide greifen dabei auf XML-Schemata und auf Ausdrücke zurück, die in XPath formuliert werden. InfoPath erlaubt, auch Skripte (VBScript oder JScript) bei der Eingabevalidierung zu berücksichtigen. Das Actions- und Event-Modell von XForms hingegen ist so gestaltet, dass es der Wirtssprache die Integration mit beliebigen Skriptsprachen ermöglicht, selbst aber keinerlei Scripting-Mechanismen anbietet. Generell wählt InfoPath häufiger prozedurale Verfahren, während XForms eher zur reinen XML-Lehre der deklarativen Ansätze neigt. InfoPath verwendet XSL zur Gestaltung der Datensichten und benutzt vorzugsweise Tabellen als Layout-Raster, XForms überlässt beide Gestaltungsaspekte abermals der Wirtssprache.

InfoPath umfasst eine vollständige Umgebung sowohl für die Gestaltung der Form Templates wie auch zugleich für deren Anwendung zur Datenbearbeitung, die auf Windows-Desktop-Systemen einsetzbar ist. XForms erlauben demgegenüber den Einsatz mit unterschiedlichen Wirtssprachen auf beliebigen Plattformen und Gerätetypen mit unterschiedlichen, jeweils geeigneten Präsentationsmechanismen – unter der Voraussetzung, dass eine entsprechende Implementation bereit steht. Diesem Vorbehalt steht der Vorzug gegenüber, dass XForms auch mit den heute gängigen Web Browsern eingesetzt werden können und daher kein Client-Deployment benötigen – die Unterstützung der verwendeten Features durch die Implementation immer vorausgesetzt.

Sowohl XForms als auch InfoPath sind noch sehr jung. Wie intensiv sie die Anwendungslandschaft prägen und welche Entwicklung sie selbst nehmen werden, bleibt abzuwarten. XForms definiert eine Lösung für ein präzise umgrenztes Teilproblem, so dass es immer mit anderen komplementären Technologien verbunden werden kann oder muss; damit stehen XForms in der Tradition von XML-Klassikern wie XPath. InfoPath dagegen ist bereits eine einsatzfertige Technologiemischung und führt insbesondere in einer von Microsoft-Produkten geprägten Umgebung schnell zum Erfolg.

Beide Technologien im Zusammenhang betrachtet, erlauben allerdings eine klare Prognose: Anwendungsspezifische XML-Dokument-Editoren werden als Benutzerschnittstellen-Technologie an Bedeutung gewinnen.

Damit ergänzen sich solche Editoren hervorragend mit der nach wie vor vielversprechendsten Schnittstellentechnologie für verteilte Anwendungen, die nämlich nichts anderes als XML-Dokumente verarbeitet: Web Services.

3.9.4 Web Services

Unter dem Begriff Web Services werden Verfahren zusammengefasst, mit denen ein Computer-Prozess Funktionen eines anderen Prozesses aufrufen und in den Besitz eines eventuellen Funktionsergebnisses gelangen kann. Die Prozesse können auf unterschiedlichen Computersystemen laufen. Traditionell wurden sol-

chen Mechanismen als Entfernte Prozedur- oder Funktionsaufrufe bezeichnet (Remote Procedure/Function Call, RPC/RFC) und meist mit proprietären, plattformspezfischen Mitteln realisiert. Das Besondere an Web Services ist demgegenüber, dass sie sich offener Web-Technologien und XML-Formate bedienen.

Es gibt keine einzelne, konkrete Web Service-Technologie. Vielmehr werden Web Services stets durch ein Bündel komplementärer Technologien realisiert. Eine bestimmte Zusammenstellung solcher Technologien wird als Interoperabilitätsprofil bezeichnet. Interoperabilitäsprofile werden von der Web Services Interoperability Organization (WS-I)[1] standardisiert.

Meist wird unter Web Services ein Bündel von vier Technologien verstanden. Sie beschreiben nicht nur einen offenen Standard für Web-/XML-basierte RPCs, sondern darüber hinaus auch Verfahren, mit denen sich Web Services selbst beschreiben können, und mit denen diese Beschreibungen in Katalogen publiziert werden können. Diese Technologien sind:

- HTTP als Transportprotokoll.
- SOAP (Simple Object Access Protocol) als RPC-Protokoll. SOAP definiert u.a. ein XML-Dokumentformat, mit dem die auszuführende Funktion identifiziert und die Ausführung parametrisiert wird, sowie ein Format, in dem das Funktionsergebnis zurückgegeben wird.
- WSDL (Web Services Description Language) ist ein XML-Format, mit dem alle technischen Merkmale eines Web Service beschrieben werden können. Diese Beschreibung kann verwendet werden, um die Entwicklung von Web Service-Clients zu automatisieren, oder sogar um zur Laufzeit dynamisch auf den bis dahin unbekannten Web Service zuzugreifen.
- UDDI (Universal Description, Discovery, and Integration) umfasst eine Reihe XML-Spezifkationen zur Realisierung von Registraturen, in denen beispielsweise WSDL-Dokumente abgelegt werden können. Solche Registraturen sind ihrerseits Web Services.

Ein Client kann beispielsweise einen ihm bereits bekannten UDDI-Service per HTTP und SOAP nach den WSDL-Beschreibungen bestimmter Web Services fragen. Aufgrund der so gewonnenen Informationen generiert der Client eine SOAP-Anfrage für den gefundenen, ihm bis dahin unbekannten Web Service und kontaktiert diesen in einem zweiten Schritt direkt. Eine alltägliche Entsprechung zu dieser Vorgehensweise ist der typische Gebrauch des Branchen-Telefonbuches: an einer bekannten Stelle können die Kontaktdaten eines bislang unbekannten Service-Anbieters nachgeschlagen werden. Für die eigentliche Kontaktaufnahme ist jedoch der Klient selbst verantwortlich, und das Nachschlagewerkzeug leistet dabei keinerlei Unterstützung (ein Gegenbeispiel ist die Telefon-Auskunft mit Weitervermittlung).

[1] http://www.ws-i.org/

Ein wichtiges Merkmal von (Web-) Services ist, dass sie zustandslos sind. Sie stehen bereit und warten auf Anfragen von Clients, beantworten diese und stehen anschließend wieder bereit. Das unterscheidet sie von Komponentenarchitekturen wie Enterprise Java Beans[1], bei denen Server-seitig meist dynamisch Objekte erzeugt werden, die einer bestimmten Client-Sitzung zugeordnet sind, und die den so genannten Konversationszustand (conversional state) dieser Sitzung widerspiegeln.

Die beiden beschriebenen Merkmale, die Verwendung eines nicht-vermittelnden Nachschlagemechanismus und die Zustandslosigkeit, sind typische Kennzeichen so genannter Service-orientierter Architekturen (SOA). Ihr Vorteil liegt in der Möglichkeit, Systeme relativ spontan und flexibel miteinander zu koppeln. Wird eine SOA auf der Basis offener, robuster Standards realisiert, wie dies bei Web Services der Fall ist, kommen als weitere Vorzüge die Plattformunabhängigkeit und die große Auswahl an verfügbaren Werkzeugen und Implementationen hinzu.

Web Services sind daher immer dann die Schnittstellentechnologie der Wahl, wenn der Client einer Schnittstelle zum Entwicklungszeitpunkt noch nicht bekannt ist oder wenn die Zahl der unterschiedlichen Clients absehbarerweise groß sein wird. Web Services sind jedoch nur eine Schnittstellentechnologie. Zur Realisierung der Funktionalität, die als Web Service nutzbar sein soll, müssen andere Technologien verwendet werden. Nahe liegend ist die Verwendung von .NET oder (SAGA-konform) J2EE; beide bieten heute eine schlüssig integrierte Web Services-Unterstützung.

Die Grenzen von Web Services liegen grundsätzlich im vergleichsweise hohen Aufwand, der für das unablässige Ein-, Aus- und Umpacken der Nutzdaten in mehrfach ineinander verschachtelter XML-Dokumente getrieben wird (siehe Kapitel 3.9.3). Sollen zwei Systeme exklusiv miteinander gekoppelt werden, also ohne dass weitere Systeme hinzutreten werden, und spielt die Performanz dieser Kopplung eine kritische Rolle, dann ist der Einsatz anderer, effizienterer Schnittstellentechnologien unter Umständen unumgänglich.

Eine weitere Grenze von Web Services liegt unglücklicherweise gerade in der Eigenschaft, die wesentlich zu ihrer Attraktivität beiträgt: sie sind vergleichsweise simpel. Zustandslose Dienste ohne besonderen Schutzbedarf sind mit Web Services schnell realisiert, wie beispielsweise ein öffentliches Nebenstellenverzeichnis. Sitzungsorientierte Dienste, mit denen authentisierte Benutzer transaktionssichere Manipulation an kritischen Daten vornehmen können, sind mit den heute etablierten Web Services-Profilen allein nicht zu machen. Die benötigten Technologien zur Lösung aller möglichen Einzelprobleme stehen zwar zur Verfügung oder befinden sich zumindest in der Entwicklung. Ob die jeweils notwendige Kombination von Technologien wirklich noch eine Vereinfachung bedeutet, muss im Einzelfall ernsthaft hinterfragt werden. Maßstab sind dabei die traditionellen Komponenten-Plattformen, die zwar komplex sind, die aber die benötigten

[1] Teil von J2EE (siehe Kapitel 3.9.6)

Schnittstellen-Leistungsmerkmale bereits als in sich stimmiges Paket bereitstellen.

3.9.5 „.NET“

Zu Beginn sollen einige im Zusammenhang mit „.NET“ immer wieder auftauchende zentrale Begriffe geklärt werden[1]:

- **.NET:**
  Die Microsoft Plattform für XML-Web Services, die Informationen, Geräte und Anwender in einer einheitlichen und personalisierten Weise miteinander verbindet.
- **.NET Framework:**
  Eine Umgebung für die Entwicklung, Bereitstellung und Ausführung von XML-Web Services und anderen Anwendungen. Es setzt sich aus zwei Hauptkomponenten zusammen:
  - Common Language Runtime
  - Klassenbibliotheken wie ASP.NET, ADO .NET und Windows Forms.
- **.NET-Plattform:**
  Besteht aus Tools, Geräten, XML-Web Services, Server und Anwendererfahrungen.

Im Folgenden wird in erster Linie das Microsoft .NET Framework als Middleware-Lösung näher betrachtet. Dieses ähnelt in gewisser Weise dem Ansatz der Java Virtual Machine (JVM), denn durch die Installation des Frameworks (z.B. auf Windows 2003) werden die Schnittstellen der integralen Bestandteile des Betriebssystems (z.B. Win32-API) abstrahiert und in neu geordneter Form angeboten. Dies hat in erster Linie Auswirkungen auf die Anwendungsentwicklung. Die folgende Abbildung zeigt einen Überblick der Komponenten des Frameworks.

[1] Entsprechende Definitionen von Microsoft sind unter http://www.microsoft.com/Net/basics_glossary.aspx und http://msdn.microsoft.com/library/deu/default.asp?url=/library/DEU/netstart/html/cpglon.asp zu finden.
Interessant in diesem Zusammenhang ist auch die „Deutsche Community-Site für .NET, Windows Scripting und mehr“, wie sie sich selbst bezeichnte, unter http://www.it-visions.de/(ywfmy1553hzbgfvfpx3xb045)/default2.aspx?start=http://www.it-visions.de/about/HolgerSchwichtenberg.asp

Bild 30: Komponenten des .NET-Frameworks

Die Anwendungen werden in einer von „.NET“ unterstützten Sprache programmiert und können auf die umfangreichen „.NET“-Klassenbibliotheken zurückgreifen. Durch das „.NET“ Framework werden eine große Anzahl an Programmiersprachen unterstützt. Der jeweilige Compiler übersetzt den Quellcode in einen Befehlscode (keinen Maschinencode), der als Intermediate Language (IL) bezeichnet wird;. die Kombination aus solchen Kompilaten und zugehörigen Metadaten wird als "Assembly" bezeichnet und ist die typische Deployment-Einheit der .NET-Welt. Ergebnis dieser Aktion ist z.B. eine EXE-Datei. Wird diese EXE-Datei geladen, wird sie von der Common Language Runtime (CLR) mit ihrem JIT-Compiler (Just-In-Time) in Maschinencode umgesetzt.

Neben der Generierung und Verwaltung von Maschinencode bietet die CLR weitere Leistungen, insbesondere zur Speicherverwaltung (Garbage Collection), und führt IL-Programme darüber hinaus in einer kontrollierten Weise aus. IL-Programme werden daher auch als "Managed Components" bezeichnet. Wesentliches Merkmal dieser kontrollierten Ausführung ist die Code Access Security (CAS). Sie erlaubt die Definition und gewährleistet die Durchsetzung von Ausführungsrechten. Dabei wird nicht nur die Identität des ausführenden Benutzers herangezogen, sondern auch der Autor und die Herkunft des Programmes.

Neben Managed Components ist auch die Ausführung von herkömmlichem "Native Code" möglich, der direkt mit dem Prozessor und dem Betriebssystem interagiert. Die CLR kontrolliert die Ausführung dieses Codes zwar nicht in der beschriebenen Weise, dient aber als Vermittler zwischen "Managed" und "Unmanaged Code", beispielsweise um mit Hilfe so genannter "Interop-Assemblies" eine Brücke aus der .NET- zurück in die .COM-Welt zu schlagen.

Für die Erstellung des Quellcodes bietet Microsoft

- zum einen ein kostenloses Software Developer Kit (SDK), das bereits ausreicht, um „.NET-Programme“ zu erstellen,
- zum anderen Visual Studio.NET, der Nachfolger des bisherigen Visual Studio Version 6

an.

Das Microsoft .NET-Framework kann im Gegensatz zu Java und der JVM nur für Microsoft Betriebssysteme genutzt werden. Wichtige Teile des Frameworks (die Common Language Infrastructure (CLI) und die Programmiersprache C#) wurden als ISO-Standard verabschiedet. Basierend auf diesen Standards sind auch nicht windowsbasierende Implementierungen von .NET möglich[1]. Ein Beispiel hierfür ist Mono, das derzeit in der Version 1.0[2] erschienen ist.

.NET und Web-Services

.NET-Framework (siehe Kapitel 3.9.5) unterstützt die Entwicklung von professionellen Web Services. .NET ist die Nachfolgetechnologie von Windows DNA (Distributed interNet Applications Architecture) als internetkompatible Software Architektur. .NET beinhaltet einen eigenen Service Layer für Web Services. Die folgende Abbildung (Bild 31) zeigt das Zusammenspiel der einzelnen Bausteine hinsichtlich der Web Services.

[1] In wie weit diese technischen Möglichkeiten am Ende durch rechtliche Belange, wie Patente oder Urheberrecht, beschränkt werden, muss sich erst noch zeigen.

[2] Siehe auch http://www.mono-project.com/about/index.html.

Bild 31: Microsoft .NET Framework

Durch die Einführung von ASP.NET, dem Nachfolger der Active Server Pages, wird den Zielen

- einer möglichst einfachen und variablen Entwicklungsumgebung
- und den angesprochenen Web Services

Rechnung getragen.

Auf der anderen Seite bietet Visual Studio.NET die Möglichkeit, auf relativ einfache Weise (Client-) Anwendungen zu schreiben, die Web Services auf Basis von XML und SOAP nutzen.

Kernstück der Web-Services unter Windows ist der Internet Information Server (IIS) (siehe Kapitel 3.10).

3.9.6 Java 2 Enterprise Edition (J2EE)

Die Java 2 Enterprise Edition umfasst eine Menge von Middleware-Diensten, die die Entwicklung von serverseitigen Applikationen erleichtern. Wichtige Bestandteile der J2EE Technologien sind:

- Enterprise JavaBeans (EJB)
  Enterprise-Beans sind serverseitige Komponenten, welche die Anwendungslogik implementieren. Auf diese können die Clients dann zurückgrei-

fen. Enterprise-Beans werden in einem EJB-Container serverseitig installiert. Dieser stellt ihnen bestimmte Dienste und Laufzeitumgebungen zur Verfügung.

- Java Naming and Directory Interface (JNDI)
  Hierbei handelt es sich um einen Namens- und Verzeichnisdienst, der zum einen die Möglichkeit bietet, Referenzen auf entfernte Objekte
  - unter einem bestimmten Namen und
  - an einem definierten Platz zu hinterlegen (Binding).

  Zum anderen ist es über JNDI möglich, gebundene Objekte über deren Namen wieder zu finden (Lookup).
- Java IDL/Corba
  Java IDL bildet eine Schnittstelle zu Corba, mit Java IDL können Java-ORBs implementiert werden.
- Java Remote Method Invocation (RMI) und RMI via IIOP (RMI-IIOP)
  RMI wird für die verteilte Kommunikation zwischen Objekten eingesetzt. Mit RMI-IIOP ist J2EE kompatibel mit CORBA.

Daneben gibt es noch weitere Dienste:

- Java Database Connection (JDBC)
- Java Message Service (JMS)
- Java Servlets / Java Server Pages (JSP)
- Java Transaction API (JTA)
- Java API for XML (JAXP)
- u.v.m.

Bild 32 gibt einen groben Überblick über das Schichtenmodell von J2EE.

Bild 32: Schichtenmodell J2EE

J2EE und Webservices

Die J2EE Architektur (siehe Kapitel 3.9.6) basiert auf der Programmiersprache Java. Deren Vorteil ist, dass damit geschriebene Programme plattformenabhängig angewendet werden können. Ursprünglich wurde J2EE als Architektur für serverseitige Anwendungen entwickelt. Die Plattform wurde hinsichtlich einer Unterstützung von XML-basierten Web Services erweitert.

Die Geschäftslogik-Schicht, die mit EJB (Enterprise Java Beans) Komponenten realisiert wird, beinhaltet die Geschäftsprozesse und die Datenlogik. Sie stellt die Verbindung zu Datenbanken mittels JDBC (Java Database Connectivity) her und kann ebenfalls auf externe Web Services zugreifen. Zugriffe auf J2EE Applikationen können zum einen unter der Verwendung von Web Service Technologien erfolgen, wobei Web Service Anfragen durch Servlets bearbeitet werden. Zum anderen können herkömmliche Clients wie Applets oder Applikationen parallel dazu wie gewohnt direkt auf EJB Komponenten zugreifen. Web Browser und drahtlose Geräte werden üblicherweise über Java Server Pages (JSP) mit EJB Komponenten verbunden.

Entwicklungsumgebungen werden von verschiedenen Anbietern zur Verfügung gestellt, z.B. von IBM, SUN und BEA.

3.9.7 Component Object Model (COM)

Basis vieler von Microsoft hervorgebrachter Technologien ist das Component Object Model (COM). Vergleichbare komponentenorientierte Technologien sind CORBA (Common Object Request Broker Architecture) von der Object Management Group (OMG) oder Java Beans von SUN.

COM ist eine Weiterentwicklung von OLE (Object Linking and Embedding), welches primär der Erzeugung von Compound Documents diente. COM ist ein Binärstandard für Komponenten und daher unabhängig von Programmiersprachen.

COM-Komponenten können mit verschiedene Programmiersprachen erzeugt werden, hierzu gehören u.a.:

- C++
- C
- Java
- Visual Basic
- Delphi.

Gleichzeitig können bei einigen dieser Sprachen COM-Komponenten selbst wieder verwendet werden. Die einzige Anforderung an eine Programmiersprache besteht darin, dass Zeiger-Strukturen realisiert werden können und Funktionen entweder explizit oder implizit mittels Zeiger aufgerufen werden können. Objektorientierte Sprachen liefern Mechanismen, die die Implementierung von COM-Komponenten vereinfachen.

Die häufigste Form, in der COM-Komponenten auftreten, sind dll-Dateien. Weitere Varianten sind:

- Dynamic Linking Libraries (*.DLL, *.OCX)
- ausführbare Windows Dateien (*.EXE)
- Java-Klassen (*.CLASS)
- Skriptdateien (*.SCT, *.WSC).

COM bietet mit dem Dienst Distributed COM (DCOM) eine transportprotokollneutrale Middleware zur Nutzung entfernter Komponenten auf anderen Rechnern. DCOM gehört zum Standard von Windows NT[1]. Der Aufruf von Komponenten auf entfernten Rechnern basiert dabei auf Remote Procedure Calls (RPC). Es ist somit in der ISO/ OSI-Schicht 7 (Application Layer) angesiedelt und kann in der Theorie auf verschiedenen Transportprotokollen (z.B. TCP/ IP, IPX/ SPX) aber auch auf HTTP aufsetzen. Die Nutzung von HTTP ist mittels der COM Internet Services (CIS) eines IIS Version 4 möglich, in dem das DCOM-Protokoll durch HTTP getunnelt wird. Die Sicherheit von DCOM kann durch das Werkzeug DCOM Configuration Utility (DCOMCNFG.exe) administriert werden. Insbesondere wird hiermit festgelegt, welches Maß der Impersonifizierung verwendet werden soll, also die Fähigkeit einer Softwareroutine, den Benutzerkontext zu wechseln.

Die Nutzung von COM-Komponenten ist nur unter Windows möglich. Anwendungen, die auf diese zurückgreifen, müssen für eine Portierung auf eine andere Plattform angepasst werden.

Die Erweiterung von COM und DCOM unter Windows 2000 ist COM+. COM + beinhaltet darüber hinaus die Integration der bisherigen Windows NT 4.0 Option Pack Komponenten und damit Laufzeitdienste, die mit genutzt werden können.

[1] Dies gilt auch für Windows 2000, XP und Server 2003.

3.9.8 Fazit

Aus den technischen Betrachtungen wird deutlich, dass die bisherige Komponententechnologie (COM, DCOM) von Microsoft zwar weitergeführt wird, gleichzeitig aber auch mit dem .NET-Framework ein Technologiewechsel stattfindet. Dem gegenüber steht die Java 2 Enterprise Edition (J2EE) als alternative Plattform. Grundlegende Unterschiede bei beiden Plattformen, die auch eine nicht unwesentliche Rolle bei den oben betrachteten Web-Services einnehmen, sind die Plattformabhängigkeit, die unterstützten Programmiersprachen und Anzahl der Lösungsanbieter. Die nachfolgende Tabelle gibt einen weiteren Aufschluss über die Unterschiede.

Tab. 22: Gegenüberstellung J2EE und .NET

Parameter	J2EE	.NET
Allgemein	Trademark von SUN Eine Sprache – Viele Anbieter	Produkt-Suite Viele Sprachen – ein Anbieter
Standard	Industriestandard	In Teilen (CLI und C#) ISO-Standard
Sprachen	Java	C#, VB, C++, J#, Java, COBOL und weitere...
Komponentenmodell	Enterprise JavaBeans	.NET (Web) Services; COM+
Interpreter	JRE (Java TM Runtime Environment)	CLR (Common Language Runtime)
Anbieter	BEA, IBM, SUN, Oracle...	Microsoft
Betriebssystem	Unix, Windows, Linux, OS/390...	Windows
Browser	Beliebig, mit Java Support	Beliebig
Web-Server	Beliebig	MS IIS, Apache, Tomcat
Web-Server-Komponenten	JSP, Servlets	ASP.NET
Datenbank-Zugriff	JDBC	ADO.NET
Verzeichnisdienst	Beliebig, über JNDI	Active Directory

3.10 Webserver

3.10.1 Überblick

In Hinblick auf eine Webservermigration steht neben den weiterführenden Microsoft-Produkten mit dem Internet Information Server 5.0 und 6.0 auch der Apache Webserver als die alternative Lösung zur Verfügung.

Für den Einsatz des Apache Webservers sind keine grundlegenden technischen Einschränkungen bekannt, in dieser Hinsicht bietet er alle notwendigen Funktionalitäten für den Einsatz in einem produktiven Umfeld. Diese Einsatzfähigkeit hat der Apache in der Realität in zahlreichen Einsatzszenarien unter Beweis gestellt.

Im Einzelfall sind jedoch die Aufwände für ein Migrationsprojekt genauer zu ermitteln. Bei einer Migration von einfachen HTML-Seiten bzw. CGI-Anwendungen werden sich die Migrationsaufwände in der Regel in einem überschaubaren Rahmen halten.

Hingegen erfordert eine Migration von komplexen Anwendungen, insbesondere zur Generierung von dynamischen Inhalten auf Basis der ASP-Technologie, in der Regel eine Neuimplementierung der Anwendungen, wodurch erhöhte Aufwände entstehen. Dem stehen jedoch aus technischer Sicht keinerlei Probleme entgegen, da ausreichend alternative Technologien, wie z.B. PHP und JSP zur Verfügung stehen.

3.10.2 Einleitung

Der bekannteste Dienst des Internet ist das World Wide Web (WWW). Es ist eine klassische Client-Server-Anwendung, bei welcher der Client passiv Informationen vom Server bezieht. Die Grundlage des World Wide Web basiert auf dem zustandslosen Protokoll HTTP (Hypertext Transfer Protocol) und der Seitenbeschreibungssprache HTML (Hypertext Markup Language). Der Server übernimmt die Aufgabe, Client-Anfragen zu beantworten und die gewünschten Inhalte auszuliefern. Webserver haben auch die Aufgabe, dynamisch generierte Inhalte, z.B. durch eine Datenbankanwendung, an die Client-Systeme zu liefern. Über bestimmte Schnittstellen ist es auch möglich, komplette Programme auf den Servern zu starten und Aktionen ausführen zu lassen. Die Aktionen werden in der Regel von den Client-Systemen initialisiert. Dadurch können vom Client aus bestimmte Prozesse auf einem Server angestoßen werden. Durch die Ausbreitung des Internets bzw. von Intranet-Lösungen haben sich die Ansprüche und Aufgaben an die Web-Server immer weiter erhöht, aus diesen Gründen entstanden unterschiedliche Lösungen und Programme.

3.10.3 Internet Information Server 4.0

Der Microsoft Internet Information Server (IIS) ist ein Datei- und Anwendungsserver für das Internet und Intranet. Der IIS 4.0 ist Teil des Windows NT Server 4.0 Option Pack. Auf Basis des Betriebsystem Windows NT 4.0 werden mit den IIS die Grundfunktionalitäten eines Webservers bereitgestellt.

Für eine erfolgreiches Zusammenspiel zwischen der Client- und Serverseite erfolgt die Unterstützung aller relevanten Internetprotokolldienste:

- HTTP 1.1
- SMTP
- NNTP
- FTP.

Die HTTP-Unterstützung des ISS 4.0 umfasst die folgenden Leistungsmerkmale:

- Pipelining
  Dies ermöglicht das Senden von vielen Clientanforderungen, bevor eine Reaktion des Webservers erfolgt.
- Keep Alives
  Durch das Aufrecht erhalten von Client-Server-Verbindungen kann ein Client für mehrere Anforderungen eine einzige oder eine geringere Zahl von Verbindungen einsetzen.
- HTTP PUT und DELETE
  Dies ermöglicht das Löschen oder Bereitstellen von Dateien durch Benutzer über die Verwendung eines Browsers. Auch die RFC 1867-Unterstützung ermöglicht die Steuerung von Datei-Uploads über andere Programme.

Die SMTP-Unterstützung wird durch einen implementierten SMTP-Mail-Dienst, der SMTP-Mail-Nachrichten senden und empfangen kann, bereitgestellt. Der Dienst kann zur Kommunikation zwischen dem Webserver und beispielsweise den Kunden verwendet werden.

Der integrierte NNTP-Dienst (Network News Transport Protocol) ermöglicht die Einrichtung lokaler Diskussionsgruppen auf einem einzelnen Server. Eine Unterstützung von Newsfeed oder Replikation ist nicht möglich.

3.10.3.1 Webanwendungen

Der Internet Information Server bietet folgende Erweiterungen für den Server an:

- CGI-Programme
- ISAPI-Anwendungen
- ASP-Anwendungen.

Das Common Gateway Interface (CGI) ist eine Möglichkeit der Generierung von dynamischen Inhalten. Das CGI ist eine Schnittstelle zum Aufruf von Programmen, derer sich der Server bedienen kann. CGI wurde ursprünglich für UNIX-Umgebungen entwickelt und beansprucht allerdings unter Windows NT sehr viele Systemressourcen. CGI-Programme haben den Vorteil, dass sie fast jeder Webserver ausführen kann und sie in der Regel einfach zu programmieren sind.

Das Internet Service Application Programming Interface (ISAPI) ist eine direkte Schnittstelle zum IIS. Über ISAPI kann auf Server-Objekte zugegriffen werden.

Der IIS 4.0 ermöglicht durch den Einsatz von Active Server Pages (ASP) das Erstellen von dynamischen HTML-Seiten oder Webanwendungen. Mit der ASP-Technologie wird eine serverseitige Skriptumgebung bereitgestellt. ASP-Seiten sind Dateien, die neben herkömmlichen HTML-Tags auch Skriptbefehle enthalten können. Die entsprechenden Skriptbefehle werden auf dem Server ausgeführt und zur Erzeugung von HTML-Code genutzt. Der dynamische und statische HTML-Code wird in Form einer HTML-Seite an den anfordernden Browser zu-

rückgegeben. Die Verwendung von ASP-Seiten ermöglicht die Gestaltung von interaktiven Inhalten für die Benutzer. Auch Datenbankzugriffe lassen sich mit den ASP-Seiten realisieren.

Im Zusammenhang mit der Entwicklung von Webinhalten werden durch den IIS 4.0 folgende Technologien unterstützt:

- **Microsoft Script Debugger**
  Dieser ermöglicht den Test von ASP-Anwendungen.
- **COM-Programmierschnittstelle**
  Diese ermöglicht den Entwicklern Zugriff auf die COM-Komponenten, die auf die Protokollfunktionen des ISS zugreifen.
- **Java Virtual Maschine**
  Diese ermöglicht das Erstellen und Ausführen von Java-Komponenten innerhalb einer virtuellen Maschine.
- **IIS Admin-Objekte**
  Diese bieten den Entwicklern Zugriff auf die notwendigen Komponenten zur Erstellung von Verwaltungsdienstprogrammen.
- **Transaktionale ASP-Seiten**
  Diese ermöglichen ASP-Seiten und deren aufgerufenen Komponenten, Teil eine Transaktion zu sein, die jedoch vom Microsoft Transaction Server (s.a.) verwaltet werden muss.
- **Prozessisolierung**
  Hiermit können ASP und ISAPI-Anwendungen (Internet Server-API) in getrennten Prozessen ausgeführt werden. Die Prozesse werden neben dem Serverhauptprozess ausgeführt.
- **Laden und Entladen von Komponenten**
  D.h., Webentwickler können dynamisch Komponenten einer Webanwendung laden oder entladen.

3.10.3.2 Authentifizierung und Sicherheit

Das Sicherheitsmodell ist für alle NT-Server-Komponenten gleich, die gleichen Funktionen die für die Datei- oder Datenbankserver zur Verfügung stehen, können auch für den IIS genutzt werden. Es können die vorhandenen Domänenbenutzer und –gruppen zur Vergabe von zugeschnittenen Rechten und Berechtigungen verwendet werden, der IIS verwendet die gleiche Verzeichnisdatenbank wie die anderen Windows NT Server. Den Benutzern kann ein eingeschränkter Zugriff auf die Netzwerkressourcen wie HTML-Seiten, Webanwendungen und Dateien ermöglicht werden. Für die feingranulare Rechtevergabe können auch die Dateisystemberechtigungen des NTFS verwendete werden.

Die Verwendung des Secure Sockets Layer (SSL) ermöglicht ein Verfahren zum sicheren Austausch von Informationen zwischen Clients und Server. Es besteht

auch die Möglichkeit, dass der Server die Client-Identität überprüfen oder authentifizieren kann und der Benutzer sich nicht am Server anmelden muss.

Der integrierte Certificate Server bietet die Möglichkeit, eine Zertifizierungsinstanz einzurichten und die X.509-Standardzertifizierung für Clients zur Verfügung zu stellen.

3.10.3.3 Zusätzliche Komponenten des Internet Information Servers

Neben der Kernkomponente des IIS bietet Microsoft verschiedene Komponenten zur Erweiterung der Webserverfunktionalitäten an. Die im folgenden beschriebenen Komponenten sind ebenfalls Teil des Windows NT Option Pack.

Microsoft Transaction Server (MTS)

Der MTS ist ein Transaktionsverarbeitungssystem zum Entwickeln, Implementieren und Verwalten verteilter Serveranwendungen. Die Transaktionsverarbeitung kann beispielsweise zur Realisierung verteilter Geschäftsanwendungen eingesetzt werden.

Microsoft Script Debugger

Der Microsoft Script Debugger soll das Auffinden von Programmierfehlern in ASP-Dateien unterstützen. Der Debugger kann in Verbindung mit dem Internet Explorer ausgeführt werden und zur Fehlerkorrektur verwendet werden.

Microsoft Index Server

Der Index Server kann als Suchmaschine für die Internet- und/oder Intranetinhalte verwendet werden. Der Server kann die Textinhalte der gespeicherten Inhalte indizieren und diese können über Webformulare für die Benutzer durchsuchbar gemacht werden. Der Index Server kann neben reinen HTML-Dokumenten auch Microsoft Word und Excel Dokumente indizieren.

Microsoft Message Queue Server

Der Microsoft Message Queue Server (MMQS) lässt Anwendungsprogramme durch das Senden und Empfangen von Nachrichten asynchron mit anderen Anwendungsprogrammen kommunizieren.

Microsoft Management Console

Die Microsoft Management Console (MMC) ermöglicht die Verwaltung unterschiedlichster Aufgaben durch verschiedene Netzwerk-Verwaltungsprogramme. Durch so genannte „Snap-Ins“ innerhalb der Konsole kann die Administration der Server erfolgen.

3.10.4 Ablösende Migration

3.10.4.1 Apache

Die in der Praxis auf einem linuxbasierten System sehr häufig eingesetzte Anwendung ist der Apache-Webserver. Er ist mit einer Verbreitung von über 60%

der am häufigsten eingesetzte Webserver[1] weltweit. Er ist frei verfügbar und steht unter der Apache Software Lizenz. Der Apache-Webserver ist eines der erfolgreichsten Projekte der Open Source Community. Das Projekt hat sich aus dem NCSA-Server (National Center for Supercomputing Application, Uninversity Illinois) entwickelt, dem immer mehr Patches hinzugefügt wurden („A patchy web server“) und der als Basis für die erste Beta-Version 1995 diente. Zwischenzeitlich ist er auf nahezu alle Plattformen portiert worden. Der Apache Server ist heute der weitverbreiteste Webserver auf Linux/Unix-Plattformen, er läuft jedoch auch auf einer ganzen Reihe von anderen Plattformen, wie Windows NT oder Novell Netware.

Seit der Version 2.0.35 vom April 2002 ist die Entwicklungsreihe 2.0 des Apache-Webservers als stabil freigegeben und wird auch von den Entwicklern für den Produktiveinsatz empfohlen. Derzeit wird auch noch die Entwicklungsreihe 1.3.x zusätzlich zu der neuen 2.0.x weiter gepflegt.

Durch seine Lizenzbestimmungen und seine hohe Qualität wird der Apache-Webserver auch in kommerziellen Produkten verwendet. IBM liefert beispielsweise Apache im Rahmen des Websphere-Produktes aus.

Funktionsumfang

Der Apache-Webserver besteht aus seinem Kern und einer großen Anzahl von Modulen, die in Abhängigkeit von den jeweiligen Anforderungen einkompiliert bzw. geladen werden können. Durch den modularen Aufbau ist der Apache-Server sehr leicht erweiterbar und kann den geänderten Anforderungen angepasst werden. Im normalen Lieferumfang der Software sind schon eine Vielzahl von unterschiedlichen Modulen enthalten, diese können noch durch weitere Module (z.B. Eigenentwicklungen) erweitert werden. Apache Module sind Codesegmente, die der Apache API Spezifikation entsprechen und in den Apache Web-Server geladen werden können. Apache Module können entweder statisch fest eingebunden sein oder dynamisch über die Konfigurationsdatei des Webservers geladen werden. Dieses modulare Design zur Erweiterung von Web-Server Eigenschaften erhöht ungemein die Flexibilität des Systems. Die Effizienz und die Geschwindigkeit des Web-Servers erhöht sich, wenn anstelle von externen Applikationen interne Prozesse abgearbeitet werden können.

Unter den vielen Modulen finden sich Authentifikations-, Sicherheits- und Skript- beziehungsweise Interpretermodule für Programmiersprachen, wie zum Beispiel PHP, Java, Python, Tcl und Perl. Für die Verwendung der Module bestehen zwei unterschiedliche Möglichkeiten:

- Die Module können bei der statischen Übersetzung des Webservers fest eingebunden werden
- Die Module können im Betrieb des Servers dynamisch geladen werden. Diese so genannte DSO-Funktionalität (Dynamic Shared Objects) spart

[1] http://news.netcraft.com/archives/2003/03/

bei einer Änderung der Server-Konfiguration das erneute Übersetzen. Ein Neustart des Servers ist ausreichend, ein Graceful-Restart ohne Unterbrechung des Dienstes ist möglich.

Indem nur die tatsächlich benötigten Module benutzt werden, bleibt der Apache kleiner als eine Standardversion und belegt weniger Speicherplatz. Gleichzeitig bedeuten weniger Module auch weniger Angriffsfläche, wodurch die Sicherheit des Systems erhöht wird.

Die folgende Tabelle gibt eine kleine Auswahl der verfügbaren Module wieder.

Tab. 23: Apache-Module

Modul	Funktion
Standard- und Zusatz-Module	
mod_cgi	Ausführung von CGI-Skripten (Common Gateway Interface).
mod_dav	Integrierte DAV Unterstützung (HTTP Extensions for Distributed Authoring – WebDAV). Bearbeiten von Dateien und Verzeichnissen direkt über HTTP auf dem Webserver. DAV steht für Distributed Authoring and Versioning.
mod_fastcgi	Integrierte FastCGI Unterstützung.
mod_frontpage	Integrierte FrontPage Unterstützung.
mod_iserv	Integrierte Java Servlet Unterstützung.
mod_php3	Integrierte PHP 3 Unterstützung.
mod_php4	Integrierte PHP 4 Unterstützung.
mod_perl	Integrierte Perl Unterstützung.
mod_alias	Stellt die Alias- bzw. Redirect-Anweisungen zur Verfügung.
mod_autoindex	Generiert Verzeichnisindizies.
mod_include	Wird benötigt für Server-Sides Includes.
mod_mime	Sorgt für Generierung entsprechende MIME-Headers.
mod_log_config	Zur Führung von einer oder mehrerer Logfiles, der Inhalt kann an die entsprechenden Bedürfnisse angepasst werden.
mod_deflate	Dient der Komprimierung von verschiedenen Dateitypen vor der Übertragung zum Browser. Ist insbesondere bei eingeschränkten Bandbreiten sinnvoll, die Kompression muss von den Browsern unterstützt werden.
mod_proxy	Erweitert den Apache-Webserver um die Funktionalität eines Proxys bzw. Proxy-Caches.
mod_rewrite	Ermöglicht die Verwendung von internen Aliasen und externen Redirects.
mod_speling	Korrigiert Tippfehler der Benutzer.
mod_ssl	Stellt die Protokolle SSL (Secure Sockets Layer) und TLS (Transport Layer Security) zur Verfügung.
mod_usertrack	Mittels HTTP-Cookies wird das Nutzerverhalten protokolliert.
mod_vhost_alias	Für die massenhafte Konfiguration von virtuellen Hosts, insbesondere für Service-Provider interessant.
Module zur Authentifizierung	
mod_access	Zugriffskontrolle auf Basis von Hostnamen oder IP-Adressen.

Modul	Funktion
mod_auth	Für die Konfiguration von passwortgeschützten Verzeichnissen bzw. Dokumenten. Sehr einfache Variante eines Authentifizierungsmoduls, sollte nur einer geringen Anzahl von Nutzern angewendet werden.
mod_auth_digest	Nutzer- Authentifikation mittels MD5 Digest Authentication, die Übermittlung der Passwörter erfolgt nicht im Klartext.
mod_auth-dbm	Nutzer-Authentifikation mittels Berkeley-DB-Dateien, sinnvoll für die Verwendung bei einer größeren Anzahl von Benutzern.
mod_auth_ldap	Nutzer-Authentifikation mittels LDAP.
mod_auth_kerb	Nutzer-Authentifikation mittels Kerberos, unterstützt die Versionen 4 und 5.
mod_auth_notes	Nutzer-Authentifikation mittels Lotus Notes Server.
mod_auth_oracle	Nutzer-Authentifikation mittels Oracle-Datenbank, es gibt auch noch weitere Module für beispielsweise MySQL und Postgres-Datenbanken.
mod_auth_smb	Nutzer-Authentifikation mittels SMB-Server (Samba, Windows NT).

Diese Auflistung der verfügbaren Module ist nicht vollständig und bietet nur einen Ausschnitt über die Möglichkeiten des Apache-Webserver.

Aber nicht alle Module für den Webserver sind kostenlos verfügbar. Es finden sich im kommerziellen Umfeld immer mehr Unternehmen, die native Apache-Module anbieten. Einige Beispiele sind:

- Allaire mit der Java-Servlet-Engine Macromedia JRun und dem Application-Server Macromedia ColdFusion,
- Sun Microsystems mit seinem Active Server Pages Modul.

Verwandte Themen

Für die Integration einer Suchfunktionalität innerhalb einer Website kann der Apache-Webserver durch ein entsprechendes Programm ergänzt werden. Es stehen unterschiedliche Softwareeinheiten zur Auswahl, im Folgenden wird beispielhaft das Suchsystem HTDig[1] beschrieben. HTDig ermöglicht die Indexierung ganzer Websites, das Programm erzeugt mittels eines so genannten Robots einen Suchindex, der über ein geeignetes CGI-Skript abgefragt werden kann. Die folgenden Punkte geben die Kernfunktionalitäten der Software wieder:

- Anlage eines Suchmaschinen-Index (über eine oder mehrer Website, bzw. von Teilbereichen einer Website).
- Einschränkung der Indexierung durch die Verwendung von Filtern, Filterkriterien können Dateitypen und bestimmte URLs sein.

[1] http://www.htdig.org/

- Durch die Verwendung von externen Zusatzprogrammen können auch Dateiformate(PDF. DOC, usw.) indexiert werden.
- Es bestehen zahlreiche Abfragemöglichkeiten und es können verschiedene Suchalgorithmen verwendet werden (Wörter, Wortteile, Synonyme, usw.).
- Die Such-Seite und die entsprechende Trefferliste kann über einfache Template-Dateien angepasst werden.
- Umlaute werden innerhalb der Suchbegriffe unterstützt.
- Der verwendete Robot unterstützt den Standard für „Robot Exclusion“ und die „Basic-WWW-Authentication“, zur Indexierung geschützter Inhalte.

Die HTDig-Distribution steht unter der GNU General Public License (GPL) und somit zur freien Verfügung.

Administration

Die Konfiguration des installierten Apache ist relativ einfach, da für die meisten Konfigurationen nur Einträge in einer gut dokumentierten Datei abgeändert oder hinzugefügt werden müssen. Diese ist eine einfache Textdatei, die mit jedem Texteditor editierbar ist. Für Administratoren, die eine graphische Oberfläche bevorzugen, gibt es bereits einige kommerzielle und nicht-kommerzielle Projekte zur Apache-GUI[1].

Migration

Im Rahmen einer Migration ist zu unterscheiden, welche Daten bzw. Inhalte migriert werden sollen. Es kann differenziert werden in:

- HTML-Dateien
- CGI-Programme (Perl, PHP, C, usw.)
- Programm-Module, die ISAPI (Internet Server Application Programming Interface) des Internet Information Servers nutzen
- und Active Server Pages.

HTML-Seiten

Statische Inhalte, also reine HTML-Seiten, können ohne weitere Anpassung auf den neuen Webserver exportiert werden und dürften bei einer Umstellung des Webservers die geringsten Probleme und Aufwände bereiten.

Common Gateway Interface

Programme, die für das Common Gateway Interface (CGI) entwickelt wurden, nutzen auch den spezifischen CGI-Standard. Dieser legt fest, wie die Programme und die Web-Server interagieren. Dieser Standard ist nicht sprachspezifisch und wird von Apache-Webserver unterstützt. Für die Entwicklung von CGI-

[1] s.a. http://gui.apache.org/

Programmen stehen zahlreiche Auswahlmöglichkeiten zur Verfügung. Eine der am weitesten verbreiteten und portabelsten Skript-Sprachen ist Perl. Perl steht unter anderem auf MS-DOS, UNIX/ Linux, OS/ 2, Macintosh und jeder Windows-Variante zur Verfügung. Perl bietet auch den Web-Entwicklern umfangreiche Möglichkeiten zur Text- und Datenmanipulation. Anwendungen, die in Perl entwickelt wurden, können sehr leicht auf den Apache-Webserver migriert werden. Apache verfügt mit dem Module „mod_perl“ über die volle Perl-Implementation, darüber hinaus kann oftmals eine Performance-Verbesserung bei der Ausführung erzielt werden. Das Perl-Modul bettet einen Perl-Interpretor in den Apache-Webserver ein, so dass für das Ausführen des Programmcodes kein separater Prozess mehr gestartet werden muss und ein enormer Geschwindigkeitszuwachs erzielt werden kann. Bei der Portierung der Perl-Anwendungen sind nur minimale Änderungen am Programmcode notwendig.

PHP ist eine der sich am schnellsten verbreitenden Skript-Sprachen, die sich durch die sehr gute Unterstützung von unterschiedlichsten Datenbanksystemen und der relativ einfache Syntax auszeichnet. PHP ist wie Perl auf vielen unterschiedlichen Systemen lauffähig. PHP-Anwendungen, die für den Internet Information Server entwickelt wurden, können mit minimalem Aufwand auf den Apache-Webserver portiert werden.

ISAPI

Anwendungen, die ISAPI nutzen, können nur bei Apache-Webservern weiterverwendet werden, wenn diese auf einem Windows NT oder 2000 basierten System betrieben werden. Apache beinhaltet als Standardfunktionalität unter Windows-Systemen die komplette ISAPI-Kompatibilität. Die Applikationen müssen in der neuen Apache-Umgebung nur neu kompiliert werden. In der Regel ist also keine Code-Änderung notwendig, jedoch werden ISAPI-Filter und die Microsoft-Erweiterungen für asynchrone Dateioperationen nicht unterstützt.

ASP

Applikationen, die auf der ASP-Technologie aufbauen, wurden in der Regel zur Generierung von dynamischen Web-Inhalten entworfen. Dabei können verschiedene Grundlagen

- Visual Basic Script (VBScript)
- JScript
- und ActiveX Data Objects (ADO) für den Zugriff auf Datenbanken

angewandt werden. Um ASP-Seiten auf dem Apache-Webserver auszuführen, wird die komplette Microsoft-kompatible Entwicklungsumgebung (VBScript, JScript, ADO) benötigt. Die Firma Sun Microsystems bietet mit seinem „Sun One Active Server Pages 4.0“-Produkt[1] eine kompatible Umgebung zur Ausführung von ASP-Seiten innerhalb des Apache-Webservers an. Der Webserver kann auf

[1] S.a. http://sun.de/Produkte/software/chilisoft/

einem NT-Betriebssystem bzw. auf einen Unix/Linux-Betriebssystem betrieben werden.

Das Produkt unterstützt:

- ASP 3.0
- VBScript 5.5
- JScript 5.5.

Für die Migration auf einen Apache-Webserver auf einem Linux-System sind in einem ersten Schritt die gesamten ASP-Dateien auf die neue Ziel-Plattform zu kopieren. In einem weiteren Schritt sollten die verwendeten COM-Objekte innerhalb der ASP-Applikationen bestimmt und mit den unterstützen Objekten unter Linux abgeglichen werden. Zahlreiche Objekte werden durch die Sun One ASP unterstützt. Sollte das benötigte Objekt nicht unterstützt werden, besteht die Möglichkeit, die mitgelieferte COM-to-Java Bridge zu verwenden und die Funktionalität mittels Java zu implementieren. Zusätzlich sind noch Änderungen in Bezug auf die Groß- und Kleinschreibung und der ASP- bzw. Scripting Engine Version zu überprüfen. Eine genaue Beschreibung ist der entsprechenden Dokumentation zu entnehmen. Das Thema der notwendigen Datenbank-Migration wird nicht in diesem Abschnitt betrachtet. Genaue Informationen sind im Kapitel Datenbanken enthalten.

Neben der Möglichkeit, die ASP-Applikationen in ihrer bisherigen Form beizubehalten, besteht natürlich auch die Möglichkeit, alternative Technologien einzusetzen. Dies bietet sich an, wenn signifikant eine größere Plattform-Unabhängigkeit gewünscht wird. Dabei ist jedoch mit höheren Migrationsaufwänden zu rechnen, da die Applikations-Realisierung in einer neuen Technologie in der Regel erhöhte Aufwände bedingt. Allerdings kann der Migrationsprozess auch zu einer Konsolidierung und Optimierung der Inhalte und Applikationen genutzt werden.

Eine echte Alternative für viele Anwendungszwecke kann der Einsatz der PHP-Technologie sein. Insbesondere aus der Kombination

- Linux
- Apache
- MySQL
- PHP

hat sich in den letzten Jahren eine sehr beliebte Plattform (LAMP) für die Generierung von Web-Inhalten entwickelt. Wenn eine Umwandlung der ASP-Applikationen in PHP erfolgen soll, kann die Betrachtung der Projektinhalte von „ASP-to-PHP“[1] eventuell hilfreich sein. Das Projekt stellt auf seinen Homepage einen ASP-to-PHP-Konverter zur Verfügung und bietet Unterstützung im Rahmen seiner Mailing-Liste an.

[1] http://asp2php.naken.cc

Neben dieser Möglichkeit kann auch der Einsatz von javabasierter Technologie erwogen werden. Javabasierte Web-Applikationen stellen eine interessante Alternative zu den Web-Applikationen auf Basis von ASP dar. Die derzeitig gebräuchlichsten Java-Applikationen basieren auf der Java 2 Standard Edition (J2SE) und Java 2 Enterprise Edition (J2EE) Spezifikationen von Sun Microsystems. Die Java-Technologie, basierend auf einem Industrie-Standard, bietet den Vorteil der Plattform-Unabhängigkeit. J2SE Web-Applikationen erlauben die Entwicklung von dynamischen Inhalten mittels Java Server Pages (JSP) und Java Servlets. Beide Technologien ermöglichen u.a. die Entwicklung von personalisierten Inhalten und den Zugriff auf externe Datenquellen. Für die Ausführung der JSP-Seiten und Servlets kann auf das Open Source Produkt „Tomcat“[1] zurückgegriffen werden. Das Tomcat-Projekt wurde im Kontext der Apache Software Foundation (ASF) entwickelt. Tomcat bietet eine skalierbare Ausführungsumgebung für JSP-Seiten und Java-Servlets und stellt somit für Anwendungen, die keine komplexe Geschäftslogik beinhalten, eine sehr gute Alternative zu ASP-Lösungen dar. Die Tomcat-Version 4.x unterstützt die Servlet 2.3 und die JSP 1.2 Spezifikation.

Für komplexe Anwendungsszenarien, die erweiterte Funktionalitäten benötigen, kann auf die Standards der Java 2 Enterprise Edition zurückgriffen werden. Mittels so genannter Enterprise Java Beans (EJB) besteht die Möglichkeit, Anwendungen für komplexe Geschäftsvorgänge und –regeln zu realisieren, die gleichzeitig den Zugriff auf externe Systeme benötigen. Die J2EE Umgebung benötigt einen Applikations-Server, der die Ausführung der EJB übernimmt. Der Applikations-Server muss befähigt sein, das Session-Management für die Benutzer zu gewährleisten, entsprechende Schnittstellen zu externen Anwendungen bieten und die notwendige Hochverfügbarkeit (Cluster, Load-Balancing, Failover) gewährleisteten. Neben den bekannten kommerziellen Produkten wie z.B. IBM Websphere, BEA Weblogic, Oracle Application Server und einigen anderen besteht auch die Möglichkeit, ein Open Source Produkt einzusetzen. Das Projekt „JBoss“[2] bietet einen vollständigen Java-Applikations-Server auf Open Source Basis an. Der Applikations-Server unterstützt die J2EE-Spezifikation, bietet einen integrierten Webserver, einen JSP und Servlet-Engine, Unterstützung von Enterprise Java Beans, ferner Clustering und zahlreiche weitere Funktionalitäten.

Eine detaillierte Beschreibung der Migrationsprozeduren von ASP-Applikationen auf Java-basierte Technologien bieten beispielsweise auch die Unternehmen SUN[3] und Oracle[4] an, so dass an dieser Stelle darauf verzichtet wird.

---

1 http://jakarta.apache.org/tomcat/index.html

2 http://www.jboss.org

3 http://developer.iplanet.com/docs/migration/webserver/IIS_50.pdf

4 http://otn.oracle.com/tech/migration/asp/content.html

3.10.5 Fortführende Migration

3.10.5.1 Internet Information Server 5.0

Neuerungen

Der Internet Information Server ist integraler Bestandteil des Windows 2000 Servers. Die Nachfolger-Version der Internet Information Server 4.0 verfügt über eine Reihe von neuen Funktionalitäten, die wichtigsten Neuerungen werden in der folgenden Tabelle aufgeführt.

Tab. 24: Erweiterte Funktionalitäten der Internet Information Server 5.0

Funktion	Beschreibung
Datenbereitstellung	
WebDAV	Unterstützung des WebDAV-Standards zum gemeinsamen Bearbeiten von Dateien und Verzeichnissen direkt über HTTP auf dem Webserver.
Web-Verzeichnisse	Unterstützung von Web-Verzeichnissen, dienen den Nutzern als herkömmliche Dateiverzeichnisse auf dem Web-Server und stehen unmittelbar im Zusammenhang mit der WebDAV-Funktionalität.
Frontpage Unterstützung	Erlaubt die Entwicklung und Verwaltung von Webinhalten mittels Microsoft Frontpage. Mittels des graphischen Frontend kann der Administrator Web-Inhalte auf den Web-Server erstellen und verändern.
Unterstützung von multiplen Web-Sites	Erlaubt das Hosting von verschieden Web-Sites auf einem Server und einer IP-Adresse.
HTTP 1.1-Kompression	Ermöglicht die HTTP-Kompression bei der Kommunikation zwischen dem Web-Server und kompressionsfähigen Client-System, insbesondere bei eingeschränkten Bandbreiten sinnvoll.
PICS Rating	„Platform for Internet Content Selection“[1]-Rating ist ein technischer Standard zum Einsatz eines Bewertungssystems von Webinhalten des W3-Konsortiums. Mit PICS verbindet sich die inhaltliche Bewertung und die Möglichkeit der Filterung von Webseiten nach bestimmten Merkmalen. Dazu wird im HTML-Header eines Dokuments ein PICS-Code eingefügt, der im Browser nicht sichtbar ist.
Webbasierte Applikationen	
XML-Integration	Ein XML-Parser in Windows 2000 ist als COM-Komponente implementiert und stellt eine vollständige XML-Basis für Anwendungen zur Verfügung.
Windows Skript Komponenten	Entwickler können mittels der Skripting-Technologie wiederverwendbare COM Module für Webanwendungen entwickeln
Bestimmung der Browser-Eigenschaften	Mittels ASP können die genauen Browser-Eigenschaften der Client-Systeme ermittelt werden
Prozess-Trennung	Der Administrator kann einzelne Applikations-Prozesse von den Kern-Prozessen und anderen Anwendungs-Prozessen isolieren.

[1] http://www.w3.org/PICS/

Funktion	Beschreibung
ADSI 2.0	Erlaubt den Zugriff auf die Objekte, Eigenschaften und Methoden des Active Directory Service Interface. Die Integration des Web-Servers und des Active Directory ermöglicht die Zuweisung von unterschiedlichen Web-Sites auf einen Web-Server zu bestimmten Nutzer-Domänen.
Verwaltung	
Management Delegation	Erlaubt die Übertragung von Verwaltungsaufgaben.
Prozess Throttling	Ermöglich die Begrenzung der CPU-Zeit für eine Netzanwendung oder Seite. Damit kann sichergestellt werden, dass Prozessorzeit für andere Websites oder für Nicht-Netzanwendungen verfügbar ist.
DFS	Distributed File System, ist ein Dateisystem, bei dem Dateien transparent über mehrere Computer hinweg verteilt werden können. Dieses kann für die Dokumenten-Root, dem Ort an dem die Web-Inhalte im Dateisystem abgelegt werden, verwendet werden.
Authentifikation und Sicherheit	
Kerberos	Die Nutzer-Authentifikation kann mittels Kerberos erfolgen, die alte Windows-Anmeldung mittels des Windows LAN Manager (NTLM) ist aber immer noch möglich.
Verschlüsselung	Anwendung von SSL 3.0 und TLS (Transport Layer Security) zur verschlüsselten Datenübertragung
Digest Authentication	Ermöglicht die verschlüsselte Passwortübertragung für die Authentifizierung.
IP- und Domänen-Beschränkungen	Der Administrator erhält die Möglichkeit, den Zugriff auf Inhalte für Computer und Domänen zu erlauben bzw. zu verbieten.
Zertifikate	Unterstützung von Client- und Serverzertifikaten.

3.10.5.2 Internet Information Server 6.0

Zum Lieferumfang des Windows Server 2003 gehört der Internet Information Server 6.0 (IIS 6.0), der erstmalig in der Standardinstallation vollständig gesperrt und nicht automatisch im System integriert ist. Der Administrator muss den Installationsvorgang explizit initialisieren und bestimmte Server-Funktionalitäten aktivieren.

Aus der Kombination der folgenden Technologien aus der Windows 2003 Server Produktgruppe

- Internet Information Server 6.0
- ASP.NET
- ASP
- COM+
- Microsoft Message Queuing (MSMQ)

sollen zukünftig die Möglichkeiten eines Applikationsservers angeboten werden.

Für diese neue Rolle des Internet Information Server wurden einige Neuerungen implementiert, die im Folgenden kurz skizziert werden.

Für Verbesserungen in Hinblick auf Zuverlässigkeit und Skalierbarkeit wurden innerhalb der Verarbeitungsarchitektur Änderungen vorgenommen. So können Fehler automatisch erkannt und im Bedarfsfall Prozesse neu gestartet werden. Parallel kann der Web-Server eingehende Anforderungen in einer Warteschlange aufnehmen. Der IIS 6.0 ist in der Lage, die Statusüberwachung von Arbeitsprozessen, Anwendungen und Websites durchzuführen. Mit dem Windows 2003 Server wurde auch ein neuer Kernelmodustreiber eingeführt, dieser soll den Datendurchsatz des Web-Servers optimieren.

Der IIS 6.0 kann in das Autorisierungsframework der Windows 2003 Servers mit eingebunden werden, zusätzlich kann mit dem Autorisierungs-Manager eine Delegierungs- und Autorisierungsaktionen vorgenommen werden. Die Verwaltung des IIS 6.0 erfolgt nun auf XML-Metabasis und ermöglicht den Administratoren direktes Bearbeiten der Konfiguration.

Neu ist auch die Integration von ASP.NET und IIS, den Entwicklern werden erweiterte Funktionalitäten des .NET Framework zur Erstellung von Anwendungen angeboten. Für Entwickler und Anwender können zur Internationalisierung Unicode-Standard genutzt werden.

3.11 Datenbanken

3.11.1 Überblick

Die technischen Betrachtungen zur Datenbank-Migration zeigen auf, dass neben dem weiterführenden Microsoft-Produkt MS SQL Server 2000 durchaus adäquate OSS-Lösungen als Alternativen zur Verfügung stehen und eine ablösende Migration rechtfertigen. Wichtige Vertreter solcher OSS-Lösungen sind MySQL, PostgreSQL, Firebird und MaxDB. Daneben stehen aber auch noch kommerzielle Produkte wie Oracle und DB2 zur Verfügung, die auch bei Behörden schon vielfach im Einsatz sind und hier nicht in die technischen Betrachtungen einbezogen wurden.

Die aufgeführten OSS-Lösungen bieten unterschiedliche Funktionalitäten und ihre Eignung muss daher im Einzelfall bezüglich der jeweiligen Anforderungen geprüft werden.

Hervorzuheben ist, dass die benannten OSS-Lösungen allesamt plattformunabhängig sind und es auch installationsfertige Windows-Versionen gibt, die im Internet als Download erhältlich sind. Damit können diese Datenbanksysteme auch bei einer punktuellen Migration eingesetzt werden.

3.11.2 Einleitung

Für die Pflege, Verwaltung und Speicherung großer Datenmengen werden Datenbank-Systeme eingesetzt. Datenbank-Systeme speichern zusammengehörige Datenelemente in einer Form bzw. in gruppierten Datensätzen, zwischen den

Strukturen und Gruppierungen können definierte Beziehungen bestehen. Durch den Einsatz einer gut geplanten und strukturierten Datenbank können redundante Datenelemente vermieden werden.

Daten aus einem Datenbank-System werden in der Regel den Benutzern nicht direkt zur Verfügung gestellt. Der Zugriff erfolgt über eine Anwendung, diese greift auf die Daten zu und bietet sie den Benutzern in entsprechender Form dar. Somit muss gewährleistet sein, dass entsprechende Schnittstellen zwischen dem Datenbank-System und der Applikation bestehen. Eine entsprechende Kommunikationskomponente gewährleistet die Verbindung zwischen den Client- und Server-Systemen. Anwendungen, die auf den Client-Systemen ausgeführt werden, können über das Netzwerk auf den Datenbankserver zugreifen. Die Datenbank-Server müssen in der Lage sein, eine größere Zahl paralleler Client-Zugriffe zu bewältigen. Die Aufgabe des Servers besteht dann in der Vermeidung von logischen Problemen bei parallelen Lese- und Schreibzugriffen durch die Client-Systeme.

Datenbanken setzen sich in der Regel aus zwei Komponenten zusammen, der eigentlichen physikalischen Datenbank und dem Datenbankmanagementsystem (DBMS). Das Datenbankmanagementsystem erfüllt u. a. die folgenden Aufgaben:

- Überwachung der Datenbeziehungen innerhalb der Datenbank.
- Überprüfung und Sicherstellung der korrekten Datenspeicherung, unter besonderer den definierten Beziehungsregeln zwischen den Daten.
- Wiederherstellung von konsistenten Daten bei einem Systemfehler oder ähnlichen Ereignissen.

Das DBMS definiert auch die Befehle und Anwendungen, die verwendet werden müssen, um mit den Daten in der Datenbank zu arbeiten. Die gebräuchlichste Sprache ist die Structured Query Language (SQL) für Datenbanksysteme.

3.11.3 MS SQL Server 7.0

Der Microsoft SQL Server ist eine SQL-basierte, relationale Client-Server-Datenbank. Das Datenbank-System besteht aus dem eigentlichen Speicherort für die Daten und dem Datenbankmanagementsystem (DBMS).

3.11.3.1 Serverarchitektur

Der Server ist die Komponente des MS SQL Servers, die SQL-Anweisungen von den Clients entgegen nimmt und die entsprechenden Aktionen ausführt.

Die SQL-Anweisungen werden von den jeweiligen Client-Systemen mittels eines Protokolls auf Anwendungsebene gesendet, diese ist spezifisch für den MS SQL Server und wird als Tabular Data Stream (TDS) bezeichnet. Unterstützt werden die Versionen 4.2 und 7.0. Die jeweiligen Pakete werden von dem OLE DB-Provider und dem ODBC-Treiber für den MS SQL Server erstellt. Die TDS-Pakete werden mittels des eingesetzten Netzwerkprotokolls an den Server bzw. in umgekehrter Richtung an den Client versendet. Der Open Data Service auf

dem MS SQL Server verwaltet die Datenpakete und ruft die entsprechende Funktion im MS SQL-Server auf.

Bild 33: Serverarchitektur des MS SQL Servers

Der eigentliche Datenbankserver besteht aus zwei Hauptkomponenten, dem relationalen Modul und dem Speichermodul. Die beiden Module kommunizieren über OLE DB-API.

Die Funktionen des relationalen Moduls bestehen in der Analyse der SQL-Anweisungen, der Optimierung des Ausführungsplans und der Ausführung der Operationen aus dem Ausführungsplan.

Das Speichermodul hat u. a. folgende Aufgaben:

- Datei- und Speicherplatzverwaltung,
- Verwaltung des Datenpuffers und der E/A Operationen
- Verwalten von Transaktionen und Verwenden von Sperren
- Protokollierung und Wiederherstellung
- Implementierung der Dienstfunktionen (BACKUP, RESTORE, DBCC und Massenkopieren).

3.11.3.2 Datenbankarchitektur

Die Strukturierung der Daten in einer Datenbank erfolgt innerhalb von logischen Komponenten, diese wiederum werden in Form von Dateien physisch auf dem Datenträger gespeichert. Bei der Arbeit mit der Datenbank wird der Benutzer in erster Linie die logischen Komponenten (Tabellen, Views, Stored Procedures, usw.) verwenden.

Jede MS SQL Server-Installation verfügt über mehrere Datenbanken, insgesamt gibt es vier System-Datenbanken und ein oder mehrere Benutzerdatenbanken.

Neben den System-Datenbanken sind nach der Installation die eigentlichen Inhalts-Datenbanken anzulegen. Diese Produktiv-Datenbanken sind in Form von unterschiedlichen Objekten organisiert. In der folgenden Tabelle werden die wichtigsten, im MS SQL Server als Objekte vorhandene Komponenten aufgeführt.

Tab. 25: Als Objekte vorhandene Komponenten im MS SQL-Server

Komponenten	Erläuterung
Tabellen	Die eigentlichen Daten der Datenbank sind innerhalb der Tabellen gespeichert. Die Tabellen bestehen aus Spalten und Zeilen, die Zeilen enthalten die jeweiligen Datensätze. Für die Spalten lassen sich Datentypen festlegen, diese definieren die Art der Daten, die in den Spalten aufgenommen werden.
Benutzerdefinierte Datentypen	Neben den Basisdatentypen des MS SQL Servers können die Benutzer benutzerdefinierte Datentypen anlegen.
Views	Views sind definierte Sichten auf eine virtuelle Tabelle oder gespeicherte Abfrage. In der Datenbank sind SELECT-Anweisungen gespeichert, dessen Resultset den Inhalt der virtuellen Tabelle bildet. Views erfüllen folgende Funktionen: ● Zugriffsbeschränkungen für Benutzer auf bestimmte Zeilen oder Spalten in der Tabelle ● Verknüpfte Darstellung von Spalten aus mehreren Tabellen ● Zusammenfassung von Informationen
Stored Procedures	Sind eine Gruppe von Transact-SQL-Anweisungen, die zu einem einzigen Ausführungsplan kompiliert wurde. Stored Procedures erfüllen u.a. folgende Funktionen: ● Implementierung von programmübergreifender Programmlogik, für die Ausführung von häufig anfallenden Aufgaben. ● Leistungssteigerung, die Stored Procedures werden kompiliert im Cache gehalten ● Der benutzerseitige Zugriff auf die Tabellen kann verhindert werden.
Einschränkungen	Stellen ein Verfahren zur Integritätssicherung der Datenbank zur Verfügung. Einschränkungen definieren die Regeln bezüglich der zugelassen Werte innerhalb der Spalten.
Regeln	Gewährleisten die Abwärtskompatibilität, sie erfüllen z.T. dieselben Funktionen wie die CHECK-Einschränkungen. Dienen zur Beschränkung der Werte in einer Spalte.
Standardwerte	Geben die Werte an, die in der Spalte verwendet werden, wenn beim Einfügen eines Datensatzes kein Wert in der Spalte angegeben wurde.
Trigger	Entsprechen einer besonderen Form von Stored Procedures, sie werden automatisch ausgeführt sobald eine UPDATE-, INSERT- oder DELETE-Anweisung für eine Tabelle gemacht wurde.
Tabellenindizes	Ein Index der mit einer Tabelle verknüpft ist und das Abrufen von Zeilen beschleunigt.

3.11.3.3 Client-Komponenten

Der Zugriff auf den Microsoft SQL Server erfolgt nicht direkt durch den Benutzer. Um auf die Daten zugreifen zu können, werden spezielle Applikationen eingesetzt. Für den Zugriff können

- Dienstprogramme der MS SQL Servers,
- Programme von Drittanbietern,
- und behördeninterne Eigenentwicklungen

verwendet werden. Der Zugriff auf den MS SQL Server erfolgt über die Datenbank-API (Application Programming Interface). Diese setzt sich aus zwei Teilen zusammen: Den Sprachanweisungen, die an die Datenbank übergebenen werden und einem Satz von Funktionen oder objektorientierten Schnittstellen und Methoden, diese senden die Sprachanweisungen an die Datenbank und verarbeiten die Ergebnisse. Als Sprachanweisungen verwendet der MS SQL Server **Transact-SQL**, unterstützt werden alle Anweisungen des Entry Levels von SQL-92 und weitere SQL-92 Features (aus dem Intermediate und Full Level), darüber hinaus gibt es noch Microsoft-spezifische Transact-SQL-Erweiterungen.

Der MS SQL Server unterstützt zwei Hauptklassen von Datenbank-APIs:

- OLE DB – Der systemeigene Provider unterstützt Anwendungen, die mit Hilfe von OLE DB geschrieben wurden oder APIs, die OLE DB verwenden (z. B. ActiveX Data Objects (ADO)). Außerdem werden Objekte und Komponenten, die OLE DB verwenden, unterstützt (z.B. ActiveX und Windows DAN-Anwendungen).
- ODBC – Der Treiber unterstützt Anwendungen und Komponenten, die mit Hilfe von ODBC geschrieben wurden.

Zusätzlich unterstützt der MS SQL Server die DB-Library und Embedded SQL.

3.11.3.4 Kommunikationskomponenten

Es werden mehrere Methoden zur Kommunikation zwischen den Clientanwendungen und dem Server unterstützt. Bei der Kommunikation auf einem Computer zwischen Server und Anwendung werden prozessübergreifende Technologien, zum Beispiel Named Pipes oder Shared Memory, verwendet. Anwendungen, die auf einem anderen Client-System betrieben werden, verwenden die Netzwerk-Interprocess Communication (IPC). Die IPC basiert auf der API und den Netzwerkprotokollen. Folgende Protokolle stehen zur Verfügung:

- TCP/ IP
- Novell IPX/ SPX
- Apple Talk
- Banyan VINES.

3.11.3.5 Skalierbarkeit

Der Microsoft SQL Server ist für die Verwaltung von Datenbanken ausgelegt, die einen Umfang von einem Terabyte oder mehr haben können. Der MS SQL Server verfügt über einige Features, die der Effizienzsteigerung des Datenbank-Systems dienen.

Der MS SQL Server maximiert das Ausmaß des parallelen Zugriffs auf Daten, indem für jede Abfrage eine geeignete Sperrstufe ausgewählt wird. Die Zugriffe werden durch dynamische Sperrvorgänge auf der Zeilen- bzw. Tabellenebene optimiert.

Durch das Datenbanksystem werden auch VLDB-Umgebungen (Very Large Database) unterstützt, die Größe der Datenbanken kann ein Terabyte oder mehr betragen. Für die Transact-SQL-Anweisungen BACKUP und RESTORE ist es möglich, dass sie parallel auf mehrere Sicherungsmedien schreiben und auch inkrementelle Sicherungen erzeugen können.

Zur Beschleunigung der Abfragebearbeitungen ist ein Abfrageoptimierer in den MS SQL Server integriert. Für die Unterstützung von Multiprozessor-Maschinen können parallele Ausführungspläne erstellt werden, um die SQL-Anweisungen aufzuteilen.

Der MS SQL-Server unterstützt verteilte Abfragen, es können Transact-SQL-Anweisungen ausgeführt werden, die auf heterogene OLE DB-Datenquellen verweisen.

Die Datenintegrität wird bei der Durchführung von Aktualisierungen (Änderungen) dadurch sichergestellt, dass Aktualisierungen immer in einem konsistenten Status enden. Wird dieser nicht erreicht, so erfolgt ein Rollback zurück zum Ausgangspunkt, d.h. bis zum letzten konsistenten Status.

Ferner besteht die Möglichkeit der verteilten Transaktionen, dabei werden die Transaktionen von einem Transaktions-Manager verwaltet.

3.11.3.6 Zugriffssteuerung

Der MS SQL Server bietet zwei Arten der Benutzer-Authentifizierung an:

- SQL Server-Authentifizierung
  Im MS SQL-Server müssen entsprechende Anmeldekonten und Kennwörter vorhanden sein – diese haben keinen Zusammenhang mit den NT-Nutzerkonten. Die Anmeldung und Passwortabfrage erfolgt direkt am MS SQL Server.
- Windows NT-Authentifizierung
  Hier müssen die Windows NT-Konten und Gruppen im MS SQL Server aufgenommen werden, die eigentliche Authentifizierung erfolgt aber an der NT-Domäne.

Der Administrator kann festlegen, ob die Authentifizierung über Windows NT oder im gemischten Modus erfolgen soll.

3.11.3.7 Systemintegration

Der MS SQL Server unterstützt die Verwendung der Windows NT-Benutzer und Domänenkonten, somit steht für den MS SQL Server die Windows-NT-Authentifizierung zur Verfügung. Die Benutzer werden nicht von dem MS SQL Server authentifiziert, der Server stellt den Client-Systemen eine vertraute Verbindung zur Verfügung.

Neben der Integration in die NT-Benutzer-Authentifizierung kann der MS SQL Server eng mit folgenden Produkten verbunden werden:

- Datenspeicherdienst für den Microsoft Internet Information Server, der in der Regel für die Generierung von dynamischen Webinhalten auf ASP-Basis eingesetzt wird.
- Als Datenspeicher für den Sites Server, der für die Verwaltung von Web-Sites eingesetzt wird.

3.11.3.8 Administration

Für die Administration des MS SQL Servers werden mehrere Werkzeuge bereitgestellt.

- **MS SQL Server-Agent**
  Dieser ermöglicht das Erstellen und Planen von Aufgaben, die einmalig oder periodisch ausgeführt werden sollen. Es können Warnungen für den Administrator ausgegeben werden, wenn bestimmte Systemzustände eintreten.
- **MS SQL Server Profiler**
  Dieser erlaubt die Überwachung und Analyse der Netzwerklast bei den Übertragungen von und zu einem Server.
- **MS SQL Server-Systemmonitor** – Dieser erlaubt die Einbindung in den Windows NT-Systemmonitor, der zur Überwachung der Leistung des SQL Servers und der graphischen Darstellung dient.
- **MS SQL Server Enterprise Manager**
  Dieser stellt einen Snap-In für die Microsoft Management Console (MMC) für die Verwaltung des MS SQL Servers zur Verfügung.
- **Indexoptimierungs-Assistent**
  Dieser erlaubt die Analyse über die Verwendung der Indizes von SQL-Anweisungen.

Zusätzlich ist es möglich, mittels der SQL Distributed Management Objects (SQL-DMO) innerhalb von Anwendungen Automatisierungsaufgaben einzubinden. Wiederkehrende Aufgaben können auch als Aufträge implementiert werden.

3.11.4 Ablösende Migration

Datenbanken, oder genauer Relationale Datenbank-Management-Systeme (RDBMS) gehören zu den Wegbereitern für den Einsatz von Linux in unterneh-

menskritischen Anwendungsbereichen. Die Software AG hat mit AdabasD bereits 1997 ein vollkommerzielles (seinerzeit SAP-zertifiziertes) RDBMS für Linux angeboten. Oracle und Informix folgten 1998 und haben damit die Kredibilität von Linux im professionellen Umfeld deutlich gesteigert. Die unter dem Acronym LAMP bekannte Kombination von Linux, Apache, MySQL und PHP ist seit Beginn der kommerziellen Internetnutzung eine der beliebtesten Infrastrukturen für Webshops und dynamische Webseiten. Mit PostgreSQL, Firebird, MaxDB (früher SAPDB) und Ingres stehen eine ganze Reihe von vollwertigen RDMBS mit Transaktionsunterstützung, Triggern und Stored Procedures auch unter Open Source Lizenzen zur Verfügung. An hochwertigen Optionen für den Einsatz von Linux und Open Source Software im Bereich der Datenbanksysteme mangelt es sicher nicht.

Im Rahmen einer Migrationsstrategie spielen RDBMS insofern eine besondere Rolle, als sie immer mit mindestens einer Anwendung verbunden sind. Idealerweise liegen die Daten einer Organisation in nur einem Datenbanksystem in normalisierter Form (ohne Redundanz) vor. Idealerweise ist die Abfragesprache (SQL), mit der die Anwendungen auf der Datenbank arbeiten, standardisiert und jede Anwendung sollte mit jedem RDBMS problemlos zusammenarbeiten. In der Realität finden sich in den meisten IT-Infrastrukturen mehrere RDBMS, in denen teilweise die gleichen Daten mehrfach verwaltet werden und die von verschiedenen Anwendungen mit unterschiedlichen SQL-Dialekten und herstellerspezifischen Spracherweiterungen und über herstellerspezifische Schnittstellen abgefragt werden. Eine Migration bietet vor diesem Hintergrund die Chance, eine Konsolidierung der Software- und Datenstrukturen durchzuführen. Gleichzeitig müssen bei einer Migration neben dem Datenbestand auch die Anwendungen umgestellt werden, was in vielen Fällen nicht ohne Eingriff in die Client-Software möglich ist. Selbst wenn die Datenbankanbindung mittels ODBC oder JDBC standardisiert ist und keine Trigger oder Stored Procedures verwendet werden, muss bei einer Datenbankmigration clientseitig der ODBC/JDBC-Treiber ausgetauscht werden. Die Zentralisierung und Konsolidierung des Datenbestandes ist also offensichtlich nicht einfach zu haben, andererseits ist sie ein sehr attraktives Ziel, weil dadurch im laufenden Betrieb erhebliche Pflegeaufwände und damit Kosten reduziert werden können.

Diese Vorüberlegung zeigt, dass eine Alternative zur fortführenden Migration nur in folgenden Fällen in Frage kommt:

- Das derzeit unter Windows laufende RDBMS ist auch für ein Open Source Betriebssystem erhältlich (z.B. Oracle auf Linux). In diesem Fall bleibt das Datenbanksystem als kommerzielle Software erhalten. In einer linux-basierten Serverinfrastruktur ergeben sich aus Administrationssicht auch in dieser Variante durchaus Vorteile. Für MS-SQL wird es aber voraussichtlich keine Linux-Version geben.
- Die Anwendungen sind mit ODBC oder JDBC an das bisherige RDBMS angebunden. In diesem Fall können die Daten in ein anderes Datenbank-

system übernommen und die Clientanbindung durch Austausch des ODBC-Treibers (auf Systemebene auf dem Client) auf das neue RDBMS umgelenkt werden. Hier steckt der Teufel im Detail. Wenn die Anwendung mit Stored Procedures oder Triggern arbeitet, müssen auch diese portiert werden. (Auch das kann gelegentlich ohne Änderungen an der Clientsoftware durchgeführt werden.)

- Es handelt sich um eine Access-Anwendung mit dateibasierter Datenhaltung. Hier können die Daten sehr leicht in ein zentrales RDBMS übernommen und die Access-Anwendung auf die ODBC-Schnittstelle umgestellt werden.
- Der Client liegt im Quelltext vor und kann im Rahmen eines Migrationsprojektes an das neue RDBMS angepasst werden. Der Migrationsaufwand hängt hier neben den schon genannten Faktoren (Verwendung von Triggern und Stored Procedures) auch von der verwendeten Programmierschnittstelle ab. Wenn die Datenbankanbindung direkt über eine Schnittstelle des Herstellers implementiert wurde (z.B. embedded SQL), muss mit erheblich mehr Aufwand gerechnet werden, als wenn eine Abstraktionsebene wie ActiveX Data Objects (ADO) dazwischen geschaltet wurde.
- Schließlich gibt es noch die Möglichkeit, mit dem Hersteller einer Anwendung zusammenzuarbeiten und auf diesem Wege eine Datenbankmigration zu erreichen. Die feste Bindung an ein bestimmtes RDBMS wird auch von vielen Anbietern kommerzieller Datenbankanwendungen als Marktnachteil gesehen, so dass von einer nennenswerten und wachsenden Bereitschaft zu einer Migration insbesondere zu einem Open Source RDBMS ausgegangen werden kann.

Wenn die grundsätzliche Möglichkeit für eine Datenbankmigration gegeben ist, muss ein geeignetes RDBMS als Zielsystem ausgewählt werden. Bei der Betrachtung möglicher Zielsysteme konzentrieren wir uns in diesem Migrationsleitfaden auf Open Source Datenbanken. Die folgende Übersicht zeigt die aktuell unter Open Source Lizenz verfügbaren Datenbanksysteme.

Tab. 26: unter Open Source Lizenz verfügbare Datenbanksysteme

Datenbank	Version	Lizenz	Abfrage	Transactions	Stored Procs
GDBM www.gnu.org	1.8.3	GPL	Hash		
Berkeley DB www.sleepycat.com	4.3	BSD Type	Hash	X	
SHORE www.cs.wisc.edu/shore/	1.1.1	BSD	SDL/ODL		
ZOPE www.zope.org	2.7.3	Zope PL	DTML		
mSQL www.hughes.com.au	3.6	Hughes	MSQL		

Datenbank	Ver-sion	Lizenz	Abfra-ge	Trans-actions	Stored Procs
MySQL www.mysql.com	4.1.	GPL	SQL	X	
PostgreSQL www.postgresql.org	7.4.6	BSD	SQL	X	(X)
Firebird firebird.sourceforge.net	1.5	InterBase PL	SQL	X	X
MAXDB www.mysql.com	7.5	GPL/ LGPL	SQL	X	X
Ingres open-source.ca.com/projects/ingres/	r3	CATOSL	SQL	X	X

Die Hash-Systeme sind nicht relational organisiert. Für eine Migration kommen in erster Linie die letzten vier Systeme mit SQL-Schnittstelle in Frage. Im folgenden werden diese vier Systeme charakterisiert.

3.11.4.1 MySQL

MySQL wird von der gleichnamigen schwedischen Firma entwickelt und vertrieben. Die Datenbank steht unter GPL und ist damit Freie Software ohne Einschränkung. Da auch die Programmierschnittstellen unter GPL stehen, müssen die damit gelinkten Programme ebenfalls unter GPL stehen, sobald sie verbreitet bzw. kommerziell vermarktet werden. Alternativ bietet MySQL AB auch kommerzielle Lizenzen an, die es Anbietern kommerzieller Anwendungen ermöglichen, MySQL zu verwenden, ohne ihre eigene Software unter GPL stellen zu müssen. MySQL bietet reguläre Support- und Wartungsverträge, Schulungen sowie Beratung an.

Die Hersteller schätzen die Zahl der Datenbankinstallationen weltweit auf 4 Millionen. Die größte Beliebtheit hat MySQL zusammen mit Linux, Apache und PHP für die Erzeugung dynamischer Webseiten.

MySQL kann mit dem gleichen Frontend (SQL-Parser) auf verschiedenen Backends zur Datenablage arbeiten. Mit InnoDB als Backend besitzt MySQL auch Transaktionsunterstützung. Stored Procedures und Views bietet MySQL zurzeit nicht.

Die Datenablage findet bei MySQL typischerweise im Dateisystem statt. Die Datenstrukturen belegen dabei nur so viel Plattenplatz, wie für die Speicherung des Inhalts tatsächlich erforderlich ist. Eine Allozierung von Plattenplatz für eine Tabelle oder Datenbank ist nicht nötig. Ein einziger laufender Datenbankserver kann beliebig viele Datenbankinstanzen verwalten.

MySQL ist insgesamt sehr schlank und bei allen Lesezugriffen außerordentlich schnell. Sie wird typischerweise eher für kleine und mittlere Datenbestände und für leichte Anwendungen eingesetzt. Allerdings zeigt die Referenzliste von MySQL AB, dass die Datenbank auch für große Anwendungen und Datenbe-

stände geeignet ist und sich durchaus mit allen vollkommerziellen Datenbanksystemen messen kann.

3.11.4.2 PostgreSQL

PostgreSQL hat einen universitären Ursprung und ist aus dem 1986 entwickelten Postgres Datenbank-System entstanden. Seit 1995 unterstützt Postgres SQl als Abfragesprache und seit 1996 gibt es die Software unter dem Namen PostgreSQL. PostgreSQL ist ein reines OSS-Projekt und wird von einer großen internationalen Entwicklergemeinde vorangetrieben. Die Nutzung von PostgreSQL unterliegen der BSD-Lizenz[1]. Zwischenzeitlich liegt das OSS-Datenbanksystem in der Version 8.0 vor.

http://www.postgres.de/info.whtml

Einige der wichtigsten Funktionen die von PostgreSQL unterstützt werden[2], sind nachfolgend kurz aufgeführt:

- Unterstützt werden der ANSI-SQL-Standard SQL92 und aus dem SQL99-Standard die 3 Kategorien Framework, Foundation und Host Language.
- Tabellen können mit der Definition von Primär- und Fremdschlüsseln referenziert werden.
- Sprachkonstrukte wie Outer Joins, Views und Mengenoperationen auf eine oder mehrere Tabellen werden genauso unterstützt wie Transaktionskontrolle und Stored Procedures.
- PostgreSQL stellt u.a. folgende Schnittstellen zur Verfügung:
  - ODBC
  - JDBC
  - C
  - C++
  - PHP
- Ins Tabellen können Binärdateien (Large Objects), wie z.B. Bilder gespeichert werden.
- Die Datenkommunikation zwischen Server und Client kann mit SSL verschlüsselt werden. Zusätzlich unterstützt PostgreSQL Kerberos-Authentifizierung.

Eine weitgehend vollständige Liste der Fähigkeiten findet man auf den deutschen Internetseiten von PostgreSQL unter http://www.postgres.de/features.html.

---

1 http://www.opensource.org/licenses/bsd-license.php

2 Quelle: http://www.postgres.de/info.whtml

Konzeptuell bietet PostgreSQL einige Besonderheiten, indem es anstelle von Prozeduren benutzerdefinierte Funktionen und ein über die Funktionalität von Triggern hinausreichendes Regelkonzept anbietet.

Die Datenhaltung von PostgreSQL findet im Dateisystem statt. Eine Allozierung von Datenbank- oder Tabellenplatz ist nicht erforderlich. Ein Datenbankserver kann mehrere Datenbankinstanzen bedienen. Die Datenbank kann im laufenden Betrieb gesichert werden.

PostgreSQL wird typischerweise für mittelgroße Datenbestände eingesetzt. Über ein Windows-basiertes Administrationstool lässt sich ein Migration-Wizard für Access Datenbanken einbinden, mit dem die Übernahme von Daten aus Access weitestgehend automatisiert werden kann.

3.11.4.3 Firebird

Firebird ist Mitte 2000 als eigenständiges Projekt aus der von Borland in die Open Source entlassenen Interbase Datenbank Version 6.0 entstanden. Eine kleine engagierte Community arbeitet an der Fortentwicklung des Datenbanksystems. Als Dokumentation stehen im Wesentlichen die von Interbase übernommenen PDF Dateien zur Verfügung. An einer Aktualisierung wird gearbeitet. Mit der Fortentwicklung fallen auch einige Schnittstellen weg, die nur für Interbase vorhanden sind.

Als RDBMS für den professionellen Einsatz kommt Firebird heute noch nicht wirklich in Frage.

3.11.4.4 MaxDB

Die MaxDB ist als universitäres Forschungsprojekt an der Technischen Universität Berlin gestartet. Hier reichen die Anfänge sogar auf das Jahr 1977 zurück. Das System wurde in den 80ern von Nixdorf als DDB/4 weiterentwickelt und vermarktet, kam dann über Siemens/Nixdorf als Adabas D zur Software AG und wurde 1997 von der SAP gekauft. Im Jahr 2000 wurde die SAPDB unter GPL gestellt, ohne dass jedoch die Investition der SAP in deren Weiterentwicklung reduziert wurde. 2004 wurde die SAPDB schließlich in das Produktportfolio von MySQL AB eingegliedert und in MaxDB umbenannt. Die MaxDB wird nach wie vor von der SAP als zertifizierte Plattform für das R/3-System und dessen Nachfolger angeboten und als Kerntechnologie in eigenen Produkten eingesetzt. Zum Funktionsumfang gehören neben einer Transaktionsunterstützung auch Trigger und Stored Procedures.

Die SAP ist weiterhin bestimmend an der Fortentwicklung der MaxDB beteiligt. Ein wesentlicher Augenmerk der Fortentwicklung wie auch der Qualitätssicherung liegt naheliegenderweise auf der im Zusammenhang mit R/3 erforderlichen Funktionalität. Da R/3 als Applikationsserver die gesamte Geschäftslogik beinhaltet, wird das Datenbanksystem hier hauptsächlich zur performanten Lieferung und Sicherung von relationalen Daten genutzt. Stored Procedures spielen in die-

sem Umfeld keine Rolle. Entsprechend fehlt es der MaxDB in dieser Hinsicht an Vielseitigkeit und Flexibilität.

Für die Datenhaltung benutzt die MaxDB Devspaces, die im Dateisystem oder auf Raw-Devices angelegt und die jeweils komplett zu einer Datenbankinstanz alloziert werden. Die Datenbank ist reorganisationsfrei und kann im laufenden Betrieb gesichert werden.

Die MaxDB ist ein Schwergewicht unter den Open Source Datenbanken. Als Migrationsziel für Access-Datenbanken kommt sie nur in Ausnahmefällen in Frage.

3.11.4.5 Ingres

Seit Anfang 2004 steht mit Ingres r3 von Computer Associates (CA) ein weiteres etabliertes Datenbanksystem mit industriellem Hintergrund unter Open Source Lizenz zur Verfügung.

Datenbankprozeduren werden mit einem übersichtlichen Funktionsumfang in erster Linie für den Einsatz als Trigger im Zusammenhang mit Regeln angeboten. Bei einem zeitgemäßen Einsatz der Datenbank in einer Mehrschicht-Architektur bietet Ingres eine JDBC-Schnittstelle mit Updatefähigen Result-Sets.

3.11.4.6 Zwischenbilanz

Das Angebot an alternativen Migrationszielen im Open Source Bereich ist vielfältig und attraktiv.

Eine pauschale, einfache und eindeutige Entscheidung für das eine oder andere System lässt sich aus den charakteristischen Merkmalen nicht ableiten.

Alle fünf beschriebenen SQL Datenbanksysteme sind plattformunabhängig. Insbesondere sind für alle fünf auch installationsfertige Windows-Versionen zum Download im Internet erhältlich.

Zur Unterstützung eines detaillierteren Vergleichs der möglichen Zielsysteme einer Migration ist ein exakter Vergleich der Featurelisten in Hinblick auf die tatsächlich im Ursprungssystem genutzten Datenbankfunktionalität erforderlich.

Einen guten Überblick verschafft eine Web-Site[1] bei MySQL, auf der verschiedene Datenbanksysteme miteinander in ihren Features verglichen werden können.

Einige zusätzliche Anhaltspunkte werden in der folgenden Tabelle gegeben:

[1] http://dev.mysql.com/tech-resources/features.html

Tab. 27: Zusammenstellung SQL Datenbanksysteme

Feature	MySQL	Post-greSQL	Ingres	MaxDB
Lizenz	GPL	BSD	CATOSL	GPL
Dokumentation von Drittanbietern	X	X	X	X
TableSpace	unlimited	unlimited	unlimited	unlimited
SSL / Network Traffic Encryption		X		
Kerberos Authentication		X		
ODBC	X	X	X	X
JDBC	3.0	3.0	3.0	3.0
Perl	X	X		X
PHP	X	X		X
Python	X	X		X
.NET	C[1]	C	X	C
Gruppen/Rollenkonzept		X	X	X
Online Backup		X	X	X
Inkrementelles Backup				X
Erweiterung des DB space im laufenden Betrieb	Via LVM	Via LVM	Via LVM	X
Raw Devices	(X)			X
Namespaces		table		owner. table

3.11.4.7 Hinweise

Bei der Übernahme von Daten aus Datentypen, die im Zielsystem nicht identisch vorhanden sind, ist es in der Regel möglich, einen geeigneten Typ mit größerem Wertebereich zu identifizieren. Allerdings muss sowohl bei der Datenübernahme als auch beim Übergang zu einer ODBC Anbindung darauf geachtet werden, dass die ODBC-Schnittstelle eigene Vorstellungen und Definitionen von Datentypen besitzt.

[1] C: Kommerzielles Produkt von Drittanbietern (alternativ mit Microsoft .NET ODBC Connector odbc_net.msi)

3.11.4.8 Empfehlungen zur Unabhängigkeit

Wenn eine ablösende Migration zurzeit nicht in Frage kommt, lassen sich aus den Überlegungen und Erkenntnissen in diesem Zusammenhang einige Empfehlungen zur Datenbankprogrammierung ableiten, die eine spätere Migration erleichtern können.

- Auf Stored Procedures und herstellerspezifische Erweiterungen verzichten.
  Wenn eine Verlagerung von Geschäftslogik oder Funktionalität vom Client hin zum Server gewünscht ist, lässt sich das heute sehr gut mit 3-Schicht Architekturen erreichen. Im Sinne einer plattformunabhängigen Implementierung bietet sich hier Java sowohl für den Client als auch für den Applikationsserver (Tomcat) an.
- Die Datenbankanbindung mit standardisierten Schnittstellen vornehmen (ODBC, JDBC) oder eine Abstraktionsebene einschalten, die optional und ohne Änderungen im Programmcode auf ODBC, JDBC oder andere Schnittstellen umgestellt werden kann.
- SQL Statements im Programmcode isolieren und modularisieren.

3.11.5 Fortführende Migration

3.11.5.1 Microsoft SQL Server 2000

Mit der Version des MS SQL Server 2000 wurden insbesondere neue Webfunktionalitäten integriert. Der Schwerpunkt der Weiterentwicklung lag im Bereich der XML-Fähigkeit und der verbesserten Skalierbarkeit. In dem folgenden Abschnitt werden die wichtigsten neuen Funktionalitäten aufgeführt.

Internet und Intranet

Die wichtigsten Erweiterungen des MS SQL Server 2000 für den Bereich der Internet- und Intranetlösungen sind in der folgenden Tabelle enthalten.

Tab. 28: Erweiterte Internet- und Intranetlösungen MS SQL Server 2000[1]

Funktion	
XML	• Unterstützung von XML, XPath, XLS und HTTP: • Anzeige und Zugriff auf relationale Daten durch die Verwendung von XML-Ansichten. • URL- und HTTP-Zugriff auf Daten im Internet. Für die Generierung von Abfragen können SQL, XML-Vorlagen oder XPath in URLs eingebettet werden. • Es können SELECT-Statements in XML-Form zurückgegeben werden. • XML-Dokumente können mittels Transact-SQL und Stored Procedures bearbeitet werden.

[1] Die erweiterten Funktionalitäten der Enterprise Edition werden nicht aufgeführt und können in Whiptepapers und entsprechenden technischen Beschreibungen nachgelesen werden

Funktion	
Integriertes Datamining	Erlaubt die Analyse relationaler und OLAP-Daten („Online Analytical Processing”-Daten) für Trendanalysen und Vorhersagen.
Unterstützung von multiplen Instanzen	Hosting separater Datenbank-Instanzen für Anwendungen oder Kunden.
Sicherheit	Unterstützung von SSL-Verbindung und Kerberos.

Verwaltung und Entwicklung

In der Tabelle werden die wichtigsten Neuerungen bzgl. der Verwaltungs- und Entwicklungsoptionen des Microsoft SQL Server 2000 wiedergegeben.

Tab. 29: Verwaltungs- und Entwicklungsfunktionalitäten

Funktionen	
Active Directory Integration	Integration des zentralen MS-Verzeichnisdienstes.
Assistent zum Kopieren von Datenbanken und DTS	Verschieben und kopieren von Datenbanken und Objekten zwischen Servern. Der Data Transformation Services ermöglicht das Importieren und Exportieren von Primär- und Fremdschlüsseln zwischen unterstützten Datenbankprodukten.
Benutzerdefinierte Funktionen und neue Trigger	Erstellen von wieder verwendbaren Transact-SQL-Funktionen. Erweiterte Trigger für Codeausführungen anstelle oder nach einem Vorgang.
Datentypen, Indizes und Sortierungen	Neue Datentypen (bigint, sql_variant, table) können verwendet werden und es können Indizes in Spaltentypen definiert werden, wenn die Daten in den Spalten von anderen Spalten berechnet werden. Auf Spaltenebene wird eine Sortierung ermöglicht, das ermöglicht die Speicherung von Objekten, die unterschiedliche Sortierungen in derselben Datenbank aufweisen.
Analysis Services virtuelle Cubes und der MDX-Generator	Der Analysis Services ermöglicht das Entwickeln von OLAP-, Datawarehousing- und Datamining-Lösungen. Der Editor für virtuelle Cubes ermöglicht deren Bearbeitung. Mittels des MDX-Generator können multidimensionale Ausdrücke erstellt werden.

3.12 Groupware

3.12.1 Überblick

Im Focus der technischen Betrachtungen zur Migration von Groupware und Messaging stehen sowohl die Abdeckung der Funktionalitäten von Exchange 5.5 durch alternative Lösungen, die auf linuxbasierten Systemen eingesetzt werden können als auch die Fortführung mit Exchange 2003. Bezüglich der ablösenden Migration ist die Nutzung in heterogenen Systemumgebungen mit linuxbasierten Serversystemen und windowsbasierten Clientsystemen mit der weitgehend vollständigen Weiternutzung von Microsoft Outlook ein Hauptaspekt der technischen Untersuchung.

Für die Anbindung des Outlookclients an die zur Verfügung stehenden alternativen linuxbasierten Groupwarelösungen stehen zahlreiche Möglichkeiten zur Verfügung. Über so genannte Connectoren lassen sich Outlookclients an fast alle hier betrachten Systeme anschließen. In der Regel lassen die Connectoren eine Anbindung in Echtzeit an die entsprechenden Serversysteme zu und erlauben somit eine konfliktfreie Nutzung der Gruppenfunktionalitäten. Über die Möglichkeit der Outlook-Konnektivität verfügen die Lösungen von OpenGroupware, Exchange4Linux, Kolab, Samsung Contact und Scalix. Diese Gruppe von Groupwarelösungen setzt sich sowohl aus rein kommerziellen Produkten (Scalix, Samsung Contact) und Produkten, die als OSS (OpenGroupware, Exchange4Linux, Kolab) verfügbar sind, zusammen. Die Outlook-Connectoren sind bei den kommerziellen Lösungen bereits Bestandteil der Produkte, für die OSS-Lösungen müssen die Connectoren als kommerzielles Zusatzprodukt erstanden werden.

Neben der Nutzung in heterogenen Systemen spielt auch die Nutzung in rein linuxbasierten Systemumgebungen eine wichtige Rolle und damit die Frage nach alternativer Client-Software zu MS Outlook. In der Regel verfügen die Lösungen noch über weitere Zugriffsmöglichkeiten, diese werden entweder in Form einer Webapplikation (Scalix, Samsung Contact, OpenGroupware, Open-Xchange, php-Groupware) oder durch den Zugriff mittels weiterer Groupwareclientsysteme realisiert. Der Einsatz der Web-Clients lässt jedoch naturgemäß keine Nutzung im Offline-Betrieb zu. Die Mail-Funktionalitäten der Webapplikationen können allerdings mit allen Mail-Clients, die POP 3 und IMAP unterstützen, genutzt werden. Neben dem webbasierten Zugriff bieten die Lösungen von Kolab, OpenGroupware, Open-Xchange und Samsung Contact auch die Anbindung alternativer Groupwareclientsysteme. Die Anbindung des linuxbasierten Groupwareclients „Kontact“ ist sowohl an die Kolab-, Open-Xchange- als auch an die OpenGroupwarelösung möglich. Die vollständige Unterstützung der Konnektivität von Kontact und OpenGroupware wird in der nächsten Version des Clientsystems realisiert. Für die Samsung Contact-Lösung steht ein Java-basierter, plattformunabhängiger, integrierter Client zur Verfügung.

Hinsichtlich der fortführenden Migration hin zu MS Exchange 2003 ist im Ergebnis festzuhalten, dass eine Einführung nur in Verbindung mit einer Einführung von Active Directory möglich ist. Dabei handelt es sich um eine grundlegende strategische Entscheidung, für die an dieser Stelle nochmals auf die technischen Betrachtungen zu AD in Kapitel 3.7 verwiesen wird.

3.12.2 Einleitung

Wie bereits im Kapitel 2 aufgeführt, ist davon auszugehen, dass in den meisten Behörden als Groupware-Lösung Exchange in der Version 5.5 eingesetzt wird. Daher sollen zunächst die Ausgangssituation beschrieben und mit Blick auf die ablösende Migration unterschiedliche Groupware-Lösungen betrachtet werden, die auf linuxbasierten Betriebssystemen eingesetzt werden können. Es werden sowohl reine Open Source Projekte als auch kommerzielle Produkte betrachtet. Die Produkte verfolgen zum Teil sehr unterschiedliche Ansätze, Ziele und Ziel-

gruppen. Grundsätzlich kann aber primär zwischen den rein webbasierten und den klassischen Client-Server-Lösungen unterschieden werden. Aufgrund der großen Anzahl unterschiedlicher Lösungen können nicht alle auf dem Markt verfügbaren Lösungen betrachtet werden. Die betrachteten Lösungen wurden auf Basis unterschiedlichen Anforderungsszenarien ausgewählt.

3.12.3 Ausgangslage – Microsoft Exchange 5.5

An dieser Stelle werden die wichtigsten Merkmale und Funktionalitäten der Groupware-Lösung von Microsoft bezüglich der Version 5.5 beschrieben.

3.12.3.1 Basisinfrastruktur

Microsoft Exchange Server setzt eine Windows NT 4 Domänenstruktur als Basis voraus, die vorrangig zur Authentifizierung verwendet wird.

3.12.3.2 Logische Struktureinheiten

Die größte Struktureinheit von Microsoft Exchange Server ist die Organisation. Eine Organisation kann sich über mehrere NT Domänen erstrecken.

Des weiteren werden in Exchange Standorte (Sites) zur Strukturierung eingesetzt. Ein Standort stellt eine verwaltungstechnische Einheit dar. In einem Standort wird eine Gruppe von Exchange Servern logisch zusammengefasst, die miteinander über eine schnelle Netzwerkverbindung kommunizieren. Die Exchange Server eines Standortes stellen sich die Mails direkt zu und replizieren die Verzeichnisinformation direkt miteinander. Die Weiterleitung (Routing) von Mails zwischen Standorten muss ausdrücklich konfiguriert werden.

3.12.3.3 Basiskomponenten

Microsoft Exchange Server 5.5 setzt sich aus den folgenden Basiskomponenten zusammen:

- Exchange-Verzeichnis (Directory Service, DS),
- Message Transfer Agent (MTA),
- Informationsspeicher (Information Store, IS)
- und die Systemaufsicht (System Attendant, SA).

Das **Exchange-Verzeichnis** speichert alle Informationen über die Benutzer, die Ressourcen und die Organisation in einer Datenbank (dir.edb). Dazu gehören Listen der auf den Server registrierten E-Mail-Anwender, Server-Namen und Serverkonfigurationen. Zu beachten ist die Tatsache, dass sämtliche Konfigurationsinformationen in dem Verzeichnis gespeichert werden.

Der **Informationsspeicher** besteht aus zwei Datenbanken, dem „Privat Information Store“ (priv.edb) und dem „Public Information Store“ (pub.edb). Der „Privat Information Store“ speichert die Nachrichten und Dateianhänge für die Benutzer, deren Postfächer sich auf dem betreffenden Server befinden. Der „Public Information Store“ speichert den Inhalt von Repliken der öffentlichen Ordner.

Der **Message Transfer Agent** (MTA) übernimmt die Nachrichtenübermittlung an andere Server, Standorte und externe Systeme. In Kombination mit dem Exchange-Verzeichnis entscheidet der MTA über das Routing der Nachrichten. Eingehende Nachrichten werden vom MTA an den Informationsspeicher weitergegeben. Der MTA übernimmt auch die Konvertierung von Nachrichten in andere Formate.

Die **Systemaufsicht** stellt die Verwaltungsinstanz für den Exchange Server dar. Mittels dieser Komponente können beispielsweise neue E-Mail-Benutzer generiert sowie Überwachungs- und Wartungsaufgaben ausgeführt werden. Die Systemaufsicht überwacht die Netzwerkverbindungen zu anderen Exchange Servern und erstellt Routing-Tabellen.

Die folgende Tabelle zeigt die entsprechenden Komponenten und beschreibt in kompakter Form deren jeweilige Funktionen.

Tab. 30: Basiskomponenten Exchange 5.5

Komponente	Funktionen
Verzeichnis	• Verwaltung der Informationen zu den Empfängern, Verteillisten, Servern und der Messaging-Infrastruktur • Das Verzeichnis kann von anderen Komponenten zum Informationsabgleich genutzt werden, beispielsweise zum Abgleich von Adressen. • Innerhalb einer Organisation erfolgt die Replikation der Verzeichnisinformationen aller Server automatisch.
MTA	• Bildet die Kernkomponente der Kommunikationsinfrastruktur des Exchange Servers. • Nachrichtenübermittlung an andere Server, Standorte und Systeme • Formatkonvertierungen für andere Systeme
Informationsspeicher	• Speicherung der an einzelne Benutzer gesendeten Nachrichten • Verarbeitung und Speicherung der Informationen innerhalb der öffentlichen Ordner • Die privaten und öffentlichen Informationen werden in zwei getrennten Datenbanken gehalten • Informiert die Clients über neue Nachrichten und nimmt ebenfalls vom Client Nachrichten entgegen.
Systemaufsicht	• Protokollierung der Messaging-Aktivitäten • Überwachung der Nachrichtenverbindungen zwischen den Servern • Aufbau von Routing-Tabellen • Überwachen der Verzeichnisreplikationen und die Auflösung von Widersprüchen • Protokollierung der Nachrichtenversendung • Generieren von E-Mail-Adressen für neu erstellte Empfänger

3.12.3.4 Optionale Komponenten

Optionale, modulare Komponenten, wie z. B. unterschiedliche Konnektoren und der Schlüsselverwaltungsserver, können den Funktionsumfang des Exchange Servers erweitern.

Konnektoren (Connectors) vermitteln zwischen verschiedenen Systemen oder Standorten Nachrichten.

- Site Connector und Directory Replication Connector (verbindet Standorte zu einem unternehmensweiten System)
- Dynamic RAS Connector (verbindet Standorte via asynchroner Wählverbindungen)
- Internet Mail Service (verbindet Standorte via SMTP oder das Exchange System mit dem Internet)
- Internet News Service (verbindet Exchange per NNTP mit Internet News)
- MS Mail Connector und Directory Synchronization (bietet die Anbindung zu MS Mail 3.x Systemen)
- Microsoft Schedule+ Free/ Busy Connector
- X.400 Connector (verbindet Standorte mittels dedizierter Bandbreitensteuerung oder das Exchange System mit fremden X.400 Systemen)
- Connector for cc:Mail (verbindet Exchange mit Lotus cc:Mail Systemen).

Es kann zwischen internen und externen Konnektoren unterschieden werden. Die internen Konnektoren verbinden zwei Exchange Standorte miteinander und sind in erster Linie logische Objekte, die die Administration vereinfachen. Die externen Konnektoren sind zusätzlich Software-Komponenten und sorgen für die Anbindung des Microsoft Exchange Servers an andere Mailsysteme. Die Konnektoren sorgen für die richtige Konvertierung des Nachrichteninhaltes und der Adressinformationen. Dadurch werden Nachrichten aus Exchange im fremden System lesbar und Nachrichten des fremden Systems können von Microsoft-Exchange-Benutzern gelesen werden.

Der **Schlüsselverwaltungsserver** (Key Management Server, KMS) kann zur Verwaltung von Schlüsseln eingesetzt werden, mit deren Hilfe sich Nachrichten verschlüsselt versenden oder mit einer digitalen Signatur versehen lassen.

Eine weitere optionale Komponente ist der **Chat-Server.** Dieser ermöglicht die Realisierung so genannter „Internet Relay Chats“ (IRC), womit wiederum die gleichzeitige Kommunikation einer großer Anzahl von Teilnehmern miteinander erlaubt wird.

Seit der Version 5.5 wurde auch der so genannte **Server Scripting Service** implementiert. Der Service sorgt dafür, dass Skripte, die in einer Skriptsprache wie Perl, VB Script oder JScript geschrieben wurden, in einem öffentlichen Ordner hinterlegt werden können. Der Dienst sorgt für die Ausführung der Programme

beim Eintreten von bestimmten Ereignissen. Mit Hilfe der Skripte können Aufgaben automatisiert werden.

3.12.3.5 Protokollunterstützung

Exchange unterstützt eine ganze Reihe von unterschiedlichen Protokollen, die Wichtigsten werden im folgenden Abschnitt erläutert.

Das Simple Mail Transfer Protocol (SMTP) stellt ein Standardprotokoll zur Nachrichtenübermittlung im Internet dar.

Für die Zustellung von Nachrichten an nicht immer verbundene Client-Rechner findet das POP3-Protokoll Anwendung. Dieser Standard ist auf den Austausch zwischen nur temporär verbundenen E-Mail-Clients und -Servern zugeschnitten. Mail-Clients arbeiten mit POP3 beim Lesen von Nachrichten. Der Versand von Nachrichten erfolgt mittels SMTP.

Einen anderen Ansatz verfolgt der IMAP4-Standard, dieser wird von den meisten E-Mail-Produkten unterstützt. Die große Stärke von IMAP4 gegenüber POP3 ist die Fähigkeit, Nachrichten selektiv vom Server zu laden. So können beispielsweise Nachrichten getrennt von eventuell vorhandenen Anhängen heruntergeladen werden.

Durch die Integration von HTTP können Dokumente in öffentlichen Ordnern über das Internet zugänglich gemacht werden. Durch die Verwendung des Microsoft Internet Information Server (IIS) und des Exchange Servers 5.5 können die Benutzer durch Outlook Web Access (OWA) auf Funktionalitäten zurückgreifen, die sonst nur mit dem Outlook-Client möglich wären. Die Informationen werden mittels der Active Server Pages generiert, somit ist die HTTP-Unterstützung in erster Linie eine Erweiterung des Internet Information Servers. Die HTTP-Unterstützung erfordert deshalb auch das Vorhandensein eines Internet Information Servers mit ASP-Funktionalität. Die Nutzer können beispielsweise private und öffentliche Ordner einsehen, Mails senden und empfangen und weitere Funktionen verwenden. Der vollständige Funktionsumfang ist jedoch nur mit dem Microsoft Internet Explorer nutzbar.

NNTP sorgt für die weltweite Verbreitung von Newsgroups. Die Inhalte der Newsgroups werden über NNTP von Server zu Server übertragen. Der Exchange Server kann die Inhalte von Newsgroups über die NNTP-Anbindung in den öffentlichen Ordnern zur Verfügung stellen.

LDAP erlaubt Clients den Zugriff auf Verzeichnisinformationen aus dem Microsoft Exchange Server-Verzeichnis.

3.12.3.6 Produktvarianten

Exchange Server 5.5 wird in zwei verschiedenen Versionen eingesetzt:

- Standard Edition
- Enterprise Edition

Die Enterprise Edition unterstützt ein Exchange Cluster mit zwei Knoten auf Basis von Windows NT 4 Enterprise Edition.

3.12.3.7 Anwenderfunktionalitäten

Die dem Anwender durch Besitz eines Postfaches zur Verfügung stehenden Funktionalitäten sind:

- E-Mails (Post) empfangen und senden
- Aufgabenverwaltung
- Terminverwaltung
- Adresslisten (allgemeine Adressbücher und persönliche Kontakte)
- Journalführung und Notizen.

Als typische Client Software wird in diesem Leitfaden Microsoft Outlook angenommen. Outlook ist in den Versionen 97 (Ver. 8), 98 (Ver. 8.5), 2000 (Ver. 9) und 2002 (Ver. 10, XP) erschienen.

Outlook und Exchange bieten die Möglichkeit, Daten offline zu speichern und zu bearbeiten und bei vorhandener Netzwerkverbindung zu synchronisieren (klassischer Fall beim Einsatz von Notebooks).

Outlook selbst ermöglicht als PIM (Personal Information Manager) den Einsatz von Persönlichen Ordnern, die in Form von Dateien (*.pst) gespeichert werden.

In öffentlichen Ordnern (Public Folder) können z.B. Workflows oder Gruppenpostfächer bereitgestellt werden. Die Verwendung von öffentlichen Ordnern ermöglicht die gemeinsame Nutzung von Informationen. Benutzer, die mit den entsprechenden Zugriffsrechten ausgestattet sind, können die in den Ordnern gespeicherten Informationen lesen und/oder schreiben.

3.12.3.8 Client-Server-Kommunikation

Die Kommunikation zwischen Client und Server erfolgt in typischer LAN Umgebung mit Outlook-Clients via MAPI (Messaging Application Programming Interface) und somit über RPC (Remote Procedure Calls).

Durch die Unterstützung von SMTP, POP3, IMAP und HTTP können verschiedenste Kommunikationsszenarien zwischen Client und Server realisiert werden.

3.12.3.9 Server-Server-Kommunikation

Die Kommunikation zwischen Exchange Servern kann durch die vielfältigen Konnektoren gesteuert werden. Befinden sich zwei Server innerhalb desselben Standortes, kommunizieren sie via RPC.

3.12.3.10 Verwandte Themen

Durch den Einsatz von Mailsystemen existiert die erhöhte Gefahr des Virenbefalls. In Exchange besteht für Dritthersteller die Möglichkeit, Virenschutz-Software durch Nutzung der eigens geschaffenen Virenschutz-API zu implementieren.

Die Integration von FAX-Lösungen in Exchange Umgebungen wird von vielen Drittherstellern adressiert.

Die Archivierung von E-Mails oder die Verdrängung von längerer Zeit nicht genutzten Mail-Objekten (Hierarchical Storage Management, HSM) ist durch Software von Drittherstellern realisierbar.

3.12.4 Ablösende Migration

Das jeweilige Ziel einer ablösenden Migration kann von Anwendungsfall zu Anwendungsfall verschieden sein. Es ist im Vorfeld einer Migration genau zu ermitteln, welche tatsächlichen Ansprüche an ein Groupware-Produkt gestellt werden. Die folgende Liste zeigt beispielhaft einige Kriterien für die Auswahl einer Groupware-Lösung:

- Welche Client-Systeme müssen unterstützt werden?
  - Nur webbasierte Clients
  - Outlook-Clients (MAPI-Unterstützung)
  - Linuxbasierte Client-Systeme
  - Clients in heterogenen Systemlandschaften (Windows- und linuxbasierte Systeme)
- Welche Groupware-Funktionalitäten müssen von dem Neusystem unterstützt werden?
- Welche Ansprüche werden an die Skalierbarkeit der Systeme gestellt?
- usw.

Die Verifizierung der Ansprüche an ein neues Groupware-Produkt ist unabdingbar und im Vorfeld des jeweiligen Projektes durchzuführen.

3.12.4.1 phpGroupware

Ein Vertreter der rein webbasierten Lösungen ist die unter GPL stehende Groupware-Lösung „phpGroupware“[1]. Die Generierung der dynamisch erzeugten Inhalte geschieht auf Basis der Skriptsprache PHP. Die Inhalte werden mittels eines Webservers zur Verfügung gestellt, die Datenverwaltung und -haltung kann in einer MySQL-Datenbank erfolgen. Als Datenbanksysteme können aber auch PostgreSQL, Oracle und Sybase gewählt und für die Adressverwaltung ein LDAP-Directory eingesetzt werden. Die Benutzer-Authentifizierung kann ebenfalls mittels verschiedener Technologien (SQL, SQL_SSL, LDAP, HTTP, NIS, PAM) realisiert werden.

Für die E-Mail-Funktionalität lassen sich beliebige Mailserver einsetzen, diese müssen die Protokolle SMTP und POP3/ IMAP unterstützen. Eine Unterstützung von serverbasierten Filterregeln und Abwesenheitsprofilen ist zurzeit nicht möglich.

[1] Weiterführende Informationen zu PHPGroupware: http://www.phpgroupware.org/

phpGroupware ist ein modular aufgebautes System. Bei der Integration kann zwischen zahlreichen Modulen ausgewählt werden. So stehen neben jenen zur Realisierung klassischer Groupware-Funktionalitäten noch weitere Module bereit.

Tab. 31: Auswahl an phpGroupware-Modulen

Module	Funktion
Addressbook	Kontakt-Manager
Admin	Administration
Backup	Sicherungswerkzeug
Calendar	Kalender, inklusive Versand von Einladungen und Zugangs-berechtigungen
Cdb	Kontaktdatenbank
Email	E-Mail-Client
Forum	Nachrichten und Diskussionsforum
Projects	Projektmanagement
Timetrack	Zeiterfassung
ToDo	Aufgabenverwaltung
TTS	Trouble Ticket System

Die Module können optional durch administrative Eingriffe aktiviert werden. Die Weboberflächen basieren auf einem Template-System, es kann zwischen drei Typen für die Layout-Beschreibungen (XML, eTemplates, HTML) unterschieden werden. Die Definition der Farben, Schriften und der Ausrichtung erfolgt mittels CSS (Cascading Style Sheets). Problematisch ist die teilweise Verwendung von Javascript innerhalb der Weboberflächen, denn nicht alle Browser können den Javascriptcode fehlerfrei darstellen und außerdem ist die Verwendung in vielen Behörden aus Sicherheitsgründen nicht erlaubt.

Der Einsatz einer rein webbasierten Lösung bietet viele Vorteile:

- Ein Zugriff über Webbrowser ist möglich, ebenso der gesicherte Zugriff über HTTPS von außen.
- Die Installation eines speziellen Clients ist nicht notwendig.
- Die Betriebssystemunabhängigkeit bietet insbesondere in heterogenen Client-Landschaften Vorteile.
- Die Softwareaktualisierung erfolgt nur auf dem Server.

Diesen Vorteilen stehen aber auch Nachteile gegenüber:

- Ein Zugriff auf die Daten ist nicht möglich, wenn die Benutzer offline sind oder keinen Zugang zu dem entsprechenden Netzwerk haben. Problematisch ist das besonders für Mitarbeiter, die im Außendienst sind.
- Es existiert keine Synchronisation mit mobilen Endgeräten (PDAs).

Abschließend ist festzustellen, dass die vorgestellte Lösung keine Alternative zu der Outlook–Exchange-Lösung darstellt. Jedoch kann das vorgestellte Groupwa-

re-Produkt insbesondere für kleinere Organisationen mit nicht so hohen Ansprüchen an die jeweilige Funktionstiefe eine günstige Lösung sein. Vorteilhaft ist die Flexibilität in Hinblick auf die Anpassungsmöglichkeiten der einzelnen Module an die tatsächlichen Bedürfnisse der Organisation.

Eine ähnliche Lösung bietet auch PHProjekt an. Beide Projekte, PHPGroupware und PHPProjekt, haben eine Live-Demoversion[1] ins Internet gestellt, durch die sich die Interessenten einen ersten Eindruck über deren Leistungsumfang verschaffen können.

3.12.4.2 Kolab

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beauftrage in den Jahren 2002 bis 2003 ein Firmenkonsortium, eine Freie Software Groupware-Lösung für den Einsatz im BSI zu erstellen. Darauf aufbauend entwickelte sich das Kolab-Projekt[2], das Ende 2004 die zweite Generation der Software fertiggestellt hat. Eine Nutzung der Kolab Groupwarelösung ist aufgrund der bestehenden OSS-Lizenz (GPL) ohne Zahlung von Lizenzgebühren möglich, zur Unterstützung der Nutzer werden auch kommerzielle Dienstleistungen[3] angeboten. Desweiteren erlaubt die freie Lizenz (GPL) jedem Erweiterungen, Verbesserungen und Veränderungen an Kolab vorzunehmen.

Kolab ist eine plattformübergreifende Groupware-Lösung, die sowohl mit GNU/Linux-Clients als auch mit Windows-Clients nutzbar ist. Die Funktionalitäten sind mit der Outlook/Exchange-Kombination von Microsoft vergleichbar. Das Clientsystem Outlook wird mit Hilfe eines Plugins zum vollwertigen Kolab-Client und bietet so die gleiche Funktionalität wie der GNU/Linux-Client Kontact.

Serversystem

Die zentrale Komponente ist der Kolab-Server, die wiederum auf eine Reihe weiterer freier Komponenten zurückgreift. Die einzelnen Komponenten werden in den folgenden Tabellen aufgeführt.

Tab. 32: Zentrale Kolab-Server-Komponenten

Komponenten	Aufgaben
Cyrus IMAP	IMAP / POP3 Mail-Server
Cyrus SASL	Authentifizierung
OpenLDAP	Verzeichnisdienst, z.B. für die Nutzerverwaltung
Postfix	Mail-Transfer-Agent
Apache / PHP	Webserver für das Webfrontend

[1] PHPGroupware : http://de.demos.phpgroupware.org/
PHProjekt : http://www.phprojekt.com/demo.php

[2] Kolab: http://www.kolab.org/

[3] z.B. Kolab-Konsortium: http://www.kolab-konsortium.de/

Tab. 33: Optionale Kolab Server-Komponenten

Komponente	Aufgabe
Amavisd-New	Ansteuerung von Spamfilter und Virenscanner
z.B. ClamAV	Virenscanner
z.B. Spamassassin	Spamfilter

Die Kolab-Lösung baut auf einem Client-Server-Ansatz auf, der eine asynchrone Nutzung der Groupware-Funktionalitäten durch die Benutzer gewährleistet. Diese haben z.B. die Möglichkeit E-Mails, Termine, Kontakte und persönliche Aufgaben mit der entsprechenden Client-Software offline zu nutzen, d.h. ohne Verbindung zum Kolab-Server. Die Änderungen werden durch eine spätere Daten-Synchronisation mit dem Server abgeglichen.

Als mögliche Nutzerzahlen werden vom Kolab-Projekt maximal einige Tausend Nutzer für einen einfachen, voll integrierten Server empfohlen. Die hohe Skalierbarkeit der Kolab-Lösung auf ein Vielfaches der Nutzerzahl eines einfachen Servers beruht auf drei Eigenschaften:

- Der Multilokationsfähigkeit: Mehrere Kolab-Server bilden einen Verbund; jeder einzelne Kolab-Server bedient eine feste Teilmenge aller Groupware-Nutzer des Verbundes.
- Der Möglichkeit die einzelnen Kolab-Serverkomponenten (s.o.) auf einzelnen Servern zu betreiben: Ein Verbund aus Servern bildet somit einen einzigen geclusterten Kolab-Server.
- Den Clusterfähigkeiten von Cyrus IMAP, OpenLDAP und Postfix: Ein Verbund von Servern bildet somit eine einzelne geclusterte Kolab-Serverkomponente.

Für den produktiven Einsatz ist auch die Möglichkeit der einfachen Sicherung und Wiederherstellung von Daten entscheidend. Die Architektur des gesamten Kolab-Systems vereinfacht die Backup- und Recoverymöglichkeiten stark: Die Mailboxen werden als gewöhnliche Verzeichnisse im Dateisystem des Kolab-Servers abgebildet und sind somit mit üblichen dateisystembasierten Backupwerkzeugen handhabbar. Neben kompletten Mailboxen können mit denselben Backupwerkzeugen auch einzelne E-Mails, Termine, etc. gesichert und wiederhergestellt werden, da sie als einzelne gewöhnliche Dateien abgelegt werden.

Neuerungen bei Kolab2 sind unter anderem:

- die Möglichkeit für Mehrfachstandorte (Multilokationsfähigkeit),
- die explizite Vergabe von Zugriffsrechten,
- die gemeinsame Bearbeitungsmöglichkeit für Verzeichnisse,
- die volle Mehrkontenfähigkeit,
- die automatische Annahme von Terminen

- einfachere Integration externer Verzeichnisdienste (LDAP).

Client-Systeme

Der Zugriff auf die Mail- und Groupware-Funktionalitäten kann sowohl mit einem Windows- als auch mit einem GNU/Linux-Client erfolgen. Bei Kolab1 wurde als Referenz-Client Microsoft Outlook 2000 berücksichtigt, Kolab2 berücksichtigt Outlook 2003.

Für Kolab-Installationen hat sich der seit Oktober 2003 am Markt befindliche Toltec Connector der Firma Radley Network Technologies CCs[1] bewährt. Der Toltec Connector ist ein kostenpflichtiges proprietäres Produkt und muss zusätzlich zu Outlook installiert werden. Der Connector ermöglicht einem Outlook-Client, seine Daten auf einem Kolab-Server zu speichern. Es stehen auf dem Markt auch noch andere Connectoren zur Verfügung, diese wurden jedoch im Rahmen der Evaluierung nicht gesondert betrachtet.

Für den Zugriff auf die Groupwarefunktionalitäten stehen den Nutzern von linux-basierten Arbeitsplätzen der Kontact Client zur Verfügung. Dieser GNU/Linux-Client ist eine verbesserte und erweiterte Version von KDEs Kontact, das die Möglichkeiten von KMail, KOrganizer, KAdressbook und weiteren Komponenten des KDE-PIM-Projektes unter einer einheitlichen grafischen Oberfläche zusammenfasst. Der Client fügt sich sehr gut in die KDE-Oberfläche ein und ist von Nutzern intuitiv zu bedienen. Kontact unterstützt u.a. die Protokolle POP3 und disconnected IMAP4. Unterstützt wird auch das Filtern eingehender E-Mails (Spam, Viren, usw.) auf der Clientseite.

Die folgende Auflistung gibt die wichtigsten Funktionalitäten der Groupware-Lösung wieder:

- E-Mails empfangen und senden,
- Kontaktverwaltung
- Rechtevergabe auf Ordnern
- Gemeinsame Bearbeitung von freigegebenen Ordnern mit z.B. E-Mails, Terminen, Kontakten, Aufgaben, etc.
- Globale Adressbücher
- Gruppenkalender und -termine
- Gruppenordner (“Shared Folders“)
- Resourcenverwaltung (Buchung von Räumen, Beamern, etc.)
- Persönliche Notizen und Aufgaben
- Frei- / Belegt-Listen

[1] Toltec-Connector: http://www.toltec.co.za/

- Weiterleitungen in andere Postfächer
- Abwesenheitsbenachrichtigungen
- Funktionspostfächer mit mehreren unterschiedlich Zugriffsberechtigten
- Lesebestätigungen
- PDA-Synchronisation.

Sicherheit

Auf die Integration von Sicherheitsstandards wurde bei der Entwicklung besonderer Wert gelegt. Die Kommunikation zwischen den Client-Systemen und dem Server kann vollständig verschlüsselt (SSL/ TLS) geschehen. Die verschlüsselte Kommunikation kann u.a. mittels der Protokolle

- IMAPS,
- SMTP über TLS und
- HTTPS

realisiert werden. Der Linux-Client unterstützt die Ende-zu-Ende-Sicherheit sowie elektronische Signaturen auf Basis internationaler Standards (S/MIME, X.509v3); die Implementierung Ägypten[1] ist vom BSI erfolgreich auf Interoperabilität[2] getestet worden.

Administration

Für die administrativen Belange sind drei spezielle Nutzergruppen mit besonderen Rechten vorgesehen. Es wird zwischen folgenden Gruppen unterschieden:

- Administratoren,
- Maintainer,
- User (Benutzer).

Die Administration kann, entsprechend der unterschiedlichen Berechtigungen, über die Verwendung der webbasierten Administrationsoberfläche erfolgen. Einfache administrative Aufgaben können mittels des Web-Frontends realisiert werden, bei komplexen Tätigkeiten sind die entsprechenden Konfigurationsdateien auf dem Kolab-Server anzupassen.

Über das Weboberfläche können beispielsweise folgende Aktionen vorgenommen werden:

- Nutzer- und globale Adressbuchverwaltung,
- Verwaltung der öffentlicher Ordner,

---

1 Ägypten: http://www.gnupg.org/aegypten/index.de.html

2 Sphinx-Interoperabilitätstests: http://www.bsi.bund.de/fachthem/verwpki/interoptests/testberichte.htm

- Verwaltung der Resourcen- und Gruppenkonten
  - teilweise Administration der Serverdienste,
  - Abwesenheitsbenachrichtigungen und Weiterleitungen.

Über das Web-Frontend wird in erster Linie der Zugriff auf den Verzeichnisdienst (LDAP) ermöglicht, weitergehende Anpassungen müssen an den entsprechenden Server-Komponenten vorgenommen werden.

Der einzelne Benutzer hat ggf. auch die Möglichkeit, bestimmte Änderungen direkt vorzunehmen. So können die Benutzer ihre persönlichen Daten modifizieren und beispielsweise zusätzliche Mail-Adressen (sog. Mail-Aliases) hinzufügen.

Migration

Bei der Migration der bestehenden Daten können prinzipiell folgende Mechanismen verwendet werden:

- Export der Verzeichnisinformationen mittels LDIF und skriptbasierte Anpassung der Daten
- E-Mails können mittels POP3 oder IMAP direkt auf Kontact migriert werden
- Transfer von Adressdaten im vCard- und Kalenderdaten im iCal-Format
- Umwandlung der Emails und der Adress- und Kalenderaten per Toltec Connector
- Extraktion von Kalender- und Adressdaten per „KDE-PIM for Windows“[1] oder per „KO/Pi“ und „KA/Pi“ und Import in Kontact.

Fazit

Aus dem Bereich der Verwaltung sind bisher keine Erfahrungen mit großen Installationen von Kolab bekannt. Nach Angaben des Kolab-Projekts existieren jedoch weltweit eine dreistellige Anzahl von Kolab-Installationen mit einer insgesamt fünfstelligen Anzahl von Benutzern, darunter einige mit mehreren Tausend Nutzern.

Der Vorteil dieser Groupwarelösung liegt in dem modularen Aufbau des gesamten Systems, bei dessen Entwicklung auf bewährte und skalierbare Komponenten zurückgegriffen wurde.

Die Möglichkeit, die Nutzerverwaltung innerhalb eines zentralen Verzeichnisdienstes zu realisieren, vereinfacht die Verwaltung der Daten. Der Verzeichnisdienst kann auch zur Datenhaltung für andere Systeme (z.B. Samba) verwendet werden. Durch die gleichzeitige Unterstützung von Linux-Clients und Windows-Clients bietet Kolab sich besonders für den Einsatz in heterogenen Client-Umgebungen an.

---

[1] http://www.pi-sync.net/, http://www.pi-sync.net/html/projects.html und http://sourceforge.net/projects/kdepimpi/

3.12.4.3 OpenGroupware.org

OpenGroupware.org (OGo) ist, ähnlich wie andere Open Source Software Lösungen, aus einem ehemals kommerziellen Produkt entstanden. Im Sommer 2003 hat die SKYRIX Software AG das gleichnamige Produkt unter den Lizenzbedingungen der GNU GPL/LGPL freigegeben. Seit diesem Zeitpunkt wird die Software unter dem Namen OpenGroupware.org als Community-Projekt weiterentwickelt. Das Hauptziel dabei ist, die Applikation zu einem der wichtigsten Open Source Groupware-Lösungen zu entwickeln. Weitere Ziele sind die Bereitstellung eines Integrationsbausteins zu OpenOffice.org, der Ausbau bereits vorhandener offenen APIs auf Basis von XML sowie eine Anbindung freier und proprietärer Groupware-Clienten. Zum aktuellen Zeitpunkt steht Ogo in Form von so genannten „Nightly build“ Paketen zum Download bereit. Ogo 1.0 soll als erstes offizielles stable Release im Frühjahr 2005 erscheinen.

Serversystem

Die folgende Abbildung zeigt die grundlegende Architektur des Groupwaresystems im Zusammenspiel mit anderen OSS Komponenten.

Bild 34: OpenGroupware-Architektur

OpenGroupware.org ist eine Server-Anwendung, die von Anwendern im Web-Browser bedient wird. Derzeit stehen Pakete für die Installation auf x86-Linux Distributionen von Debian, Suse, RedHat und Mandrake sowie für FreeBSD zur Verfügung. Neben der Kernanwendung, die in Objective-C geschrieben wurde, setzt OpenGroupware.org auf bewährte Standardkomponenten wie PostgreSQL, Apache oder Cyrus IMAP.

Der Server bietet folgende Funktionen:

- Gruppenterminplanung
- Kontakte (Personen, Unternehmen)
- Ressourcenmanagement
- Taskmanagement
- Projektcontainer zur Verwaltung von Dokumenten (inkl. Versionierung), Notizen und Aufgaben
- E-Mail (mit zusätzlichem Mail-Server, beispielsweise dem Cyrus IMAP Server)
- umfassendes Rechtemanagement für Kontakte, Termine, Aufgaben und Projekte
- Palm-Synchronisation
- CTI API zur Integration von TK-Anlagen

Das Backend zeichnet sich durch eine modulare Architektur und vor allem durch das Vorhandensein einer umfangreichen XML-RPC APIs aus. Mit diesem API können nahezu alle Funktionalitäten, die über die webbasierte Nutzerschnittstelle oder andere Clients genutzt werden können, ausgeführt werden.

Zur Unterstützung einer großen Anzahl von parallel arbeitenden Nutzern besteht die Möglichkeit der horizontalen Skalierung durch die Verwendung eines Software Loadbalancers[1].Dieser verteilt die einzelnen OGo Prozesse ja nach Lastsituation auf verschiedene Nodes im Clusterverbund. Dieses Verfahren kann auch zur Gewährleistung von Ausfallsicherheit genutzt werden.

Clientsysteme

OpenGroupware.org bringt von Haus aus eine gut ausgebaute webbasierte Nutzerschnittstelle mit. Der Anwender verfügt über die Möglichkeit, die Ansichten der Schnittstelle seinen persönlichen Bedürfnissen anzupassen. Zentrale Komponenten zur Organisation von Gruppen- und Einzelterminen, Ressourcen und Kontakten sind ebenso integriert wie Projektcontainer, die sowohl Aufgaben, Notizen und Dokumente aufnehmen und entsprechend der vergebenen Zugriffsrechte den Teammitgliedern zur Verfügung stehen. In jedem Projektcontainer lassen sich beliebige Ordnerstrukturen erzeugen, in denen Dokumente mittels eines Check-In/Check-Out Verfahrens versioniert gespeichert und ab OGo 1.0 zusätzlich über WebDAV zur Verfügung gestellt werden. Über den eingebauten WebMailClient wird der Zugriff auf IMAP4 Postfächer ermöglicht, wobei auch serverseitige Filter, Abwesenheitsnotizen und Mailquotas über den Webbrowser verwal-

[1] Der Loadbalancer steht im Rahmen des Hersteller Maintenanceservice zur Verfügung.

tet werden können, sofern diese Funktionen vom IMAP Server unterstützt werden[1].

Outlook Anwender benötigen hingegen einen properitären und kostenpflichtigen Connector, welcher von der SKYRIX Software AG unter dem Produktnamen „ZideLook“ angeboten wird. Die Lösung besteht aus einem "MAPI Storage Provider"-Plugin für Outlook und einem zusätzlichen Servermodul für OpenGroupware.org. Zwischen Server und Client erfolgt keine Synchronisation der Daten sondern ein Direktzugriff auf die "live" Daten des Groupware-Servers. Das ZideLook-Plugin übersetzt dabei die MAPI Aufrufe von Outlook in Aufrufe gemäß dem standardisierten WebDAV Protokoll und sendet sie an den ZideStore Server. Dieser liefert die OGo Groupware Daten im XML Format aus. Der noch fehlende Replikationsmechanismus schränkt jedoch die Nutzung für mobile Anwender ein. ZideLook funktioniert problemlos neben anderen Outlook Diensten wie z.B. Microsoft Exchange. ZideLook ermöglicht den Zugriff auf den privaten Kalender, auf die private Aufgabenliste, auf Gruppenkalender und Gruppen-Aufgabenlisten, auf öffentliche (globale) und private Kontakte. Aktuell werden die Outlook Versionen 2000, XP und 2003 offiziell unterstützt.

PalmOS basierte PDAs und Smartphones können direkt über den in OGo enthaltenen NetworkHotSync Daemon angebunden werden. Sämtliche Einstellungen zur Übernahme von Kontakten, Terminen und Aufgaben kann der Anwender dabei über die Webschnittstelle vornehmen. Es ist neben dem Abgleich über die klassische USB-Dockingstation auch die Datenübermittlung im mobilen Betrieb über Handys mittels IrDA/Bluetooth und WLAN möglich. Anwendern von PocketPC bzw. WindowsCE Endgeräten oder aktuellen Smartphones steht derzeit nur die Anbindung über den MS Outlook Client zur Verfügung.

Sicherheit

OpenGroupware.org unterstützt durch die Verwendung von standardisierten Komponenten und Protokollen die vollständige Verschlüsselung zwischen Server und dem jeweilig verwendeten Clientsystem. Durch eine entsprechende und korrekte Konfiguration des Apache Webservers werden die HTTP und WebDAV Verbindungen mittels SSL-Verschlüsselung gesichert. Für die Anbindung von Outlook und PalmOS Endgeräten ist der Einsatz eines geeigneten SSL-Tunnels zu empfehlen. Dies gilt auch für die Kommunikation zwischen den einzelnen Servern, sofern einzelne Komponenten wie beispielsweise der IMAP-, LDAP- oder SQL-Server zwecks Lastverteilung auf separaten Servern betrieben werden sollen und diese über ein als unsicher einzuschätzendes Netz miteinander verbunden sind.

OpenGroupware.org unterstützt derzeit keine S/MIME bzw. PGP Mailverschlüsselung im webbasierten Mailclient. Eine entsprechende Erweiterung ist geplant.

[1] Es empfiehlt sich beispielsweise die Verwendung des Cyrus IMAP Servers.

Administration

Je nach Einsatzszenario erfolgt die Administration über die Webschnittstelle oder direkt mittels der Kommandozeile auf den Servern. So sind die Verwaltung von Nutzern, Teams, Ressourcen für die Terminplanung oder die Verwaltung von Kategorien für das Kontaktmanagement einfach und auch von Anwendern ohne Linuxerfahrung über den Browser realisierbar. Durch die Verwendung von Nutzer-Vorlagen lassen sich einmal definierte Benutzerprofile auf neu einzurichtende Nutzer vererben. .Alternativ bietet sich bei der Integration großer Nutzerzahlen die Verwendung eines LDAP basierten Verzeichnisdienstes an, der über das XML-RPC API integriert werden kann. Diese Schnittstelle ermöglicht darüber hinaus den skriptgesteuerten Zugriff auf nahezu alle Funktionalitäten des OGo Applicationservers und stellt somit eine Möglichkeit zur Automatisierung komplexer Initialisierungsprozesse dar. Das Design der Web-Oberfläche ist vollständig in Templates beschrieben, wobei beliebig viele dieser Template-Sets angelegt werden können und dem Nutzer dann wahlweise zur Verfügung stehen. Auf diesem Weg kann der Administrator auch sehr einfach gewünschte Anpassungen an existierende Cooperate Design Festlegungen vornehmen. Diese einfache Möglichkeit wird außerdem zur Lokalisierung der Web-Oberfläche benutzt, die bereits heute in 13 Sprachen zur Verfügung steht.

Für Anfang 2005 hat die SKYRIX Software AG eine „All-in-one“ Distribution auf Basis von OGo 1.0 angekündigt. Neben der Groupware selbst soll die Distribution auch das Betriebssystem, den Mailserver und eine browserbasierte Managementkonsole mitbringen. Durch die aufeinander abgestimmten und vorkonfigurierten Module wird sich nach Angaben des Herstellers der Zeitaufwand für das Setup eines Produktivsystems auf weniger als eine Stunde reduzieren lassen.

Migration

Für die Übernahme von Bestandsdaten bietet OGo mehrere Möglichkeiten, die je nach Anwendungsszenario individuell zu prüfen sind. Ein einfaches Verfahren ist der Import von Kontaktdaten direkt über das Webinterface. Unterstützt werden hier Exportformate von Outlook, Netscape und Daten im .csv Format.

Eine weitere Methode, die ebenfalls ohne die Unterstützung eines Dienstleisters auskommt, ist die Übernahme des Datenbestandes mittels MS Outlook. Dazu ist der kommerzielle ZideLook MAPI Connector notwendig, über den die relevanten Datensätze direkt per Drag&Drop aus den lokalen .pst-basierten Ordnern bzw. auch aus einem parallel laufenden MS Exchange Server in das OGo Backend überführt werden.

Ist die zentrale Übernahme großer Datenbestände vorgesehen, so empfiehlt sich der Einsatz der XML-RPC Schnittstelle, über die dann bereits beim Importvorgang Objektverknüpfungen, wie sie beispielsweise zwischen Personen- und Unternehmenskontakten vorliegen, hergestellt werden können. Voraussetzung für einen reibungslosen Ablauf der Migration ist dabei ein möglichst strukturiert vorliegender Altdatenbestand und das entsprechende XML-RPC-Wissen.

Fazit

OpenGroupware.org bietet ein umfassendes Funktionalitätsspektrum und kann als eine sehr interessante freie Groupwarelösung bezeichnet werden. Der Server beherrscht alle Groupwarefunktionalitäten, die im praktischen Einsatz benötigt werden und stellt diese dem Nutzer in allen wichtigen Clientanwendungen zur Verfügung, die im Rahmen heutiger Migrationsprojekte von Bedeutung sind. Durch die Verfügbarkeit eines MAPI Connectors zu MS Outlook ist auch der Einsatz in heterogenen Umgebungen möglich. Einschränkend muss jedoch auf die noch fehlende Möglichkeit der Synchronisation und somit auch des fehlenden Offline-Betriebs hingewiesen werden.

In heterogenen Umgebungen bietet sich insbesondere auch der Einsatz der webbasierten Nutzerschnittstelle an. Mittel eines Webbrowsers kann der Nutzer auf eine einfach bedienbar und funktionale Oberfläche zurückgreifen.

Die Verfügbarkeit der XML Schnittstelle, die eine Integration der Groupwarelösung in vorhandene Systemlandschaften erlaubt, stellt einen weiteren Vorteil der Lösung dar.

3.12.4.4 exchange4linux

Der Bill Workgroup Data Exchange Server wurde von den Entwicklern des deutschen Unternehmens Neuberger&Hughes GmbH entworfen. Der Server ist als GPL-Software freigegeben und wird fortlaufend weiterentwickelt. Ziel der Entwicklung war und ist, für den Microsoft Outlook-Cient ein alternatives Server-System bereitzustellen.

Den zukünftigen Nutzern des Produktes bieten sich mehrere Möglichkeiten zur Realisierung der Groupware-Lösung an. Das Server-System kann zum einen als Debian, RedHat und All-Source-Paket frei bezogen und zum anderen in einer von Neuberger&Hughes vertrieben Komplettlösung erworben werden. Die Komplettlösung umfasst neben dem integrierten Groupware-System auch die Internetaccess-Software „Easygate“. Easygate stellt die wichtigsten Infrastrukturdienste (DHCP, DNS, File-Server, Proxy-Server, Internet) zur Verfügung.

Serversystem

Die Groupware-Funktionalitäten werden durch das Zusammenspiel mehrerer Software-Einheiten erreicht. Die folgende Tabelle beinhaltet die erforderlichen Softwarepakete für den Betrieb des Groupware-Servers. Der Server wurde auf Basis der Programmiersprache Python realisiert und kommuniziert mit den Outlook-Clients mittels Corba (s. u:).

Tab. 34: exchange4linux Komponenten

Komponenten	Aufgaben
PostGreRSQL	Zentrale Datenhaltung
PyGreSQL Python interface	Schnittstelle zwischen der Datenbank und dem Groupware-Server

Komponenten	Aufgaben
Python 2.3 1	Programmiersprache
Exchange4linux	Groupware-Server
OpenLDAP	Optional zur Userverwaltung
Samba	Optional zur Windows PDC/AD Authentifizierung
Apache 2 / mod_python	SOAP Webinterface
OmniORB(py)	CORBA Implementierung

Es besteht auch die Möglichkeit, den exchange4linux-Server mit einem Verzeichnisdienst zu implementieren. Diese Möglichkeit ist insbesondere in Verbindung mit Samba zu erwägen und bietet dann eine zentrale Benutzerverwaltung für eine NT-Domäne und die Groupware-Komponente. Diese Lösung ist jedoch mit dem Komplettsystem von N&H nicht zu realisieren, vielmehr bedarf es einiger Anpassungen an dem exchange4linux Server, die durch entsprechende Dienstleister vorzunehmen sind.

Client-Systeme

Der Zugriff auf den exchange4linux Workgroup Server erfolgt mittels des Outlook-Clients. Grundlage für den Zugriff des Clients auf den Workgroup-Server ist ein von N&H entwickelter Client-MAPI-Treiber, der auf dem Client-System zu installieren ist. Die MAPI-Clients erzeugen mittels Corba auf dem exchange4linux-Server die entsprechenden Outlook-Befehle. Der N&H MAPI Service Provider ist ein kommerzielles Produkt und entsprechend verbunden mit einer kostenpflichtigen Lizenz.

Der Server unterstützt in Verbindung mit dem Microsoft Outlook-Client folgende Funktionalitäten:

- E-Mails empfangen und senden,
- Adressverwaltung für die einzelnen Benutzer,
- Globales Adressbuch,
- Gruppenkalender und –termine,
- Gemeinsame Ressourcen,
- Aufgabenverwaltung,
- Notizen in privaten und öffentlichen Ordnern,
- Free & Busy-Funktion,
- Einladungen, mit der Möglichkeit der Zu- oder Absage,
- Abwesenheitsbestätigungen,
- PDA Synchronisation über Outlook.

Nachfolgende Neuerungen bzw. Erweiterungen werden mit der Version 3.0 realisiert, die Vorabversion wird ab Januar 2005 verfügbar sein. Der offizielle Release erfolgt nach Herstellerangaben im Frühjahr 2005. Die Version 3.0 wird zusätzlich folgende Funktionalitäten bieten:

- Offline Ordner,
- PDA -Synchronisation mit Öffentlichen Ordnern,
- Blackberry Unterstützung mittels lokaler Outlook –Synchronisation,
- Forms und Kategorien im Personal Folder sollen unterstützt werden.

Um anderen Clients oder Webapplikationen Zugriff auf den Server zu ermöglichen, wurde SWAP (Simple Workgroup Access Protocol) implementiert. Dieser offene Standard wurde im Rahmen der Baden Württemberg Open Source Layers zusammen mit weiteren Softwareherstellern[1] dokumentiert. Mehrere freie Projekte arbeiten gerade an der Umsetzung dieses neuen Standards. Zum jetzigen Zeitpunkt steht noch keine alternative Zugriffsvariante für Linux-Clients zur Verfügung.

Sicherheit

Die Datenübertragung kann verschlüsselt zwischen den Systemen erfolgen, dabei können die Standards SSL und TLS verwendete werden. Serverseitig ist es möglich, die eingehenden Mails durch Produkte von Drittherstellern auf Viren zu überprüfen. Die Realisierung von serverbasierten Filterregeln zur Vermeidung von Spam-Mails ergänzen die Sicherheitsoptionen.

Zum Schutz vor unberechtigten Zugriffen können innerhalb der öffentlichen Ordner Zugriffsrechte vergeben werden. Die Zugriffsrechte werden mittels so genannter Access Control Lists (ACL) realisiert.

Die Speicherung der Daten innerhalb eines Datenbank-Systems bietet auch eine relativ einfache Möglichkeit, einzelne Datenverluste durch unbeabsichtigte Löschvorgänge wieder rückgängig zu machen. Der Restore-Vorgang lässt sich mittels Datenbank-Werkzeugen realisieren.

Administration

Die Administration beim Einsatz der Komplettlösung erfolgt mittels eines webbasierten Frontends. Im Rahmen der Administration wird standardmäßig nur zwischen Benutzern und Administratoren unterschieden. Eine weitere Unterteilung ist nicht vorgesehen. Das Webfrontend der Komplettlösung ermöglicht die Administration von Routineaufgaben. Komplexere administrative Tätigkeiten können mittels der herkömmlichen Linux-Bordmittel gelöst werden. In größeren Installationen wird mittels LDAP und Samba eine leistungsfähige Userverwaltung aufgebaut. Damit ist auch die Gruppenverwaltung sowie die Authentifizierung gegen ein bestehendes Active-Directory möglich.

---

[1] Millenux und Tarent Computer

Migration

Für die Daten-Migration werden in Abhängigkeit vom Ausgangsszenario verschiedene Lösungsansätze vorgeschlagen.

Bei einer sehr kleinen Migration (ca. bis 10 Benutzer) empfiehlt sich, eine Kopie der Postfach- und anderer Daten in einen persönlichen Ordner auf den jeweiligen Client-Systemen abzulegen. Die Daten können dann in die neu angelegten Mailboxen des neuen Systems importiert werden. Das Verfahren ist sehr zuverlässig, aber zugleich auch sehr zeitaufwändig. Bei einer Migration von bis zu 250 Benutzern wird empfohlen, auch andere Werkzeuge einzusetzen. Die Daten der Exchange-Benutzer können mittels der Exchange Administrator Konsole und des Microsoft-Tools „exmerge.exe“ exportiert werden. Die Informationen über die Postfach-Benutzer werden in einer einfachen CSV-Datei gespeichert, die Inhalte der Postfächer können in einem frei wählbaren Verzeichnis als PST-Dateien gesichert werden. Die gleiche Vorgehensweise ist auch auf die Öffentlichen Ordner anzuwenden. Im Anschluss können die CSV-Dateien durch ein von N&H bereitgestelltes Migrationstool auf den Bill Workgroup Server importiert werden. Die gesicherten Postfächer (PST-Dateien) können dann von den Benutzern mittels Outlook auf den Server importiert werden.

Bei größeren Migrationsprojekten bestehen noch weitere technische Möglichkeiten zur Datenübernahme, die im Einzelfall zu prüfen sind.

Fazit

Die vorgestellte Groupware-Lösung bietet eine sehr gute Unterstützung der Outlook-Clients, denn alle wichtigen Groupware-Funktionalitäten werden unterstützt und stehen den Benutzern zur Verfügung. Die Lösung ist zurzeit für Anwendungsszenarien von einigen hundert Nutzern (max. 500) optimiert und wird in diesem Rahmen bei produktiven Umgebungen eingesetzt.

3.12.4.5 Open-Xchange

Im August 2004 wurde die ursprünglich kommerzielle Groupware-Komponente Comfire unter dem Namen Open-Xchange als freie Software unter GPL zur Verfügung[1] gestellt und nach dem OpenSource-Modell weiterentwickelt. Die Groupware-Komponente ist der zentrale Bestandteil des Suse Linux Openexchange (SLOX). Der Open-Xchange Server wird zukünftig den Suse Linux Openexchange Server vollständig ersetzen, diese Bekanntmachung[2] erfolgte im Dezember 2004 durch die Unternehmen Novell/Suse und Netline. In einer gemeinsamen Vereinbarung zwischen den Unternehmen Novell und Netline wurden entsprechende Festlegungen getroffen. Novell/Suse bietet weiterhin für die SLOX- als auch die Open-Xchange-Lösung den Support (1st und 2nd Level), Wartung und Schulungen an. Gleichzeitig wurde die Freigabe von Suse-spezifischen Programmcodes für die Open-Xchange-Community vereinbart. Das Unternehmen

[1] http://mirror.open-xchange.org/ox/EN/community/

[2] http://www.novell.de/presse/releases/2004/index_vibrio.php?oid=33614

Netline Internet Service wird auf der GPL-lizensierten Open-Xchange-Lösung eine kommerzielle Version (Netline Open-Xchange Server 5) anbieten, diese ist für das erste Quartal 2005 angekündigt[1].

Die folgende Beschreibung bezieht sich auf das OSS-Projekt Open-Xchange Server in der aktuellen Version 0.75.

Server-System

An dieser Stelle sollen nur die Softwarepakete betrachtet werden, die im unmittelbaren Zusammenhang mit der Groupware-Lösung stehen. Die gesamte Lösung besteht aus unterschiedlichen modularen Software-Einheiten, die im Zusammenspiel die Mail- und Groupware-Funktionalitäten realisieren. Die Basis der Groupwarelösung bildet ein Java-basierter Applikationsserver, der im Zusammenspiel mit weiteren OSS-Komponenten die Gesamtlösung darstellt. In der folgenden Tabelle werden die möglichen zusätzlichen Komponenten aufgeführt.

Tab 35: Mögliche Komponenten der Open-Xchange-Lösung

Komponenten	Aufgaben
Postfix	Mail-Transfer-Agent (MTA)
Cyrus IMAPD	Realisiert die IMAP-Funktionalität
OpenLDAP	Zentraler Verzeichnisdienst für die Nutzerverwaltung
PostGRESQL Datenbank	Datenbank zur Verwaltung der Groupware-Daten
Apache – Tomcat	Realisierung des Webfrontends (Mail, Groupware)

Vorteilhaft an der modularen Architektur ist besonders die Skalierbarkeit aufgrund der Möglichkeit, Komponenten auf verschiedene Systeme zu verteilen. Die Modularität ermöglicht auch eine flexible Erweiterung bestehender Systeme.

Die Serverkomponenten bieten umfangreiche Mail- und Groupware-Funktionalitäten. Den Benutzern stehen unterschiedliche Funktionen zur Verfügung:

- E-Mails empfangen und senden
- Terminverwaltung
- Adressenverwaltung
- Aufgabenverwaltung
- Notizfunktionen
- Dokumentenmanagement (Versionskontrolle und Ordnerstruktur)
- Projektmanagement
- Konfigurierbare Wissensdatenbank

[1] Whitepaper „From SLOX to NOX“: http://mirror.open-xchange.org/ox/EN/downloads/NetlineWP-OXfuture.pdf

- Gruppenbasiertes Diskussionsforum

Die Nutzung der Funktionalitäten kann vollständig über eine integrierte Web-Portal-Seite erfolgen.

Client-Systeme

In Hinblick auf die Unterstützung unterschiedlicher Client-Systeme muss zwischen der Mail- und der Groupware-Funktionalität unterschieden werden. Der Zugriff auf die Mailfunktionalitäten kann mittels aller POP3- und IMAP-fähigen Clients erfolgen. Zusätzlich können die Benutzer über eine speziell integrierte Webmail-Lösung auf ihre Mails zugreifen.

Die Nutzung der Groupware-Funktionalitäten kann vollständig über den browserbasierter Zugriff auf die Web-Portal-Inhalte erfolgen. Weiterhin kann mittels folgender Clientanwendungen mit dem Groupwareserver kommuniziert werden:

- Zugriff über den Client *Kontact* unter Linux
- Apples iCal
- Mozilla Calender.

Durch die Verwendung des umfangreichen Web-Interface können die Benutzer auf alle oben aufgeführten Funktionalitäten zugreifen. Den Benutzern stehen in allen Funktions-Modulen die LDAP-basierten Adressbücher, die Möglichkeit der Rechtevergabe und Suchfunktionalitäten zur Verfügung. Bei der Nutzung der Terminvereinbarungs-Funktion erfolgt eine automatische serverseitige Analyse der bereitstehenden Ressourcen für den jeweiligen Zeitraum. Die webbasierten Angebote erlauben den Anwendern die Nutzung umfassender Gruppen-Funktionalitäten.

Unter Linux kann als eigenständiger Client das Linux-Programm *Kontact*[1] verwendet werden, das im Rahmen des KDE-Desktop-Projektes entwickelt worden ist. Es vereinigt die auch eigenständig einsetzbaren Programme KMail (E-Mail-Client), KAddressbook (Adressverwaltung mit LDAP-Schnittstelle), KPIM (Terminverwaltung) und andere unter einer gemeinsamen Oberfläche, die den Umstieg von Microsoft Outlook erleichtert. Kontact kommuniziert über die WebDAV-Schnittstelle mit dem Open-Xchange-Server. Die Einrichtung erfolgt über das mit Kontact mitgelieferte Programm *Sloxwizard*, das die Netzwerk- und Anmeldeeinstellungen vornimmt.

Neben der Nutzung der Kontact-Clients können auch noch weitere Fatclients (s.o) mit dem Server kommunizieren.

Sicherheit

Für die verschlüsselte Übertragung kann auf OpenSSL zurückgegriffen werden. OpenSSL realisiert die Datenverschlüsselung zwischen den Applikationen und

[1] Informationen zu Kontact sind unter http://kontact.kde.org/ zu finden.

Komponenten. IMAP und POP3 können mittels SSL-Tunnel und SMTP mittels TLS sicher übertragen werden.

Für die Erhöhung der Sicherheit im Mailverkehr kann nachträglich ein Virenscanner installiert werden, um problematische Mails und deren Anhänge zu identifizieren. Standardmäßig kann der SIEVE-Mail-Filter zum Aussortieren von Spam-Mails verwendet werden. Der Mailfilter erlaubt bei Bedarf auch, die Größe der Mails zu beschränken und nach frei wählbaren Kriterien weitere Filter anzuwenden.

Die Systemverwaltung wird mit den herkömmlichen Mitteln (Kommandozeilenbefehle und Konfigurationsdateien) gesteuert.

Fazit

Die Groupware-Lösung Open-Xchange bietet ein modular aufgebautes Groupware-System an, bei dem die einzelnen Module auf bewährten Open Source Komponenten basieren. Als Groupware-Komponente wird der Java-basierte Applikationsserver integriert, der im Zusammenspiel mit den anderen Komponenten den Benutzern umfangreiche Groupware-Funktionalitäten bietet. Der Benutzerzugriff auf die entsprechenden Groupware-Informationen kann entweder webbasiert oder mittels so genannter Fat-Clients erfolgen (Kontact, usw.). Browserbasiert können die Anwender auf das gesamte Portfolio der Open-Xchange-Lösung zugreifen. Offen sind noch die fehlende Anbindung an den Outlook-Client und ein komfortables Administrationswerkzeug bzw. eine entsprechende Oberfläche.

3.12.4.6 Scalix

Scalix ist eine für den Betrieb in Enterprise-Umgebungen ausgelegte Groupware- und Messaging-Plattform, die auf der bewährten HP-OpenMail-Technologie basiert. Das Unternehmen Scalix hat den Quellcode sowie die Entwicklungs- und Supportmannschaft von HP übernommen. Die Technologie zeichnet sich vor allem durch hohe Stabilität, große Skalierbarkeit (mehr als 10000 User pro Server möglich), eine Vielzahl offener Schnittstellen und das Konzept „Clients of Choice“ aus, durch das die gleichzeitige Anbindung verschiedener Arbeitsplatztypen möglich wird.

Serverplattform und Architektur

Als Betriebssystemplattform wird ausschließlich Linux verwendet, dabei werden die Distributionen von RedHat und Suse auf i386- und zSeries-Plattformen unterstützt. Scalix verwendet einen selbstentwickelten Server-Kern, der aus den Elementen Message Store, Directory und Routing besteht. Der Message Store basiert auf einer Standard-Linux-Filesystemstruktur, skaliert in den Terabyte-Bereich und kann auf Basis jedes Linux-Filesystems sowie auf Raid- oder logischen Volumes angelegt werden. Dabei wird jede Nachricht ungeachtet der Zahl der Empfänger nur einmal gespeichert. Große Attachments, die an mehrere User verschickt werden, nehmen somit nur einfachen Speicherplatz in Anspruch. Der Verzeichnisdienst ist ebenfalls eine Eigenentwicklung, nach außen wird er über

eine LDAP-Schnittstelle verfügbar gemacht. Der Router basiert auf dem X.400-Standard, verarbeitet aber auch andere Adressformate. Das Internet-Gateway lässt eine Konvertierung der Nachrichten in MIME- und TNEF-Format zu, letzteres spielt vor allem bei der Querverbindung mit MS-Exchange eine Rolle, da hier Nachrichten mit allen Sondermerkmalen ausgetauscht werden können.

Bild 35: Scalix-Plattform

Eine laufende Scalix-Instanz nimmt ohne angemeldete Benutzer lediglich etwa 30 MB RAM in Anspruch. Die Grundanforderungen an die Hardware sind moderat, ein 2-CPU-Intel-System mit 2 GB RAM ist im Regelfall für 5000 User ausreichend.

Clientseite und Groupware-Funktionalität

Scalix unterstützt auf der Windows-Plattform den Outlook-Client von Microsoft (2000, XP, 2003) in deutscher und englischer Sprache. Die MAPI-Anbindung ist dabei eine im „Workgroup“-Modus laufende Online-MAPI, lokale Datenspeicherung auf dem Client findet nicht statt. Die Funktionalität der Offline-Arbeiten kann jedoch eingerichtet werden. Regeln und Abwesenheitsbenachrichtungen werden auf dem Client eingerichtet und serverseitig ausgeführt. Besprechungsplanung mit Frei/Belegt-Funktion, automatisches Buchen von Ressourcen, Zugriff auf fremde Mailboxen über Delegation sowie die Rechtevergabe auf private und öffentliche Ordner werden analog zu Microsoft Exchange gehandhabt, lediglich serverbasierte Formulare werden nicht unterstützt. Das „Look & Feel“ von Outlook im Zusammenspiel mit Exchange wird dabei weitestgehend beibehalten.

Scalix bietet weiterhin einen eigenen Webclient an. Dieser verfügt über Drop-Down-Menüs, Drag-und-Drop-Funktionalität und eine Darstellung, die an eine echte Windows-Applikation erinnert. Dabei kommen in „Scalix Web Access“ (SWA) lediglich JavaScript und dynamisches HTML (DHTML) zum Einsatz.

Technologien wie Java-Applets oder ActiveX-Elemente werden nicht eingesetzt, so dass der Webclient auch in sicheren Netzwerkumgebungen und im Zusammenhang mit Firewalls eingesetzt werden kann. Als Browser werden Internet Explorer und Mozilla bzw. Firefox auf den Client-Plattformen Windows, Linux und Apple Mac OS/X unterstützt.

Bild 36: Scalix-Clientsysteme

Standard POP/IMAP-Clients wie Mozilla Thunderbird, Outlook Express oder Ximian Evolution können ebenfalls angebunden werden, das Adressbuch wird dabei über LDAP angesprochen. Für Ximian Evolution und andere iCal-basierte Clients wird laut Herstellerangaben voraussichtlich ab Frühjahr 2005 ein Konnektor angeboten, der einen vollen Zugriff auf die Kalender- und sonstigen Groupware-Funktionen ermöglichen soll.

PDAs und Handhelds können derzeit über den Outlook-Client angebunden werden. Für die Blackberry-Plattform steht in Zusammenarbeit mit Drittherstellern eine serverbasierte Anbindung zur Verfügung.

Integration

Die Scalix-Lösung lässt sich auch in bestehende Umgebungen integrieren. So können zum Beispiel LDAP-Verzeichnisse wie OpenLDAP, Novell NDS oder eDirectory, Sun Java Enterprise System Directory Server oder auch Active Directory für die Benutzerverwaltung eingesetzt werden (Single Point of Administration). Ein Login ist über einen Kerberos-basierten Single-Sign-On oder mittels PAM-Modulen über eine NT-Domäne, ein Active Directory System, andere LDAP-Directories oder auch eine klassische Unix-Authentisierung möglich. Eine scriptbasierte Schnittstelle ermöglicht die Anbindung jeglicher linuxbasierter Viren-

scanner[1]. Gleichermaßen können wegen der Filesystem-basierten Message-Store-Architektur jegliche Backup-Tools eingesetzt werden. Eine Archivierungs-Schnittstelle ist vorhanden. Für mehrere Fax- und Voice-Unified-Communications-Produkte[2] stehen Anbindungen zur Verfügung.

Bild 37: Scalix- Integration

Administration

Für die Administration von Scalix steht eine leistungsfähige Kommandoschnittstelle (CLI) zur Verfügung, die Remote-Administration über eine einfache SSH-Verbindung ermöglicht,. Daneben wird eine Web-basierte Admin-Console (Scalix Admin Console SAC) angeboten, die eine einfache Benutzer- und Gruppenverwaltung sowie die Unterstützung der täglichen Administrationsprozesse bietet. Die Admin-Console basiert auf einer Webservices-(SOAP-)Schnittstelle, die eine Anbindung an externe Managementsysteme ermöglicht.

Das Groupware- und Messagingsystem unterstützt Multi-Server-Umgebungen. Dabei können alle Groupware-Funktionen transparent über die gesamte Umgebung genutzt werden. Message-Routing und Synchronisation von Verzeichnissen und öffentlichen Ordnern erfolgen unsichtbar für den Benutzer. Die Admin Console kann hierbei auch zur Administration einer verteilten Serverumgebung über eine einheitliche Oberfläche eingesetzt werden.

Migration

Für die Migration bzw. die Einbindung in eine bestehende Systemlandschaft bietet Scalix mittels entsprechender Werkzeuge Unterstützung an. Benutzeraccounts können mittels LDAP-Synchronisation von Exchange 5.5, Exchange 2000 und anderen Messaging-Systemen übernommen werden. Scalix bietet ein Migra-

[1] wie z.B. McAfee, TrendMicro, ClamAV, F-Secure, BitDefender oder Sophos AntiVirus.

[2] z.B. Vipcom Papageno, Ferrari Fax oder Hylafax

tionstool an, das Nachrichten einschließlich Ordnerstrukturen, Kalender- und Kontaktdaten, Notizen und öffentliche Ordner von Exchange, Lotus Notes, Novell Groupwise sowie IMAP-Servern konvertieren und übernehmen kann. Die Migration kann je nach Größe und Struktur der Umgebung entweder „auf einen Schlag“, „Standort für Standort“ oder „User für User“ im laufenden Tagesgeschäft erfolgen, wobei alle Benutzer auf dem Alt- und Neusystem während der Umstellung weiterarbeiten können. Dies ist selbst in einer Mischumgebung unter Erhalt einer Vielzahl von Groupware-Funktionalitäten möglich.

Fazit

Scalix ermöglicht vor allem für Exchange-Migrationen einen weitgehend reibungslosen Übergang. Outlook wird optimal unterstützt, die realisierte MAPI-Implementierung ist sehr umfangreich. Ein eigener leistungsfähiger Webclient ermöglicht die Online-Nutzung auf verschiedensten Client-Plattformen.

Durch die Nutzung der bewährten HP-OpenMail-Technologie wird eine stabile Basis mit einer Vielzahl von Referenzinstallationen als Grundlage des Systems verwendet.

3.12.4.7 Samsung Contact

Samsung Contact (SC) ist eine umfassende Groupware-Lösung, die für den Einsatz in Unternehmen unterschiedlicher Größenordnungen konzipiert wurde. Das System erlaubt die Verwaltung von einigen hundert bis mehreren zehntausend Benutzern auf einem Server. Die Funktionalität der Software ist weitgehend kompatibel zum Produkt Exchange der Firma Microsoft. Alle Serverkomponenten stehen für Linux (RedHat, Suse) und die meisten kommerziellen UNIX-Derivate (AIX, HP-UX, Solaris) zur Verfügung. Auch auf der Clientseite werden mehrere Betriebssysteme unterstützt. Der SC Java-Client läuft sowohl unter Linux als auch unter Windows. Ein webbasierter Client ermöglicht den Zugriff von jeder webfähigen Plattform. Über einen mitgelieferten MAPI-Provider ist es möglich, vorhandene Outlook Funktionalität (98, 2000, XP) in vollem Umfang zu nutzen.

Samsung Contact baut auf der bewährten *OpenMail*-Technologie von Hewlett-Packard (HP) auf.

Server-System

Die prinzipielle Architektur des Systems ist der folgenden Abbildung zu entnehmen:

Bild 38: Architektur Samsung Contact

Das Serversystem besteht aus mehren voneinander unabhängigen Komponenten, die sich im Sinne einer horizontalen Skalierung auch auf mehrere Server verteilen lassen. Es ist außerdem möglich, mehrere voneinander komplett unabhängige Instanzen auf einem Serversystem zu betreiben. Die folgende Tabelle gibt einen groben Überblick über die Serverprozesse und ihre jeweilige Aufgabe.

Tab. 36: Samsung Contact Komponenten

Komponenten	Funktionsbereich
Service Router	Leitet eine Message an den jeweiligen Service weiter, der zur Verarbeitung einer Message benötigt wird. Die schließt die Abarbeitung von serverseitigen Regeln zur Verteilung oder automatischen Beantwortung von Nachrichten ein.
Local Delivery	Liefert eine Message an eine lokale Mailbox aus.
Internet Mail Gateway	Dient zur Umwandlung einer Nachricht in eine MIME-konforme Internet-Mail.
Remote Client Interface	Dient der Anbindung von Mail-Clients über ein Netzwerk. Diese Art von Verbindung wird z.B. durch den MAPI-Provider und die Java-Clients benutzt. Es handelt sich dabei um eine Single-Socket-Verbindung zwischen den Client und dem Server-Prozess.
Test Service	Ein Test-Service zur Überprüfung des Mail-Routings.

Komponenten	Funktionsbereich
	Dieser generiert eine einfache Antwortmail.
Print Service	Ermöglicht den serverseitigen Ausdruck von Mails.
Request Service	Dient der skriptgesteuerten, serverseitigen Verarbeitung von Nachrichten. Damit lassen sich z.B. Mailing-Listen verwalten.
Directory Synchronisation	Erlaubt die Synchronisation von Directories zwischen mehreren Samsung Contact Servern.
Bulletin Board Service	Dient der Replikation von Bulletin Boards (Shared Folders) zwischen verschiedenen Samsung Contact Servern.
Background Search Service	Dient der asynchronen Suche von Informationen im Message-Store.
Client Directory Access Service	Bereitet die Einträge des zentralen Verzeichnisses auf, um diese z.B. als Globales Adressbuch im Outlook-Client zur Verfügung stellen zu können.
Application Link Service	Erlaubt die Anbindung externer Applikationen, wie z.B. Fax-Gateways.
POP3 Service	Stellt den Inhalt einer Mailbox über das POP3 Protokoll zur Verfügung.
omscan Service	Dient der Konsistenzprüfung des Message-Stores.
Directory Relay Service	Dient der Abfrage von Verzeichnissen auf entfernten Samsung Contact Servern.
Container Access Monitor	Überprüft die Zugriffsrechte für den Message-Store.
Notification Service	Dient der Benachrichtigung von Client-Prozessen beim Eintreten eines Ereignisses (z.B. beim Eintreffen einer neuen Nachricht oder nach dem Auffinden eines Treffers durch den Suchdienst)
LDAP Service	Exportiert das interne Verzeichnis über LDAP in der Version 3. Als LDAP-Server dient OpenLDAP.
Queue Manager	Zentraler Prozess zur sicheren Verwaltung der Message-Queues.
Item Delete Daemon	Hintergrundprozess zum Entfernen gelöschter Nachrichten aus dem Message-Store.
IMAP Service	Stellt den Inhalt einer Mailbox über das IMAP Protokoll zur Verfügung.
SMTP Relay	Dient dem Empfang von Nachrichten über SMTP. Vor der Zustellung auf einen Mailknoten wird der Empfänger im Verzeichnis gesucht. Das SMTP-Gateway unterstützt Anti-Spam-Mechanismen und eine SASL-basierte Authentifizierung.
SMS / Pager Service	Erlaubt den Empfang und die Versendung von SMS bzw. Pager-Nachrichten.

Als Mail-Transport-Agent (MTA) wird standardmäßig sendmail benutzt. Prinzipiell ist auch der Einsatz von Postfix möglich. Als Web-Server für den Webclient und das Administrations-Frontend wird Apache empfohlen.

Samsung Contact unterstützt neben einer Single-Server Installation auch eine verteilte Installation über mehrere Standorte hinweg. Die Mailbox eines Benutzers ist jedoch immer einem Server-Knoten zugeordnet. Das Verzeichnis lässt

sich standortübergreifend replizieren. Die aus dem *Microsoft Exchange*-Umfeld bekannten *Public Shared Folders* werden über Bulletin Boards (BB) realisiert. Diese lassen sich ebenfalls standortübergreifend replizieren, was vor allem bei schmalbandigen Anbindungen zwischen zwei Standorten von Vorteil ist.

Für die Einbindung externer Applikationen an die Groupware-Lösung stehen eine spezielle API zur Verfügung. Diese Schnittstelle wird von Drittanbietern[1] zur Anbindung eines Unified-Messaging-Systems (Voice, Fax) genutzt

In Hinblick auf die Hochverfügbarkeitsfähigkeit wurde Samsung Contact schon mit einem optimierten Systemdesign ausgelegt. Die meisten Systemparameter lassen sich im laufenden Betrieb verändern, ohne dass das Gesamtsystem neu gestartet werden muss. Um sich gegen den hardwareseitigen Ausfall eines Mail-Knoten wirksam zu schützen, ist es ratsam, das System in einem HA-Cluster zu betreiben. Prinzipiell lässt sich jede Cluster-Software auf Samsung Contact anpassen, die eine Übernahme eines gemeinsamen Storage-Nodes erlaubt (HP Service Guard, RedHat Advanced Server, Steeleye, Polyserve, Failsafe, Linux Heartbeat).

Clients

Samsung Contact bietet eine breite Palette an unterstützten Clients an. Neben einem MAPI-Provider zur Anbindung von Microsoft Outlook-Clients existieren noch ein in Java entwickelter Groupware-Client sowie ein entsprechendes Web-Interface. Standardmäßig erfolgt die Anbindung des Clients über das UAL-Protokoll. Dabei handelt es sich um ein einfaches Socket-Protokoll, für das eine offene C- und Java-API existiert. Der Samsung MAPI-Provider und der Web-Client nutzen die C-API, der Java-Client die Java-API.

Alternativ zu den Samsung Clients lassen sich die Inhalte der Postfächer sowie die Standard-Protokolle POP3 und IMAP4 abrufen. Daher kann ein beliebiger Mailclient mit POP3 oder IMAP-Unterstützung für den Abruf und den Versand von E-Mails genutzt werden (Eudora, Evolution, Mozilla, Netscape, Outlook Express). Für den WAP-Zugriff existiert eine angepasste Version eines Web-Clients.

Die Nutzung des Outlook-Clients ist dank der MAPI-Implementierung von Samsung Contact möglich. Es werden alle wesentlichen Funktionalitäten eines Exchange-Servers abgebildet. Dies schließt auch alle wichtigen Groupware-Features ein. SC erlaubt die Vergabe von Zugriffsrechten für andere Benutzer auf einzelne Ordner (Mail, Termine, Kontakte, Aufgaben). Die von Exchange bekannten Public Shared Folder werden in Form der Bulletin Boards zur Verfügung gestellt. Auch die Festlegung von serverseitigen Regeln zur Verteilung von eingehenden Nachrichten und die automatische Erzeugung einer Abwesenheitsnachricht wird unterstützt. Im Falle der Abwesenheit eines Benutzers kann ein Stellvertreter definiert werden, der für diesen Zeitraum entsprechende Zugriffs-

[1] z.B. von der Firma VIPcom (www.vipcomag.de) und von Ferrari (www.ferrari-electronic.de)

rechte erhält. Die Terminierung von Meetings kann, wie bei Microsoft Exchange, über eine Free-Busy-Liste, die im Verzeichnis des Samsung Contact Servers verwaltet wird, erleichtert werden. Für den mobilen Einsatz wurde eine Synchronisation von Offline Foldern implementiert.

Sicherheit

Standardmäßig bietet Samsung Contact keine Verschlüsselung der Nachrichten. Es existieren jedoch Lösungen von Drittanbietern, die eine S/MIME konforme Ende-Zu-Ende Verschlüsselung (Zertifikate) innerhalb von Outlook erlauben (z.B. Entrust). Die Verschlüsselung der Verbindung zwischen dem Client und dem Server (POP3 / IMAP) kann über einen vorgeschalteten SSL-Tunnel erfolgen.

Die Authentifizierung der Benutzer wird über eine PAM-Architektur realisiert. Diese wird sowohl von den Serverprozessen für das UAL-/IMAP-/POP3-Protokoll als auch von den Kommandozeilentools zur Administration genutzt. Neben der Authentifizierung gegen das Samsung Contact Verzeichnis ist eine weitere gegen externe Instanzen möglich. Momentan gehören PAM Module zur Authentifizierung gegen UNIX-Accounts sowie gegen externe Radius- und SMB-Server (Samba) zum Lieferumfang. Samsung Contact erlaubt eine detaillierte Festlegung von Zugriffsrechten auf folgende Server-Ressourcen in Form sog. Access Control Listen (ACLs):

- Bulletin-Boards (Public Shared Folders)
- Verzeichnisse
- Druck Server
- Service-Prozesse
- Skripts des Request Services.

Die Größe des maximal von einem Benutzer nutzbaren Speicherplatzes lässt sich in Form von Quotas limitieren.

Für die Sicherung (Backup) des Message-Stores ist keine spezielle Software nötig. Es kann jedes Produkt genutzt werden, das für das jeweilige Serverbetriebssystem zur Verfügung steht. Das Systemdesign von Samsung Contact erlaubt eine konsistente Sicherung im laufenden Betrieb. Für den Single User Backup/Restore steht ein Kommandozeilentool zur Verfügung. Damit kann ein einzelner Benutzer auf einfache Weise von einem Mailknoten auf einen anderen umgezogen werden.

Für den Schutz vor Viren kann prinzipiell jedes SMTP-basierte Virengateway zum Einsatz kommen (MIME-Sweeper, Trendmicro Viruswall). Das AHN Antivirus Produkt (www.ahnlab.com) ist serverseitig integriert. Neben dem Virenschutz wird auch die serverseitige Filterung von Mails anhand von benutzerdefinierten Mail-Filtern erlaubt. Diese werden über ein Webfrontend konfiguriert. Das SMTP-Relay unterstützt Antispamming nach RFC 2505.

Administration

Die Administration eines Samsung Contact Mail-Knotens kann auf zwei unterschiedliche Arten erfolgen: Zum einen existiert ein einfaches Webfrontend zur Anlage von Benutzern, Verteilerlisten und Verzeichniseinträgen und zum anderen gibt es eine große Fülle von Kommandozeilentools zur Administration sämtlicher Komponenten. Das Webfrontend ist für den täglichen Betrieb konzipiert. Die Kommandozeilenschnittstelle ist in erster Linie zur Automatisierung administrativer Aufgaben geeignet.

Die Administration des Systems lässt sich durch jeden Benutzer steuern, der über administrative Rechte verfügt. Ein zusätzlicher Eintrag im Systemverzeichnis legt fest, ob er als Administrator zugelassen ist.

Migration

Die Migration von einer *Exchange*- oder Outlook-Umgebung nach Samsung Contact ist auf unterschiedliche Arten möglich. Ist die Zahl der Benutzer überschaubar (< 100), so bleibt eine manuelle Übernahme der Mailboxen, Termine, Kontakte und Aufgaben in eine lokale PST-Datei und ein anschließender manueller Transfer in eine serverseitige Ordner-Struktur noch zumutbar. Die Anlage der Mailboxen und Benutzer wird in diesem Fall ebenfalls manuell erfolgen.

In großen Systemumgebungen wird eine manuelle Migration aus Kosten- und Effizienzgründen nicht sinnvoll sein. In derartigen Umgebungen sollte eines der kommerziell erhältlichen Migrationstools genutzt werden. Je nach Hersteller ist dabei eine vollautomatische Übernahme aller Daten einschließlich einer Rekonfiguration des Outlook-Clients möglich. Serverseitig können folgende Informationen migriert werden:

- Benutzer (ohne Passworte)
- Kalendereinträge
- Verzeichniseinträge
- Public Distribution Lists
- Ordnerhierachie inkl. aller Inhalte (Mails, Termine, Tasks, Kontakte)
- Bulletin Boards
- Serverbasierte Regeln
- Access Controll Listen.

Für die Vorbereitung einer solchen Migration ist die Einbindung eines externen Dienstleister mit der entsprechenden Expertise zu empfehlen.

Fazit

Samsung Contact eignet sich als vollwertiger Ersatz für einen *Microsoft Exchange Server*. Es werden alle Groupware-Funktionalitäten eines Exchange-Servers unterstützt. Die Ausnahme bilden Formularanwendungen.

Die Basistechnologie ist seit über 15 Jahren am Markt und verfügt daher über einer große Zahl von Referenzinstallationen.

3.12.4.8 Zusammenfassung

Derzeit existieren unter Linux einige Groupware-Lösungen, die einen ähnlichen Funktionsumfang bieten wie Microsoft Exchange 5.5. Grundsätzlich werden bei den Lösungen zwei verschieden Strategien verfolgt:

- Zugriff auf die Groupware-Server mittels Browser, dynamische Aufbereitung der Daten auf dem Server
- Zugriff mittels spezieller Client-Software auf den Groupware-Server.

Die folgende Tabelle gibt einen Überblick über die wichtigsten Funktionalitäten der unterschiedlichen Groupware-Lösungen.

Tab. 37: Alternative Groupware-Lösungen

	php-Groupware	**Kolab**	**OpenGroupware**	**ex-change-4linux**	**Open-Xchange**	**Scalix**	**Sam-sung Contact**
Outlook-Unterstützung							
Outlook Anbindung	Nein	Anbindung mittels Connectoren	Anbindung mittels Connector „ZideLook“	Anbindung mittels N&H MAPI Service Provider	Bedingt über POP3 oder IMAP	MAPI-Connector	MAPI-Connector
Globales MAPI-Adressbuch	Nein	Ja	Ja	Ja	Nein	Ja	Ja
Mail	Nein	Ja	Ja	Ja	Ja	Ja	Ja
Kontakte	Nein	Ja	Ja	Ja	Nein	Ja	Ja
Aufgaben	Nein	Ja	Ja	Ja	Nein	Ja	Ja
Termine	Nein	Ja	Ja	Ja	Nein	Ja	Ja
Andere Client-Systeme							

	php-Group ware	Kolab	OpenGroup ware	ex-change-4linux	Open-Xchange	Scalix	Sam-sung Contact
Brow-serba-sierter Zugriff	Ja	Nein	Ja	Nein	Ja	Ja	Ja
Linux-basierte Client-syste-me	Nein	KDE Kon-tact	Ab der kommenden KDE Kon-tact-Version 3.4[1]. Zur Zeit mittels POP und IMAP.	Bedingt über POP3 oder IMAP	KDE Kontact, Konque-ror, Mo-zilla Ca-lender	Voraus sicht-lich ab Früh-jahr 2005 iCal-basier-te Clients. Zur Zeit mittels POP und IMAP.	Java-Client und mit-tels POP und IMAP.
Palm-Pilot-Syn-chroni-sation	Nein	Ja, mittels KDE- und Out-look-Client	Ja, mittels Outlook-Client und zukünftig mittels KDE-Kontact.	Mittels Outlook	Nein	Mittels Out-look.	Mittels Outlook
Groupware-Funktionalitäten							
Web-Portal	Ja	Nein	Ja	Nein	Ja	Ja	Ja
Kontakt verwal-tung	Ja	Ja	Ja	Mittels Adress-verwal-tung	Ja	Ja	Ja
Termin-verwal-tung	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Aufga-ben-verwal-tung	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Notizen	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Der aufgezeigte Funktionsumfang der vorgestellten Groupware-Lösungen macht deutlich, dass zum jetzigen Zeitpunkt adäquate linuxbasierte Produkte zur Verfügung stehen. Aufgrund der rapiden Entwicklung im Bereich der Groupwarelösungen kann der Überblick nur eine temporäre Bestandsaufnahme darstellen, für

[1] http://www.kontact.org/groupwareservers.php

konkrete Migrations- bzw. Einführungsprojekte ist eine separate Betrachtung unerlässlich. Neben der technischen Fortentwicklung ist ein weiterer erfreulicher Trend in Hinblick auf die Lizensierung der Lösungen zu beobachten. Ursprünglich kommerzielle Groupwarelösungen wurden als freie Software unter GPL zur Verfügung gestellt und nach dem OpenSource-Modell weiterentwickelt. Sowohl die OpenGroupware.org- als auch die Open-Xchange-Lösung entwickelten sich aus ursprünglich rein kommerziellen Produkten und stehen mittlerweile unter GPL bereit.

Die Auswahl einer geeigneten Groupware-Lösung bedingt sich durch die folgenden Kriterien:

- Nutzung des Microsoft-Outlook-Clients
- Einsatz in heterogenen Client-Umgebungen, gleichzeitige Nutzung von linuxbasierten Client-Systemen und des Outlook-Clients
- Einsatz einer webbasierten Lösung.

Für die weitere Nutzung von Outlook als Clientsystem kommen prinzipiell die Produkte Kolab, OpenGroupware, Exhange4linux, Samsung Contact und Scalix in die nähere Auswahl. Die genannten Lösungen bieten alle die Möglichkeit mittels des Outlookclients auf die Mail- und Groupwarefunktionalitäten zuzugreifen.

Für Organisationen in der Größenordnung von mehreren hundert Benutzern bieten alle aufgeführten Groupwarelösungen stabile Plattformen, die sich auch schon in der Praxis bewährt haben. Samsung Contact und Scalix, die beide auf der HP-OpenMail-Technologie basieren und eine gute Outlook-Unterstützung bieten, stellen insbesondere für größere Organisationen eine viel versprechende Alternative dar. Im Gegensatz zu Scalix fokussiert sich jedoch Samsung Contact auf Lösungen mit 500 und mehr Nutzern[1]. Die guten Skalierungsmöglichkeiten der Systeme lassen auch einen Einsatz in Organisationen mit mehreren 10.000 Mitarbeitern zu.

Heterogene Client-Landschaften

Organisationen, die auf der Client-Seite unterschiedliche Betriebsysteme einsetzen und einen eigenständigen Groupwareclient (z.B. Outlook, Kontact, usw.) einsetzen wollen, haben beispielsweise die Möglichkeit Kolab, OpenGroupware oder Samsung Contact einzusetzen. Es hat sich gezeigt, dass die Entwicklung im Bereich der Groupwareserver und –client sehr schnell fortschreitet und in absehbarer Zeit voraussichtlich weitere Groupwarelösungen heterogene Clientsysteme unterstützen werden.

Webbasierte Lösungen

Für Organisationen, die einen webbasierten Lösungsansatz bevorzugen, bieten die unter GPL stehenden Groupware-Lösungen phpGroupware, OpenGroupware

[1] Samsung Contact: http://www.samsungcontact.com/de/

und Open-Xchange einen sehr großen Funktionsumfang an. OpenGroupware erlaubt zusätzlich auch eine Anbindung an den Outlookclient.

3.12.5 Fortführende Migration

3.12.5.1 Exchange 2003

Neuerungen

Die gravierenste Architekturänderung, die mit dem Erscheinen von Exchange 2000 gegenüber Exchange 5.5 vorgenommen wurde, ist die Verlagerung des Exchange Verzeichnisdienstes ins Windows 2000 Active Directory (AD). Ab der Version Exchange 2000 verfügt Exchange somit über keinen eigenen Verzeichnisdienst mehr und benötigt zwingend ein Active Directory.

Darüber hinaus kann Exchange 2003 nicht auf Windows NT Servern, sondern nur auf Windows 2000 Servern mit Service Pack 3 oder höher oder aber Windows 2003 installiert werden.

Hinsichtlich der bisherigen Exchange 5.5 Struktureinheit „Standort“ ergeben sich folgende Änderungen:

- Die Verzeichnisreplikation der Benutzerdaten obliegt einzig dem Active Directory; die dort eingeführten Standorte (Sites) sind nicht mit denen aus Exchange 5.5 zu verwechseln.
- Exchange Server werden verwaltungstechnisch in „Administrative Gruppen“ strukturiert.
- Darüber hinaus werden Exchange Server in Routinggruppen eingeteilt, die nicht mit den „Administrativen Gruppen“ übereinstimmen müssen. Die Routinggruppen bilden vielmehr die Sites ab, die unter Exchange 5.5 genutzt wurden, um die Replikation der Server auf die einzelnen Standorte zu beschränken.

Da sich auf den Exchange Servern kein Verzeichnisdienst mehr befindet, bedarf es eines Dienstes, der umfangreiche Informationen über Domänengrenzen hinweg bereithält, dem Global Catalog (GC, globaler Katalog). Der GC kann nur auf Windows Domain Controllern bereitgestellt werden. Er beinhaltet Informationen über alle Objekte einer Windows Gesamtstruktur (forest), jedoch nur ausgewählte Attribute. Diese Auswahl der Attribute kann individuell auf die einzelnen Bedürfnisse angepasst und verändert werden. Aktuelle Clients (z.B. Outlook 2000 oder höher) können Informationen direkt vom GC beziehen, ältere Clientversionen werden durch den Exchange Server bedient, der als Proxy die Anfrage weiterleitet.

Die Verteilerlisten in Exchange 5.5 wurden durch E-Mail-fähige Gruppen im Active Directory ersetzt. Im AD existieren reine Verteilergruppen und Sicherheitsgruppen. Sicherheitsgruppen sind auch E-Mail-fähig, so dass sich Redundanzen vermindern lassen. Bekanntlich befinden sich im AD Gruppen mit verschiedenen Gültigkeits-(Sichtbarkeitsbereichen): Domänen (global und lokal) und universelle

Gruppen (nur im Native Mode der Domäne). Nur die universellen Gruppen sind über Domänengrenzen hinweg sichtbar.

In Exchange 2003 wird der Entwurf nicht mehr durch das Administrationsmodell der Exchange Umgebung bestimmt, da Server durch Administrative Gruppen und Routinggruppen separat organisiert werden können. Diese Trennung ist allerdings nur möglich, wenn Exchange 2003 selbst im Native Mode ausgeführt wird, also keine 5.5- Server mehr im Einsatz sind oder sein werden.

Exchange ab der Version 2000 bietet ein Richtlinienmodell für die Verwaltung. Dieses ermöglicht es den Administratoren, in einem Vorgang Optionen für eine Objektgruppe (z.B. Benutzerpostfächer, Server und öffentliche Ordner) zu ändern.

Der Transport zwischen den Exchange 2003 Servern erfolgt nun per SMTP (Simple Message Transport Protocol).

Der Routinggruppen-Connector von Exchange 2003 ersetzt den Standort-Connector.

Folgende Konnektoren stehen zur Verfügung:

- X.400 Connector (ist nur noch in der Enterprise Version von Exchange 2000/2003 enthalten)
- Microsoft Mail Connector
- CC:Mail Connector
- Lotus Notes Connector
- Novell Groupwise.

Pro Exchange 2003 (in der Enterprise Version) Server lassen sich bis zu vier Speichergruppen mit bis zu vier Datenbanken anlegen. Dies hat insbesondere bezüglich der Datensicherung und Wiederherstellung Vorteile.

- Die Indizierung der Exchange Datenbank ist nun möglich.
- Exchange Cluster können im „Aktiv-aktiv“ Modus betrieben werden.
- Outlook Web Access (OWA) unterstützt nun WebDAV (Web Distributed Authoring and Versioning), eine Weiterentwicklung von HTTP 1.1. Hinsichtlich OWA ist es vorteilhaft, dass Exchange Server als Frontend- und BackEnd konfiguriert werden können, so dass OWA Server selbst keinen Datenbestand halten.

Des Weiteren können nun

- Chat-Dienste
- und Instant Messaging Dienste

installiert werden.

Durch die separate, neue Produktvariante „Live Communication Server“ werden unter anderem Audio- und Videokonferenzen möglich.

Das Entwicklungsumfeld von Exchange 2003 wird durch

- die Verbesserung von CDO (Collaboration Data Objects)
- erweiterte Workflow Mechanismen
- die Einführung von XML
- und die erhöhte Integration von IIS (Internet Information Server) und ASP (Active Server Pages)

aufgewertet.

Bemerkungen zur Migration

Die Migration von Exchange 5.5 nach Exchange 2000/2003 ist ein komplexer Vorgang, der einer intensiven Vorbereitung mit einer Konzeptionserstellung, einer Migrationsplanung und produktionsnaher Tests bedarf. Dieser Leitfaden kann diese Aufgaben nicht vollständig behandeln, auf einige wichtige Aspekte einer Migration soll jedoch hingewiesen werden.

Durch den Umstand, dass Exchange 2003 nur verwendet werden kann, wenn ein Windows Active Directory vorhanden ist, ergeben sich u.a. folgende technischen Randbedingungen:

- Die Domänenstruktur von Windows Active Directory hat Auswirkungen auf Exchange 2003. So bildet die Gesamtstruktur (forest) die Grenzen der Exchange Organisation.
- Die gewählte OU-Struktur der Windows 2003 Domänen hat primär keinerlei Auswirkungen auf die Migration von Exchange 2003.
- Die Einführung von Exchange 2003 bedarf einer Schemaerweiterung des Active Directory. Diese Erweiterung kann durchgeführt werden, ohne Exchange 2003 selbst installieren zu müssen (Stichwort: forestprep). Des Weiteren muss die betroffene Domäne vorbereitet werden (Stichwort: domainprep).
- Der Betriebsmodus der Windows Domänen (Native vs Mixed Mode) beeinflusst die Verfügbarkeit von universellen Gruppen und somit die Sichtbarkeit von E-Mail-Verteilern.
- Eine *Exchange 2003-Aktualisierung* kann nur durchgeführt werden, wenn zuvor eine *Betriebssystemaktualisierung* durchgeführt wurde. Exchange 2003 kann nicht auf Windows NT 4 Servern installiert werden. Dagegen kann Exchange 5.5 auf Windows 2000 Servern laufen.
- Eine *Betriebssystemaktualisierung* eines Exchange Servers bedarf einer sorgfältigen Untersuchung (Service Packs etc.), insbesondere dann, wenn zusätzliche Software von Drittherstellern (z.B. Virenschutz) installiert ist.

- Bevor die erste *Exchange 2000-Aktualisierung* durchgeführt wird, müssen die Exchange Server Mitglied einer Windows 2000 Domäne bzw. einer Gesamtstruktur sein.
- Benutzer müssen sich an einem Active Directory anmelden, wenn sie Exchange 2000 nutzen wollen bzw. sollen.

Die Komplexität des gesamten Portfolios von Migrationsszenarien (komplexe NT Domänenmodelle, mehrere Exchange Organisationen, Exchange in Ressourcendomänen, Exchange auf Domain Controllern, verteilte Standorte, Windows Gesamtstruktur etc.) wird im Rahmen dieses Leitfadens nicht dargestellt. Abschließend sei aber noch auf ausgewählte Werkzeuge hingewiesen, die die Migration bzw. die Koexistenz erleichtern können:

Active Directory Connector (ADC) ermöglicht das Replizieren einer Hierarchie von Verzeichnisobjekten zwischen einem Exchange Server 5.5-Verzeichnis und dem Active Directory. Damit spielt ADC eine wichtige Rolle bei der Migration von Exchange 5.5 auf Exchange 2000. Für die Migration von Exchange 2003 muss der ADC von der Exchange 2003 Version verwendet werden. Zu beachten ist, dass zwei Versionen des ADCs existieren (auf der Windows 2000 CD und der Exchange 2000 CD). Hinsichtlich der Migration nach Exchange 2000 ist letztere Version relevant.

Der Standortreplikationsdienst (SRS) ermöglicht es, dass Exchange 2003 Server die Exchange 5.5 Konfiguration replizieren.

Die nachfolgende Kompatibilitätsmatrix zeigt in einer Übersicht die verschiedenen unterstützten Kombinationen von Exchange 5.5, Exchange 2000, Exchange Server 2003 und Windows Server 2003.

Tab. 38: Kompatibilitätsmatrix – Exchange[1]

	Installation und Ausführung von Exchange unter		**Unterstützte Active Directory-Umgebungen**	
Exchange-Version	Windows 2000 SP3 oder höher	Windows Server 2003	Windows 2000 SP3 oder höher	Windows Server 2003
Exchange 5.5 SP3	Ja	Nein	Ja	Ja
Exchange 2000 SP2	Ja	Nein	Ja	Ja
Exchange 2000 SP3	Ja	Nein	Ja	Ja
Exchange 2003	Ja	Ja	Ja	Ja

[1] Deutsches Whitepaper von Microsoft „Microsoft Exchange Server – Kompatibilität mit Windows Server 2003“,(http://www.microsoft.com/germany/library/resourcesmod/exchange+titanium+und+windows+server+2003.doc)

Die folgende Abbildung skizziert die Möglichkeiten gemischter Umgebungen.

Bild 39: Gemischte Umgebungen – Exchange [1]

Zu den Neuerungen von Exchange 2003 gehören:

- Outlook Mobile Access ist im Exchange Server 2003 enthalten. Outlook Mobile Access bietet Benutzern von mobilen Geräten Zugriff auf ihre persönlichen Informationen.
- Im Exchange Server 2003 ermöglicht der Internet Information Server (IIS Version 6 in Windows 2003) eine neue Form der Kommunikation zwischen Outlook und Exchange, die als „RPC über HTTP“ bezeichnet wird. Auf diese Weise kann ein Outlook-Benutzer seine Daten sicher mit einem Exchange Server 2003 über eine HTTPS-Verbindung direkt synchronisieren.
- Die Unterstützung für Clustering in Windows 2000 Advanced Server ist auf zwei oder vier Knoten in der Datacenter Version beschränkt. Mit Windows 2003 und Exchange 2003 können nun wahlweise Cluster mit bis zu acht Knoten mit mindestens einem passiven Knoten realisiert werden. Hierfür ist jedoch für Exchange Server 2003 und Windows Server 2003 die Enterprise Edition Voraussetzung.

[1] Quelle: Deutsches Whitepaper „Microsoft Exchange Server – Kompatibilität mit Windows Server 2003“

- Exchange 2003 verwendet unter Windows 2003 den Datenträgerschattenkopie-Dienst (VSS) und ermöglicht so kürzere Sicherungs- und Wiederherstellungszeiten für Exchange Umgebungen.

Outlook Web Access Funktionalitäten

Auch die Version des Exchange 2003 Servers bietet, neben dem klassischen Clientzugriff mittels POP, SMTP und der MAPI-Schnittstelle, auch die Möglichkeit des webbasierten Zugriffs. Der Zugriff auf die Mail- und Groupwaredaten kann dann mittels Webbrowser erfolgen.

Für die vollständige Nutzung des Outlook Web Access (OWA) ist jedoch der Einsatz eines Microsoft Internet Explorers eine zwingende Voraussetzung. Nutzer, die alternative Browsertypen (Firefox, Opera, Mozilla, usw.) einsetzen, unterliegen zum Teil starken Einschränkungen bei der Nutzung der Exchange 2003 Webschnittstelle. Grundsätzlich kann bei der Nutzung des OWA zwischen zwei unterschiedlichen Ausprägungen unterschieden werden, zum einen gibt es die Basis- und zum anderen die Premium-Version. Die Basis-Version wird durch jeden Browsertyp unterstützt, der Nutzer muss jedoch Einschränkungen im Funktionalitätsumfang hinnehmen. Die Premium-Version, die den Internet Explorer und die Unterstützung von aktiven Inhalten (z.B. ActiveX, Active Skripting) innerhalb des Browsers benötigt, unterstützt das gesamte Funktionalitätsspektrum des OWA.

Die folgende Tabelle zeigt einen Ausschnitt der wichtigsten Funktionalitäten und der Unterstützung von unterschiedlichen Browsertypen.

Tab. 39: Outlook Web Access[1]

Outlook Web Access Funktionalitäten	Internet Explorer 6 Service Pack 1	Internet Explorer 5	Alternative Browsertypen
E-Mail, Kalender, Aufgabenliste	X	X	X
Microsoft Outlook 2003 “look and feel”	X	X	-
Mail als ungelesen kennzeichnen	X	X	-
S/MIME-Unterstützung	X	-	-
Weiterleiten von Besprechungsanfragen	X	X	X
Hinzufügen von Kontakten	X	X	-
Kontextmenüunterstützung	X	X	-
Unterstützung von „persönlichen Aufgaben“	X	X	X

[1] X: Funktion wird unterstützt; -: Funktion wird mit dem Browsertyp nicht unterstützt

Weiterführende Angaben über den Umfang bzw. die Beschränkung von Funktionen bezüglich der Browsertypen kann auf den Internetseiten[1] von Microsoft nachgelesen werden.

Alternative Clientsysteme

Für den Zugriff auf die Messaging- und Groupwarelösung Exchange 2003 steht neben den Outlook-Clients und dem Zugriff über Outlook Web Access auch eine Client-Lösung für linuxbasierte Desktopsysteme zur Verfügung. Mittels des ursprünglich von Ximian entwickelten Evolution-Client[2] stellt Novell einen Groupwareclient bereit, der sich mit der Microsoft Exchange 2000/2003 verbinden lässt. Die Anbindung erfolgt mittels des Ximian-Connectors. Dieser ursprünglich kommerzielle Connector wurde im Mai 2004 durch Novell unter der GPL veröffentlicht.

Der Zugriff auf Exchange wird bei dem Evolution-Client mittels der Protokolle WebDAV und IMAP realisiert. Der Zugriff auf zentrale Verzeichnisdienste bzw. Adressbücher kann mittels LDAP erfolgen. Nutzer können mit dem Clientsystem unter anderem folgende Funktionalitäten

- Mail,
- persönliche Adressbücher,
- globale Adressbücher,
- Kalender,
- Aufgabenordner,
- persönliche und öffentliche Ordner,
- Abwesenheitsnachrichten,
- Ressourcenverwaltung,
- und Palm-Synchronisation

nutzen. Insgesamt werden von Evolution zahlreiche gängige Protokolle unterstützt, für den Zugriff auf Emails können Protokolle wie POP3, IMAP, IMAPS und SMTP verwendet werden. Die Verwaltung von Terminen erfolgt mittels des iCalender-Standards, Adress- und weitere Informationen werden mittels der vCard-Unterstützung realisiert. Evolution ermöglicht auch die sichere Übertragung von Emails durch die Realisierung der Signatur und der Verschlüsselung mittels GPG (GNU Privacy Guard) und S/MIME.

Die unter GPL lizenzierte Lösung bietet einen vollwertigen und komfortablen Mail- und Groupwareclient an, die Nutzerführung und die optische Anmutung lässt auch die Verwendung durch ehemalige Outlook-Nutzer sehr einfach erscheinen.

---

1 http://www.microsoft.com/exchange/techinfo/outlook/OWAandIE.asp

2 Weiterführende Informationen über Evolution: http://gnome.org/projects/evolution/

Sicherheit

Microsoft bietet mit dem Exchange 2003 auch notwendige Maßnahmen zur Absicherung der Mail- bzw. Groupwareumgebung. Es stehen verschiedene Möglichkeiten zur Absicherung zur Verfügung, unter anderem sind das:

- Einschränkung der Serverdienste
- Konfiguration des Outlookclients
  - Blockieren von Anlagen in Outlook, als Mittel gegen Virenübertragung
  - Junk-E-Mail-Filter
- Verwendung von eingeschränkten Verteilerlisten und der Einsatz von Filterlisten für Absender, Empfänger und Verbindungen
- Einsatz der SSL/TSL-Verschlüsselung beim Zugriff auf Outlook Web Access
- Installation von Antivirenprogrammen von Drittanbietern.

Eine umfangreiche Dokumentation[1] und technische Beschreibung zur Absicherung von Microsoft Exchange 2003-Umgebungen wird vom Hersteller bereitgestellt.

Administration

Die Administration einer Exchange 2003-Umgebung erfolgt mit dem Exchange-System-Manager. Der Exchange-System-Manager ist eine spezielle Microsoft Management Console (MMC), die zur Verwaltung der jeweiligen Exchange-Organisation dient. Im Rahmen einer Standardinstallation von Exchange 2003 werden auch automatisch die Komponenten für den Exchange-System-Manager auf einen Server installiert.

Der Exchange-System-Manager stellt eine graphische Benutzerschnittstelle für Administratoren dar, mittels des Managers lassen sich alle Bereiche der Exchange-Serververwaltung administrieren. Im Rahmen der Administration mittels der Managementkonsole können unter anderem folgenden Objekte verwaltet werden:

- Öffentlicher Ordner
- Server
- Routing
- Richtlinien
- globale Einstellungen
- usw..

[1] Exchange Server 2003-Sicherheitshandbuch
http://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=6A80711F-E5C9-4AEF-9A44-504DB09B9065

Mit einer weiteren Microsoft Management Console-Snap-In, dem Active Directory-Benutzer und -Computer werden Empfänger verwaltet. Active Directory-Benutzer und -Computer ist ein Standardbestandteil von Microsoft Windows Server-Betriebssystemen ist. Bei der Installation von Exchange 2003 werden jedoch die Funktionen von Active Directory-Benutzer und -Computer automatisch um Exchange-spezifische Aufgaben erweitert. In Bezug auf die Empfänger können unter anderem die folgenden Aufgaben

- Erstellen von Empfängern
- Erstellen von Postfächern
- Verschieben von Postfächern
- Löschen von Postfächern
- Festlegen einer E-Mail-Adresse
- Konfigurieren von Exchange-Features

bearbeitet werden.

Fazit

Die neueste Version der Microsoft Exchange Lösung verfügt über zahlreiche neue Funktionalitäten gegenüber Exchange 5.5. Die herausragenste ist die Einbindung der Mail- und Groupwarelösung in das Active Directory, somit ist eine Umstellung auf Exchange 2003 auch immer mit der Implementierung eines Active Directorys verbunden. Da es sich dabei um eine strategische Entscheidung handelt, wird an dieser Stelle nochmals auf die technischen Betrachtungen zum AD in Kapitel 3.7.3 verwiesen.

Die Vorteile der neusten Version der Exchange-Lösung gegenüber der Version 5.5 liegen unter anderem in einer verbesserten Skalierbarkeit und Clusterfähigkeit. Diese verbesserten Funktionalitäten sind insbesondere im Rahmen einer Serverkonsolidierung relevant. Neben den architektonischen Änderungen bietet Exchange 2003 auch eine wesentlich verbesserte Version des Outlook Web Access an. Die neueste Version des Outlook Web Access bietet einen webbasierten E-Mail-Client mit einem umfassenden Funktionsumfang und verfügt beispielsweise über die Unterstützung für Nachrichtenregeln, eine Rechtschreibprüfung und unterstützt signierte und verschlüsselte E-Mails. Der Einsatz des Outlook Web Access ermöglicht auch den Zugriff von linuxbasierten Clientsystemen aus, die Verwendung von alternativen Browsersystemen schränkt jedoch die unterstützten Funktionalitäten für den Nutzer ein. Neben dem Zugriff mittels Outlook-Client kann der Zugriff auch über weitere beliebige Mailclients mittels der Protokolle SMTP. IMAP und POP3 erfolgen. Über diese Protokolle besteht jedoch nur der Zugriff auf die Mail- und nicht auf erweiterte Groupwarefunktionalitäten. Der Zugriff auf die Groupwarefunktionalitäten kann jedoch auch mittels des linuxbasierten Evolutionclients erfolgen.

3.13 Office / Desktop

3.13.1 Überblick

Im Zentrum der betrachteten Desktop-Anwendungen stehen die Office-Suiten mit ihren Standard-Anwendungen, im Leitfaden vertreten durch Microsoft Office und OpenOffice.org/Sun StarOffice (OOo/SO). Die 2003er-Version von Microsoft Office leitet eine Entwicklung ein, die in mehrerlei Hinsicht zu einer Neubewertung der Migrationsoptionen in dieser Anwendungsgattung führen wird. Antrieb dieser Entwicklung ist die Verwendung und Offenlegung von XML-Dateiformaten durch Microsoft, die den bisher verwendeten binären Dateiformaten prinzipiell vergleichbar sind. Da OOo/SO bereits seit einigen Jahren ausschließlich XML-basierte Dateiformate einsetzt, könnte auf dieser Basis der Datenaustausch zwischen beiden Suiten deutlich erleichtert werden.

Ein erleichterter Datenaustausch spielt nicht nur für die Aufwände und Komplikationen von Migrationsprojekten eine Rolle, sondern insbesondere auch für den auf Dauer angelegten Betrieb gemischter Umgebungen, in denen beide (und ggf. weitere) Produkte eingesetzt werden. Eine solche gemischte Umgebung kann innerhalb einer Organisation gezielt herbeigeführt werden, sie kann sich aber auch ohne eigenes Zutun ergeben. Die geschieht dann, wenn eine andere Organisation sich für ein alternatives Produkt entscheidet, mit dieser Organisation aber ein reger Austausch von Dokumenten stattfindet.

XML ist die gegenwärtig konkurrenzlose technologische Plattform, um in solchen Szenarien Interoperabilität zwischen den Office-Suiten herzustellen, und damit zugleich die Kooperation der verschiedenen (Teil-) Organisationen zu erleichtern. Idealerweise rückt die Normierung von gemeinsam genutzten XML-Dateiformaten in den Vordergrund, und die Bedeutung des jeweils zu seiner Bearbeitung verwendeten Werkzeugs verliert an Bedeutung.

Die technische Betrachtung der Desktop- und ganz besonders der Office-Anwendungen trägt dieser Entwicklung Rechnung und richtet ein besonderes Augenmerk auf die neuen Interoperabilitätsperspektiven, die sich aus der Verwendung von XML-Dateiformaten ergeben. Dabei werden einerseits die prinzipiellen technologischen Möglichkeiten diskutiert, und andererseits die verfügbaren Anwendungen daraufhin untersucht, in welchem Maße sie diese Möglichkeiten bereits ausschöpfen, und wo sie noch Entwicklungspotentiale bieten.

Dabei zeigt sich: vom Idealzustand, in dem sich eine Reihe von Produkten um ein normiertes XML-Dateiformat gruppiert, welches aus einer Reihe ausgereifter Alternativen ausgewählt werden kann, ist die Realität noch ein gutes Stück entfernt.

Die Ablösung des Microsoft-Desktop als ganzes hängt letztendlich maßgeblich davon ab, ob einerseits eine MS Office durch OOo/SO abgelöst werden kann, ob andererseits benötigte Windows-Anwendungen langfristig als Linuxanwendungen verfügbar sein werden oder wie gut sich diese zwischenzeitlich auf Linux-

Desktop als Windows-Anwendungen bereitstellen lassen. Dies bedarf allerdings einer individuellen Untersuchung.

3.13.2 Einleitung

Der Desktop ist die für die Benutzer sichtbare Schnittstelle, die ihnen ihre Werkzeuge und Anwendungen für die tägliche Arbeit zur Verfügung stellt. Im Vordergrund steht dabei die Arbeit mit dem Microsoft Office Paket (MS Office). Daneben stehen den Benutzern aber auch diverse andere Standard-Werkzeuge zur Verfügung auf deren Funktionalitäten auch nach einer Migration nicht verzichtet werden kann. Letztendlich gibt es noch eine Reihe von Fachanwendungen, die mehr oder weniger stark in den Desktop integriert sind und bei denen es sich häufig um Anwendungen handelt, die Windows als Betriebssystem voraussetzen und die nicht ohne weiteres unter Linux ausgeführt werden können bzw. für die es keine unter Linux lauffähige Version gibt.

Im Vordergrund der nachfolgenden technischen Betrachtungen steht die Migration der Office-Anwendung mit ihren verschiedenen Teilmodulen. Wie sich schon in der Version 1 des Migrationsleitfadens gezeigt hat spielt dabei die Interoperabilität der Anwendungen eine wesentliche Rolle. Dies zum einen hinsichtlich der Migration von bestehenden Dokumenten und deren Weiternutzung und zum anderen hinsichtlich dem Austausch und der gemeinsamen Bearbeitung von Dokumenten. Mit der Einführung von XML-Dateiformaten als Alternative zu den bestehenden Binär-Formaten (doc, xls usw.) und insbesondere mit der zusätzlichen Einführung des XML-Dateiformates jetzt auch in Word (als Alternative zum Binär-Formate .doc) in Microsoft Office 2003 gilt es die Frage nach der Interoperabilität zwischen den Office Suiten Office 2003 und OOo/SO, in der schon seit langem ein anwendungsübergreifendes XML-Dateiformat verwendet wird, bezüglich des Dokumentenaustausches neu zu untersuchen. Daher werden in der vorliegenden Version des Migrationsleitfadens die XML-Implementationen bezüglich des Dateiformates für beide Anwendungen genauer unter die Lupe genommen. Das heißt, für die jeweiligen Anwendungen werden die Form, in der hier XML-Dokumente verwendet werden untersucht und anschließend in einer Gegenüberstellung betrachtet, welche Auswirkungen (Vorteile und Nachteile) dies auf den Dokumentenaustausch zwischen den Anwendungen hat.

Die Fachanwendungen bedürfen einer besonderen Betrachtung, die eher im Zusammenhang mit der Entwicklung plattformunabhängiger Software zu sehen ist und über die Betrachtung der Basissoftwarekomponenten hinausgeht. Neben der reinen Office-Migration sind noch weitere Desktopanwendungen, wie z.B. Microsoft Projekt, zu betrachten. Letztendlich dürfen die Microsoft Anwendungen, auf dem Desktop, die nicht ohne weiteres abgelöst werden können, nicht außer Acht gelassen werden. Hierzu werden Möglichkeiten untersucht, diese unter Linux zu nutzbar zu machen.

Die technischen Betrachtungen untergliedern sich damit wie folgt:

- XML und Interoperabilität zwischen Office-Anwendungen
  Eine Grundsätzliche Betrachtung
- Ausgangslage
  MS Office 97/2000
- Ablösende Migration von MS Office 97/2000
  Ablösung durch OpenOffice.org 1.1.x bzw. StarOffice 7 mit Ausblick auf die kommenden Versionen
- Fortführende Migration von MS Office 97/2000
  Fortführung der Microsoft Produktlinie durch Office 2003
- Interoperabilität auf der Basis von XML-Dateien
  Als Teil der Gesamtbewertung der Ergebnisse der Office-Migrationsbetrachtungen
- Weitere Desktopanwendungen
  Mail-Clients, Webbrowser, Graphikprogramme u.a.
- Windows-Anwendungen unter Linux
  Windows-Emulationen unter Linux

3.13.3 XML und Interoperabilität zwischen Office-Anwendungen

In allen Migrationsszenarien, ganz gleich ob ablösende oder fortführende Migration, ist die Kompatibilität zwischen der alten und der neuen Anwendung eine entscheidende Herausforderung. Kann die neue Anwendung die Daten der alten Anwendung unmittelbar importieren? Oder sind Vor- bzw. Nacharbeiten oder explizite Konvertierungsschritte notwendig? Wie können sie bewerkstelligt werden? Welche Informationen gehen dabei verloren?

Soll sich eine Migration über einen längeren Zeitraum erstrecken oder sollen nur Teile einer Organisation migriert werden, gewinnt darüber hinaus die Rückwärts-Kompatibilität an Bedeutung. Wie können Dokumente, die mit der neuen Anwendung erzeugt oder bearbeitet wurden, mit der alten Anwendung weiter verarbeitet werden? Entstehen durch die wechselseitige Bearbeitung eines Dokumentes mit verschiedenen Anwendungen oder Anwendungs-Versionen ("Roundtrip") möglicherweise Fehler, die sich schneeballhaft vergrößern?

Die gleichen Fragen stellen sich auch dann, wenn neben der Migration innerhalb einer Organisation auch die Interoperabilität mit anderen Organisationen angestrebt wird.

Auf eine Vielzahl von Kompatibilitätsfragen zeichnen sich gegenwärtig mögliche neue Antworten ab. Grund dafür ist zum einen die wachsende Verbreitung von XML als Dateiformat. XML und seine generellen Vorteile wurden im Kapitel 3.8 beschrieben und werden in den folgenden Kapitel 3.13.3.1, 3.13.3.2, 3.13.5.2, 3.13.6.3 und 3.13.7.2 näher untersucht. Ein weiterer Grund ist aber auch die wachsende Aufmerksamkeit, mit der die Interoperabilität insbesondere von Einrichtungen der Öffentlichen Verwaltung inzwischen betrachtet wird, sowohl unter-

einander wie mit Dritten. Die Etablierung geeigneter Standards wird auf Bundesebene beispielsweise durch SAGA ebenso vorangetrieben wie auf EU-Ebene, etwa durch das IDABC-Programm (Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens), und rückt damit auch verstärkt ins Bewusstsein der Anbieter. Ein gemeinsamer Tenor aller Standardisierungsaktivitäten ist übrigens wiederum die Verwendung von XML als Format für den Datenaustausch.

Die folgenden beiden Abschnitte gehen der Frage nach, welche Beiträge XML grundsätzlich zur Interoperabilität von Office-Anwendungen leisten kann. Das Kapitel 3.13.7.1 betrachtet vor diesem Hintergrund die Eignung der verfügbaren Formate und Anwendungen.

XML dient jedoch nicht nur der Interoperabilität der Office-Suiten untereinander, sondern hat unabhängig davon noch einen weiteren Nutzen. XML erlaubt eine stärkere Integration von Office- ("Desktop"-) Dokumenten und -Werkzeugen in das Informationsmanagement der umgebenden Organisation, im Sinne der in Kapitel 3.9.3 skizzierten Prozessintegration.

Traditionell befinden sich in Office-Dokumenten häufig Informationen, die der Sache nach eigentlich in eine zentrale Datenbank gehören oder die von einem Dokumentenmanagement-System zur Qualifizierung dieser Dokumente herangezogen werden müssten. Beispielsweise kann ein Office-Dokument Verweise auf Aktenzeichen, Kundennummern, Verordnungen oder andere Dinge enthalten, die nicht nur für die Bearbeitung, Ablage und Wiederauffindbarkeit des Dokumentes von entscheidender Bedeutung sind, sondern die auch eine Bedeutung für die Prozesse haben, in deren Kontext sie verarbeitet werden.

Solche Informationen aus herkömmlichen Office-Dokumenten zu gewinnen und nutzbar zu machen ist jedoch aufwändig. Die Unterstützung der aktuellen Textverarbeitungen für XML-Dateiformate erlaubt jedoch den Einsatz von Standard-Werkzeugen und bietet so auf der technischen Ebene einen vereinfachten Zugriff auf die Dokumente und ihre innere Struktur. Darüber hinaus bieten sie unterschiedlich ausgeprägte Möglichkeiten, Textpassagen semantisch zu kennzeichnen und leisten damit einen wichtigen Beitrag zur Backend-Integration. Das Kapitel 3.9 betrachtet die aktuellen Produkte auch unter diesem Aspekt.

Im Zuge der Integration des Desktop mit dem Backend wandelt sich ganz allgemein die Funktion der Office-Anwendungen. Waren sie bisher mächtige Autorenwerkzeuge für die Gestaltung technisch weitgehend unstrukturierter Dokumente, so ordnen sie sich nun den Anforderungen zentralisierter IT-Systeme unter. Ihre Funktion wandelt sich dabei zu der von Dateneingabe-Formularen und Datenanalyse-Formatierungswerkzeugen für hochgradig strukturierte Daten – freilich mit dem vertrauten Komfort mächtiger Autorenwerkzeuge. Wenn die Interoperabilität der Office-Suiten mit Backoffice-Systemen wächst, wird sich möglicherweise zugleich die Notwendigkeit der Interoperabilität untereinander relativieren. Zunächst steht sie jedoch noch im Mittelpunkt.

3.13.3.1 Betrachtungsebenen

Wenn von der Interoperabilität von Office-Suiten auf XML-Basis die Rede ist, ist im Rahmen dieses Leitfadens der Austausch von XML-Dateien gemeint. Man kann daher auch von einer "dateibasierten Interoperation" sprechen. XML kann auch auf andere Weise helfen, Interoperabilität herzustellen. Web Services (siehe Kapitel 3.9.4) ermöglichen beispielsweise den Austausch von XML-Dokumenten zwischen zwei Anwendungs*prozessen*, allerdings ohne dass diese Dokumente jemals als Datei gespeichert werden müssen.

Um das Potenzial aber auch die Grenzen der auf XML-Dateien basierenden Interoperabilität von Office-Anwendungen auszuloten, ist eine differenziertere Betrachtung der zu lösenden Kompatibilitätsprobleme hilfreich. Die folgenden Kompatibilitätsebenen werden am Beispiel Textverarbeitung dargestellt, gelten in unterschiedlichem Maße aber auch für Tabellenkalkulationen, Präsentationsprogramme und viele andere Anwendungen:

- Dokumentenmodell
  Jede Anwendung hat eine interne Sicht auf ein zu bearbeitendes Dokument, die sich von der menschlichen Wahrnehmung unterscheidet. Ein simpler Brief auf einem Briefbogen ist für den menschlichen Betrachter ein völlig selbstverständlicher Gegenstand. Damit ein Textverarbeitungsprogramm ihn aber gestalten kann, muss es beispielsweise dafür sorgen, dass sich bei Änderungen zwar der Text mit seinen Fußnoten verschiebt, nicht aber der Briefkopf, das Datum und die Faltmarken. Dazu kennt die Textverarbeitung Konstruktionen wie Textboxen, eingebettete Objekte, Fußzeilen oder Wasserzeichen. Die Menge dieser Gestaltungsinstrumente, die zusammen das Dokumentenmodell ausmachen, sind von einer Textverarbeitung zur anderen unterschiedlich. Beispielsweise verfügt Corel WordPerfect über Instrumente wie verschachtelte Styles und positionssensitive Sprungbefehle, die im Dokumentenmodell von Microsoft Word keinerlei Entsprechung haben.

  Auf der Ebene der Dokumentenmodelle misst sich die Kompatibilität zweier Textverarbeitungen daran, in welchem Maße die Modelle identisch sind (Modellkompatibilität) und in welchem Maße die Instrumente des einen Modells in die Instrumente des jeweils anderen Modells übersetzt werden können (Modell-Abbildbarkeit).

- Dateiformat
  Das Dokumentenmodell ist ein internes Konstrukt einer Anwendung. Es ist dem Anwender zugänglich, während er mit der Anwendung arbeitet. Andere Anwendungen haben jedoch in der Regel keinen Zugang dazu. Stattdessen greifen sie auf die Dateien zu, in der die Anwendung ihre Dokumente speichert. Die Dateien enthalten zwar alle Informationen des Dokumentenmodells, können selbst aber durchaus anders strukturiert sein. Beispielsweise können sie anstelle des letzten Bearbeitungszustandes des Dokumentes einen älteren Stand speichern, und ergänzend

dazu die seither vorgenommenen Bearbeitungsschritte. Darüber hinaus kann die Datei binär kodiert sein, so dass sie nur von geeigneten Anwendungen genutzt werden kann, wie etwa das Standardformat von Microsoft Word. Sie kann aber auch in einem für Menschen mehr oder minder lesbaren Format geschrieben werden, wie etwa das RTF-Format oder die komprimierten XML-Archive, die Sun StarOffice und OpenOffice.org verwenden. Die meisten Anwendungen sind in der Lage, Dokumente in unterschiedlichen Formaten zu speichern und zu lesen. Der vollständige Informationsgehalt des Dokumentenmodells kann jedoch häufig nur in einem einzigen, nativen Dateiformat abgelegt werden; die Verwendung anderer Dateiformate ist in diesem Fall mit dem Verlust von Informationen verbunden.

Auf der Ebene des Dateiformates misst sich Kompatibilität zunächst daran, ob das Format technisch lesbar ist. Die technische Lesbarkeit kann dadurch hergestellt werden, dass es sich um ein standardisiertes Dateiformat handelt (RTF, XML), oder dass das Format dokumentiert ist. Ferner muss der letzte Bearbeitungsstand des Dokumentes aus den in der Datei gespeicherten Daten unmittelbar entnehmbar oder zumindest ableitbar sein. Schließlich muss ein Werkzeug bereit stehen, das diesen Bearbeitungsstand aufnimmt und in das Dokumentmodell der jeweils anderen Anwendung übernimmt.

- Gestaltungstreue
  Bei der Bearbeitung eines Textdokumentes ist dem Anwender oft nicht nur am Wortlaut des Textes gelegen, sondern auch an dessen Gestaltung. Moderne Textverarbeitungen bieten eine Fülle von visuellen Gestaltungsmöglichkeiten und stellen sie dem Anwender i.d.R. im Rahmen des WYSIWYG-Paradigmas zur Verfügung. Der Anwender erwartet mit einer gewissen Berechtigung, dass das Dokument immer und unter allen Umständen so aussehen wird, wie er es zum Zeitpunkt der Bearbeitung auf seinem Bildschirm wahrnimmt. "Immer" schließt dabei alle erdenklichen Drucker, alternative Betriebssysteme und -Umgebungen ein, aber im Migrationskontext auch andere Anwendungen bzw. Anwendungs-Versionen. Unglücklicherweise erweist sich WYSIWYG in der Praxis seit jeher als guter Vorsatz, der zwar meist annähernd, aber kaum je vollständig umgesetzt wird. Und der bloße Wechsel des Druckertreibers genügt, um die Gestaltung längerer, mit zahlreichen Grafiken versehener Dokumente über den Haufen zu werfen. Die technischen Gründe dafür sind ebenso vielfältig wie (zumeist) nachvollziehbar.

  Was Kompatibilität auf der Ebene der Gestaltungstreue bedeutet, muss im Einzelfall entschieden werden. Wenn eine Faltmarke an der falschen Position gedruckt wird, erfüllt sie ihren Zweck nicht mehr. Wenn sie etwas schmaler oder etwas länger ist, ist das hingegen meist kein Beinbruch. Wenn die Gestaltungsdetails des Stadtwappens einer Graustufenkonvertierung zum Opfer fallen, kann das schon wieder ein Politikum sein. Maß-

geblich sind letztlich die Anforderungen, die an ein bestimmtes Resultat gestellt werden, z.B. an den Druck auf Papier, und die auf die Übereinstimmung mit amtlichen Vordrucken oder mit Gestaltungsrichtlinien abzielen.

Da Probleme der Darstellungstreue am deutlichsten zu Tage treten, werden sie häufig als entscheidender Maßstab für Interoperabilität verstanden. Ob diese Probleme tatsächlich die Roundtrip-Interoperabilität beeinträchtigen, hängt allerdings in hohem Maße vom konkreten Anwendungsszenario ab. Unter Umständen können Mängel der Darstellungstreue toleriert werden, sofern die Interoperabilität auf den anderen Ebenen gewährleistet ist.

Die Zuordnung augenscheinlicher Kompatibilitätsprobleme zu einer der drei Ebenen ist für den Anwender jedoch häufig nicht einfach. Wenn beispielsweise eine Tabelle in einem Textdokument nach der Konvertierung aus einer Datei der Anwendung A in eine Datei der Anwendung B völlig anders aussieht, wird diese Veränderung zunächst als mangelnde Gestaltungstreue wahrgenommen und möglicherweise auf ein Dateiformat-Problem zurückgeführt. Tatsächlich handelt es sich aber womöglich um eine Inkompatibilität der Dokumentenmodelle, die ein Konvertierungswerkzeug durch einen gut gemeinten übersetzenden Eingriff zu überbrücken versucht hat.

Die richtige Identifikation der Ebene, der ein Kompatibilitätsproblem zugeordnet ist, hat aber deshalb eine entscheidende Bedeutung, weil sich daraus die in Frage kommenden Lösungen ableiten. Der folgende Abschnitt geht insbesondere der Frage nach, welche Beiträge XML-Technologien auf den unterschiedlichen Ebenen leisten können.

3.13.3.2 Maßnahmen zur Überwindung von Interoperabilitätshindernissen

Inkompatibilitäten auf der Ebene der **Gestaltungstreue** sind schwer zu beheben. Bietet beispielsweise ein Drucker eine deutlich gröbere Auflösung als ein anderer, dann verläuft die eben noch feine Schraffur im Stadtwappen unter Umständen zu einer indifferenten schwarzen Fläche. Abhilfe schafft in einer solchen Situation die Vereinheitlichung der Hardware oder eine geschicktere Aufbereitung der Grafik. In anderen Fällen mögen zwei verschiedene Drucker technisch in der Lage sein, identische Ergebnisse zu produzieren, aber die Funktionsweise der jeweils notwendigen Druckertreiber einer Anwendung ist so unterschiedlich, dass sie dennoch unterschiedliche Ergebnisse produzieren. Ein solches Phänomen wäre ein internes Problem der Anwendung. Zur Behebung dieser Art von Misshelligkeiten kann XML keinerlei Beitrag leisten. Insofern ist es fast tröstlich, dass die Mehrzahl der Gestaltungsprobleme auf Inkompatibilitäten im Dokumentenmodell zurückzuführen sind.

Inkompatibilitäten auf der Ebene des **Dokumentenmodell**s können durch die bereits angesprochenen Abbildungen von einem Modell ins andere überbrückt werden. Um eine uneingeschränkte Roundtrip-Interoperabilität zwischen beiden Modellen herzustellen, müssten diese Übersetzungen umkehrbar sein. In der

Praxis ist das selten der Fall. Prinzipielle Gründe dafür sind unter anderem die unterschiedlichen Verteilungen des Gestaltungsreichtums innerhalb der Modelle sowie die Schwierigkeit, bestimmte Merkmale eines Dokumentes als bewussten Eingriff des Anwenders oder als das Artefakt einer Modellübersetzung zu identifizieren. Die fast unausweichlichen Asymmetrien solcher Modell-Übersetzungen sind jedoch die zentrale Ursache für das schneeballhafte Anwachsen von Anomalien beim mehrfachen Hin- und Herkonvertieren eines Dokumentes zwischen zwei Formaten.

Roundtrip-Interoperabilität lässt sich unter diesen Umständen dadurch erreichen, dass nur diejenigen Gestaltungsmöglichkeiten tatsächlich in Dokumenten verwendet werden, die in allen in Frage kommenden Dokumentenmodellen identisch sind, oder deren Übersetzung so gestaltet werden kann, dass sie im Regelfall umkehrbar ist, mindestens aber frei von Schneeball-Effekten. Dazu müssen die in Frage kommenden Gestaltungsmöglichkeiten identifiziert werden. Anschließend können Dokumentenvorlagen entsprechend gestaltet werden. Der praktische Erfolg hängt schließlich aber auch davon ab, ob die Anwender über die zulässigen Gestaltungsmöglichkeiten informiert werden und sich tatsächlich an den gegebenen Rahmen halten.

Um auch diejenigen Gestaltungsmöglichkeiten nutzen zu können, die die beschriebenen Bedingungen nicht erfüllen, bietet es sich an, den Bearbeitungszyklus der Dokumente in zwei Phasen einzuteilen. In der ersten Phase erfolgt die eigentliche Bearbeitung. Sie beschränkt sich soweit wie möglich auf den Dokumenteninhalt und vermeidet daher weitestgehend gestaltende Eingriffe. Die zweite Phase beginnt, wenn die inhaltliche Bearbeitung endgültig abgeschlossen ist. In dieser Phase erfolgt das gestalterische 'Finetuning' des Dokumentes mit nur einer der beteiligten Anwendungen. Eine umlaufende Bearbeitung findet also in dieser Phase nicht mehr statt, so dass auch die damit verbundenen Probleme nicht mehr auftreten (siehe auch Kapitel 3.13.7.2).

XML kann prinzipiell bei der Abbildung von einem Modell ins andere (und umgekehrt) helfen, namentlich XSLT in Verbindung mit entsprechenden Stylesheets. Die XSL-Transformationen können nicht nur im Rahmen eines selbständigen (Anwendungs-) Prozesses auf Dateien angewendet werden, um die Abbildung auf der Ebene des Dateiformates zu leisten, sondern auch innerhalb des Prozesses einer Textverarbeitung unmittelbar auf einer internen Repräsentation des Dokumentenmodells, typischerweise allerdings während des Lesens oder Schreibens von Dateien.

Inkompatibilitäten auf der Ebene des **Dateiformat**es sind im Vergleich zu den anderen Ebenen ein technisch gesehen simples Problem, erweisen sich aber dennoch immer wieder als erhebliches Hindernis. XML sorgt auf dieser Ebene für eine substanzielle Erleichterung. Wie bereits dargelegt hat Dateiformat-Kompatibilität zwei Voraussetzungen: technische und semantische Merkmale des Dateiformats müssen bekannt sein und Werkzeuge für seine Bearbeitung müssen zur Verfügung stehen. Die letztgenannte Bedingung kann bei der Verwen-

dung XML-basierter Dateiformate als grundsätzlich gegeben angesehen werden, da erprobte und teilweise sogar frei verfügbare Standardwerkzeuge eingesetzt werden können. Diese Werkzeuge leisten sowohl den Zugriff auf die in der Datei enthaltenen Daten, als auch die Konvertierung in ein anderes Format. Lediglich das für die Konvertierung notwendige XSL-Stylesheet muss anwendungsbezogen bereitgestellt werden. Sollte die Komplexität der Konvertierung die Ausdrucksmacht von XSL-Stylesheets einmal überfordern, steht mit dem Document Object Model (DOM) ein standardisiertes und durch frei verfügbare Implementationen unterstütztes Programmiermodell für individuelle Lösungen zur Verfügung. Sollen die nutzbaren Gestaltungsmöglichkeiten einer Anwendung eingeschränkt werden, dann wird die Überwachung der Einhaltung dieser Beschränkung auf der Basis eines XML-Datenformates durch die XML-Standardwerkzeuge deutlich vereinfacht.

Ein XML-Dateiformat kann darüber hinaus im technischen Sinne als grundsätzlich bekannt angesehen werden. In der Regel wird jedes von einer Office-Anwendung erzeugte XML-Dokument ein Schema referenzieren, das jedem legitimen Verwender des Dokumentes zugänglich sein sollte, und die Validierung des Dokumentes erlaubt.

Die Semantik eines XML-Dokumentes bzw. -Schemas kann allerdings durch kein Standardwerkzeug gewonnen werden sondern muss separat in beliebiger geeigneter Form dokumentiert sein. XML gibt dafür keine Empfehlung. Eine solche Dokumentation setzt das Dokumentenmodell als bekannt voraus und beschreibt die Abbildung der einzelnen Strukturen des Dokumentenmodells auf die Strukturen des XML-Dokumentes bzw. Schemas. Dieses Wissen sowohl über die Quell- wie über die Ziel-Anwendung fließt in den XSL-Stylesheets zusammen, die zur Dateikonvertierung verwendet werden.

An die folgende Beschreibung der Ausgangslage schließt sich die Darstellung der aktuellen Office-Suiten von Sun (ablösende Migration) und Microsoft (fortführende Migration) an. Sie zeigt auf, welche XML-Unterstützung die Suiten gegenwärtig bieten und welche Strategien sie damit verfolgen. Kapitel 3.13.7.2 leitet daraus eine zusammenfassende Betrachtung ab und konkretisiert die Perspektive normierter Dateiformate.

3.13.4 Ausgangslage MS Office

Bevor nun die möglichen Migrations-Alternativen zu Office 97 bzw. 2000 betrachtet werden, soll zunächst in einer kurzen Übersicht die aktuelle Situation dargestellt werden.

MS Office steht in unterschiedlichen Paketen und Versionen zur Verfügung. Im Unterschied zum Betriebssystem ist nicht davon auszugehen, dass bei der Mehrzahl der Behörden eine bestimmte Version von MS Office eingesetzt wird. Es kann allerdings davon ausgegangen werden, dass die Versionen vor Microsoft Office 97 kaum noch und Microsoft Office 2003 noch nicht besonders häufig im Einsatz sind. Im überwiegenden Teil der Behörden wird Microsoft Office 97, 2000

oder sogar Office XP im Einsatz sein. Behörden, die bereits auf Office XP umgestellt haben, haben dies zum überwiegenden Teil im Jahr 2004 getan. Überlegungen, dieses schon wieder durch ein neues Produkt zu ersetzen, dürften dort sicherlich nicht bestehen. Daher werden für die nachfolgenden Betrachtungen die Versionen Office 97 und 2000 als Ausgangslage für eine Migration herangezogen.

Neben den Versionen spielen mit Blick auf eine Migration die unterschiedlichen Office Pakete eine wichtige Rolle. Diese Pakete, auch Editionen genannt, unterscheiden sich in der Regel durch die darin enthaltenen Einzelanwendungen. Ausgehend von dem Professional-Paket für Office 2000 werden für die nachfolgenden Betrachtungen in den Abschnitten

- Ablösende Migration von MS Office und
- Fortführende Migration von MS Office

die Einzelanwendungen

- Word
- Excel und
- Powerpoint

betrachtet. Outlook wird im Kapitel 3.12 als Bestandteil einer Groupware und Messaging Lösung mitbetrachtet. Access wird im Zusammenhang mit der Migration von Datenbanken analysiert und bewertet. Internet Explorer und PhotoEditor werden im Abschnitt „Weitere Desktopanwendungen“ zusammen mit anderen Desktop-Tools behandelt. In demselben Abschnitt gehen die Autoren auch kurz auf MS Project ein.

3.13.4.1 Funktionalitäten

Auf eine Auflistung aller verfügbaren Funktionalitäten in Word, Excel und PowerPoint muss an dieser Stelle jedoch verzichtet werden. Die beiden nachfolgenden Kapitel sollen stattdessen die wichtigen Unterschiede zwischen der Ausgangslage und den möglichen zukünftigen Alternativen in Hinblick auf eine Migration verdeutlichen.

Zunächst ist die zum Teil intensive Verwendung von behördenspezifischen Softwarelösungen als Erweiterung der Funktionalitäten von MS Office festzustellen. Das heißt zum einen, dass die mit MS Office verfügbare Programmierumgebung in vielen Behörden und anderen Organisationen zur Erstellung dokumentenspezifischen Scriptinglösungen (Makros) genutzt wird, um Arbeitsprozesse mit MS Office weitgehend zu automatisieren. Das reicht bis zur Implementierung abteilungsübergreifender Workflows. Zum anderen gibt es in den Behörden eine Reihe externer Softwarelösungen, bei denen eine mehr oder weniger starke Integration mit Office vorliegt. Daher wird nachfolgend kurz auf die Programmierumgebung von MS Office eingegangen.

3.13.4.2 Programmierumgebung MS Office

Die Programmierumgebung von Microsoft Office basiert auf der Programmiersprache BASIC. Innerhalb der Microsoft geprägten Welt wird derzeit von Visual Basic gesprochen. Diese Sprachfamilie umfasst aktuell mehrere Dialekte:

- Visual Basic (Visual Studio, Vollversion)
- Visual Basic for Application (VBA)
- Visual Basic Scripting Edition (VBS).

Alle haben denselben Grundwortschatz, unterscheiden sich aber in Funktionsumfang und Ablaufumgebung.

Die Programmierumgebung von MS Office beinhaltet Visual Basic for Application (VBA). VBA kann von Microsoft lizenziert werden, so dass Dritthersteller die VBA in ihre Produkte einbauen können.

Als Ausgangspunkt für diesen Leitfaden wird der Einsatz des Office-Paketes 97 angenommen. In früheren Versionen wurden verschiedene Programmierumgebungen für die einzelnen Produkte bereitgestellt (Word Basic, Excel VBA, Access Basic). Mit Office 97 wurde die Programmierumgebung auf VBA der Version 5 vereinheitlicht. Die folgende Tabelle zeigt die Versionierung von VBA im Zusammenhang mit den verschiedenen Office Versionen.

Tab. 40: VBA-Versionen

Office Versionen	VBA Versionen
95	Word Basic, Excel VBA, Access Basic
97	5
2000	6
XP	6.3

Im Folgenden wird primär VBA vorgestellt und hinsichtlich der Abgrenzung davon speziell die Varianten von Visual Basic (Vollversion und Scripting Edition).

Basiskonzepte von VBA

VBA ist eine Interpretersprache und nur in Office Anwendungen ausführbar. VBA basiert auf COM (Component Object Model), einer Weiterentwicklung der Technologie OLE (Object Linking and Embedding).

Office kann nicht nur COM Objekte verwenden, sondern bietet selbst COM Objekte an. Office 97 bringt über 550 eigene COM Objekte mit, Office 2000 über 600. Via COM lassen sich in Office auch externe Funktionalitäten nutzen. Mittels VBA ist es möglich, externe Programme (z.B. das Betriebssystem) in Form von DLLs (Dynamic Link Libraries) zu verwenden[1].

[1] In Visual Basic Script (VBS) ist solch eine Einbindung nicht möglich.

Die folgende Abbildung zeigt noch einmal die Möglichkeiten von VBA, Funktionalitäten zu nutzen.

Bild 40: VBA in der Office Anwendung

In VBA werden die einzelnen Bausteintypen in

- Module (moduls)
- Klassenmodule (class moduls)
- und Formulare (forms)

unterteilt.

In Modulen befindet sich „normaler“ Programmcode. In Klassenmodulen können eigene Objekte sowie deren Eigenschaften und Methoden erstellt werden.

Diese Bausteine ermöglichen es, in MS Office vorhandene Funktionalitäten zu erweitern, Abfolgen von Funktionsaufrufen zu automatisieren und zusätzliche Funktionalitäten zu implementieren. Die Erweiterungen, Automatisierungen und Ergänzungen werden als Makros und Scriptings bezeichnet. Zur Integration dieser Makros in MS Office lassen sich insbesondere die Menüleisten und Schaltflächen der Symbolleisten modifizieren, so dass dem Benutzer deren Starts erleichtert wird.

Spezielle Prozedurnamen (z.B. AutoOpen, AutoNew) kennzeichnen den Programmcode, der automatisch ausgeführt wird, wenn Office-Dateien geöffnet werden. Dies wird häufig in Vorlagen (Templates) verwendet und beinhaltet die Gefahr der so genannten „Makroviren“[1].

Insgesamt können Makros und Scriptings in folgenden Formen innerhalb von Office aufgerufen bzw. integriert werden:

- als Add-In
- innerhalb von Vorlagen (Templates)
- als Assistenten (Wizards).

[1] Siehe auch Faltblatt des BSI zu „Makro-Viren, Definition und Wirkungsweise“ (http://www.bsi.bund.de/literat/faltbl/F21Makroviren.htm)

Add-Ins unterscheiden sich aufgrund ihrer Verwendbarkeit nochmals:

- COM Add-Ins und
- Anwendungsspezifische Add-Ins.

COM Add-Ins sind kompilierte DLL- oder EXE-Dateien, die mit einer Visual Basic (Vollversion) erzeugt werden. Diese Add-Ins können anwendungsübergreifend verwendet werden.

Anwendungsspezifische Add-Ins werden mittels der integrierten Programmierumgebung von Office erzeugt und können nur innerhalb Office verwendet werden. Der Einsatz von Add-Ins ist in der Regel dort anzutreffen, wo der Programmcode ständig in der Anwendung zur Verfügung stehen soll, damit der Benutzer keine Vorlagen starten muss.

Die folgende Abbildung gibt nochmals einen Überblick über die Erweiterungsmöglichkeiten in MS Office durch eigene Programmierungen.

Bild 41: Erweiterungsmöglichkeiten von Office

Entwicklerumgebung

Mit VBA der Version 5 wurde innerhalb der Office Anwendungen eine einheitliche Entwicklungsumgebung integriert. Die so genannte IDE (Integrated Development Enviroment) wird in einem separaten Fenster gestartet, läuft aber in demselben Speicherbereich der Office Anwendung.

Die IDE bietet:

- einen Editor mit Syntaxprüfung und Farbhervorhebung
- einen Project Explorer
- ein zusätzliches Eigenschaftsfenster
- Debugger-Werkzeuge
- einen Object Browser
- bedingte Compilierung
- Schutzmechanismen vor Veränderung oder Kopieren des programmierten Codes
- und IntelliSense (Komplettierung, Drop-Down Auswahl, Infos zur Syntax).

Neben diesem Editor kann innerhalb der Anwendung auch ein Makro-Rekorder zur Erstellung des einfachen Programmcodes zum Einsatz kommen.

Fernsteuerung

Da Office selbst aus einer Vielzahl von COM Objekten besteht, ist es möglich, Office fernzusteuern, also eine COM-Automatisierung durchzuführen.

Zur Fernsteuerung können z.B. der Windows Scripting Host (WSH) oder Perl-Script verwendet werden.

3.13.5 Ablösende Migration

3.13.5.1 Einleitung

Es gibt verschiedenste Office-Software-Pakete oder -Teilanwendungen (z.B. Textverarbeitungen), die als freie oder proprietäre Software für das Betriebssystem Linux zur Verfügung stehen. Unter anderem sind dies:

- OpenOffice
- StarOffice
- Koffice
- GnomeOffice
- ThinkFree Office
- u.a.

Eine wirkliche Alternative zur MS Office Suite bieten aus heutiger Sicht auch aufgrund der Verbreitung und im Einvernehmen mit allen Experten allerdings nur die Pakete OpenOffice.org (OOo) bzw. das darauf basierende StarOffice (SO). Daher werden innerhalb des Leitfadens nur diese beiden Pakete hinsichtlich einer Migration detailliert betrachtet.

OpenOffice steht derzeit in der Version 1.1 zur Verfügung, das Äquivalent dazu ist StarOffice 7.0. Beide Versionen sind auch für die Windows Betriebssysteme NT, 2000 und XP einsetzbar. Da OOo/SO auf allen unterstützten Betriebssystemen über die gleiche Funktionalität verfügt und das selbe Dateiformat einsetzt, erleichtert es eine „sanfte“ Migration, indem im ersten Schritt nur das Office-Paket ersetzt wird. Die neuen Versionen 2.0 (OOo) und 8 (SO) stehen bereits in einer Beta-Version zur Verfügung und sollen im Laufe des Jahres 2005 als Endversion bereitgestellt werden.

Die Unterschiede zwischen OpenOffice und StarOffice

Die Entwicklung der Basistechnologie der beiden Office Suiten erfolgt auf OpenOffice.org. Im Jahre 2000 hat Sun Microsystems den Quelltext des damaligen Office-Pakets StarOffice 5.2 in das Open Source Projekt OpenOffice.org überführt. Das OpenOffice.org Projekt steht unter der Doppellizenz GPL und SISL (GNU Public License bzw. Lesser GNU Public License und der Sun Industrie Source License). Die Doppellizenz ermöglicht es einerseits, kommerzielle Pro-

dukte aus OpenOffice.org abzuleiten. Andererseits garantiert sie, dass die Spezifikationen des API und des Dateiformates für OpenOffice.org und alle Derivate verpflichtend und einheitlich sind.

Für StarOffice hat die Firma Sun zusätzliche Komponenten entwickelt bzw. hinzugenommen und ein Produktpaket aus professioneller Qualitätssicherung, umfangreicher Dokumentation, Support und Schulungsangeboten geschnürt. Einige der Sun-Komponenten sind:

- TrueType Fonts, welche an die Fonts von Microsoft angelehnt sind (siehe Bild 42)
- eine eigene Rechtschreibprüfung und Thesauri, OpenOffice verwendet meist MySpell (LGPL)
- zusätzliche Vorlagen und eine Bildergalerie
- die ADABAS Datenbank.

Darüber hinaus liefert Sun Bug-Patches oder Servicepacks für die jeweiligen Produktversionen. So gibt es derzeit alle drei Monate ein StarOffice Servicepack, das verbesserte Sicherheitsaspekte, Korrekturen für Programmfehler oder Verbesserungen der Importfilter beinhaltet. OpenOffice.org hingegen enthält diese Komponenten nur in der jeweils allerneusten Version[1].

Font Win32	*Font Unix*
MS Sans Serif	MS Sans Serif **Andale Sans UI**
WinDings	StarSymbol WinDings
Arial	Arial **Albany**
Times New Roman	Times New Roman **Thorndale**
Courier New	Courier New **Cumberland**
Comic Sans MS	Comic Sans MS **Kidprint**

Bild 42: Fontmapping MS Office OOo/SO[2]

Die StarOffice Suite ist gegenüber der freien OpenOffice.org Suite nur kostenpflichtig zu erhalten. Support wird in der Regel für beide Varianten nur kostenpflichtig angeboten. Für StarOffice ist der Support u.a. direkt von Sun und für OpenOffice.org nur von Drittanbietern erhältlich.

1 Weitere Details zu den Unterschieden finden sich unter: http://marketing.openoffice.org/conference/presentationspdf/thu1500/SOvsOOo.pdf

2 Quelle: SunMicrosystems

Bestandteile von OOo bzw. SO

OOo und SO bestehen genau wie MS Office aus verschiedenen Teilanwendungen. Hierzu gehören:

- Textverarbeitung (Writer)
- Tabellenkalkulation (Calc)
- Präsentation (Impress)
- Formeleditor[1] (Math)
- Zeichnung[2] (Draw)
- Datenbank[3] (Adabas)[4].

Im Focus der folgenden Untersuchung stehen dabei allerdings nur die ersten drei dieser Module.

In den wesentlichen Funktionalitäten stimmen die drei Office Suiten überein, insbesondere bei den Funktionalitäten, die von der Mehrheit aller Benutzer verwendet werden. Die wichtigsten Unterschiede in den Funktionen von MS Office und OOo/SO werden in den folgenden Kapiteln im Einzelnen dargelegt. Insbesondere wird auf die Unterschiede in der Darstellung von Inhalten und in der Verfügbarkeit von Funktionen eingegangen. Dabei beschränkt sich der Leitfaden auf die Module Textverarbeitung, Tabellenkalkulation und Präsentation. Auf eine mögliche Ablösung des Moduls MS Access durch ein anderes Datenbanksystem wird im Kapitel 3.11 näher eingegangen. Weitere Module der MS Office Suite und andere Anwendungen des MS Desktops werden im Kapitel 3.13.8 beschrieben.

3.13.5.2 Das XML-Dateiformat in OOo/SO

Jede Microsoft Office-Anwendung verwendet ein eigenes binäres Dateiformat, das Text, Attribute, eingebettete Graphiken, Metadaten und Layoutelemente als OLE-strukturierte Daten speichert. In Office 2003 bieten einige Anwendungen alternativ ein jeweils eigenes XML-Format an.

Analog zu seiner stärker integrierten Architektur verwendet OOo/SO im Gegensatz dazu ein einziges, einheitliches XML-zentriertes Dateiformat für alle Anwendungen; die Dateinamen erhalten jedoch eine anwendungsspezifische Erweiterung. Das Dateiformat ist ein ZIP-Archiv, das eine ganze Reihe einzelner Dateien bündelt und zugleich komprimiert. Die folgende Liste zeigt den Inhalt einer unverschlüsselten OOo/SO-Writer-Datei für ein Dokument, in dem eine Grafik und ein Makro enthalten sind (die Endung ".odt" steht für "OpenDocument Text"):

---

1 Die Funktionen, die Math bietet, sind in Microsoft über einen eigenen Editor integriert, der über Einfügen/Objekt/Neu erstellen/Microsoft Formeleditor aufgerufen werden kann.

2 Die Funktionen, die Draw bietet sind in Microsoft z.B. über die Symbolleiste Zeichnen integriert.

3 Nicht in OpenOffice.org

4 Nicht direkt vergleichbar mit Access unter Windows.

```
Archive: Eine_OOo-Writer-Datei.odt
 Length  Method  Size  Name
-------- ------ ------- ----
   39 Stored    39 mimetype
    0 Stored    0 Configurations2/
  35287 Stored  35287 Pictures/10000000E20E2459CCEB9.gif
   418 Defl:N   219 VersionList.xml
  3274 Defl:N   1014 content.xml
  1190 Defl:N   498 Basic/Standard/Module1.xml
   348 Defl:N   214 Basic/Standard/script-lb.xml
   338 Defl:N   211 Basic/script-lc.xml
  6744 Defl:N   1588 styles.xml
  1058 Stored   1058 meta.xml
  5686 Defl:N   4653 Versions/Version1
  5706 Defl:N   4671 Versions/Version2
  3609 Defl:N   3329 Thumbnails/thumbnail.png
  7115 Defl:N   1272 settings.xml
  1979 Defl:N   399 META-INF/manifest.xml
--------     ------- -------
  72791      54452 15 files
```

Der Inhalt von Passwort-verschlüsselten Paketen sieht etwas anders aus, da die inhaltstragenden Dateien zunächst ihrerseits komprimiert, dann erst verschlüsselt und schließlich im Archiv als "stored" abgelegt werden. Die Funktionen der einzelnen Dateien sind unterschiedlich, wie die folgenden Beispiele zeigen:

- `META-INF/manifest.xml`
  Diese Datei ist das Inhaltsverzeichnis des Paketes, hat daher einen festen Namen und befindet sich immer an der gleichen Stelle. Hier ist jede weitere Datei des Paketes vermerkt, zusammen mit ihrem Medientyp sowie ggf. Informationen zum gewählten Verschlüsselungsverfahren.
- `mimetype`
  Der Inhalt dieser Datei identifiziert den Dokumenttyp. Ein Textdokument hat beispielsweise den MIME-Typ "application/vnd.oasis.opendocument.-text". Diese Datei, wie auch die vier folgenden, sind in jedem Paket stets genau einmal vorhanden.
- `content.xml`
  Diese Datei nimmt den eigentlichen Inhalt des Dokuments auf, zusammen mit direkt angebrachten Formatierungen. Sie existiert genau einmal unter stets gleichem Namen.
- `meta.xml`
  Diese Datei nimmt Dokument-Metadaten auf, wie Titel, Schlüsselwörter und Bearbeitungsvermerke
- `styles.xml`
  Diese Datei enthält die im Dokument verwendeten Styles (Formatvorlagen) für die indirekte Formatierung des Dokumentes.
- `Thumbnails/thumbnail.png`
  Diese Grafik ist eine näherungsweise Miniatur des Druckbildes der ersten Seite des Dokumentes oder ein vom Dokumenteninhalt unabhängiges Bild, wenn es sich um ein verschlüsseltes Dokument handelt.

- `Versions/VersionN`
  Werden Versionsstände eines Dokumentes markiert, dann werden sie als "Archiv im Archiv" abgelegt, jede Version in einer eigenen Datei. Das Versions-Verzeichnis existiert nur, wenn auch Versionen markiert wurden.
- `VersionList.xml`
  Diese Datei inventarisiert die markierten Dokument-Versionen. Wie das `Versions`-Verzeichnis wird sie nur angelegt, wenn tatsächlich Versionen markiert wurden.
- `Pictures/*`
  In das Dokument eingebettete Bilder werden in diesem Verzeichnis in ihrem nativen Format abgelegt. Das `Pictures`-Verzeichnis wird nur angelegt, wenn das Dokument auch Bilder enthält.
- Ergänzende Unterverzeichnisse
  Eigene ergänzende Unterverzeichnisse dienen zur Aufnahme von Makros (`Basic/*` im gezeigten Beispiel) oder von eingebetteten Objekten (im Beispiel nicht gezeigt)

Zwar erfordert das Paketformat einen gewissen Aufwand für das Ein- und Auspacken. Dem stehen allerdings eine Reihe von Vorteilen gegenüber. Offensichtlich ist, dass die Pakete durch die ZIP-Kompression relativ kompakt sind und so das naturgemäß stürmische Größenwachstum von XML-Dateien neutralisieren. Dazu trägt auch die Speicherung von Grafiken in nativen Formaten bei, die stets kompakter sind als eine komprimierte XML-Repräsenation. Die Aufteilung verschiedener Teilfunktionalitäten in unterschiedliche Dateien erleichtert in einigen Szenarien die zielgerichtete automatisierte Bearbeitung. Wenn etwa in einer Reihe von Dokumenten die Stylesheets ausgetauscht werden sollen, dann kann dies geschehen, ohne den eigentlichen Dokumenteninhalt anrühren zu müssen. Wird in einem Dokument auf direkte Formatierungen verzichtet, dann gewährleistet insbesondere die Ausgliederung der Stylesheets auf technischer Ebene die immer wieder geforderte Trennung von Inhalt und Präsentation.

Eine entscheidende Rolle für die Ausgestaltung des Dateiformates spielt neben technischen Aspekten auch eine Strategie, die von Sun mit dem Schlagwort "Own your Data" identifiziert wird. Sie sieht in undokumentierten, binären und womöglich proprietären Dateiformaten eine Beeinträchtigung des Urhebers oder Eigentümers von Daten: um auf sein Eigentum zugreifen oder es Dritten zur Verfügung stellen zu können, muss eine ganz bestimmte Anwendung zur Verfügung stehen. Das kann aber nicht überall und immer vorausgesetzt werden. In diesem Sinne bietet nur ein anwendungsunabhängiges, dokumentiertes Dateiformat die Sicherheit, langfristig und in beliebiger Weise über die Daten zu verfügen.

Diese Strategie drückt sich zum einen in der konsequenten Verwendung von XML und dem weit verbreiteten ZIP-Format aus, zum anderen in der Standardi-

sierung eines Office-Dateiformates durch das OASIS[1] Open Office XML Format Technical Committee. Das inzwischen "OpenDocument" genannte Format basiert auf dem OOo/SO-Dateiformat, trägt bereits die Versionsnummer 1.0 und befindet sich gegenwärtig im Stadium eines "abgestimmten Entwurfes". OOo 2 und SO 8 werden das OpenDocument-Format verwenden. Das zum KDE-Desktop gehörende KOffice wird das Format ebenfalls unterstützen.

3.13.5.3 Ergänzende XML-bezogene Leistungsmerkmale

OOo/SO bietet einen Import-/Export-Mechanismus für fremde XML-Dateiformate. Der Mechanismus verwendet XSL-Transformationen und wird dementsprechend durch Stylesheets konfiguriert und erweitert. Filter-Stylesheets können als Pakete gebündelt und so auch durch den Anwender in einem Schritt installiert werden. Mitgeliefert werden u.a. Filter für XHTML, DocBook und die Microsoft Office 2003-XML-Formate.

Bild 43: Konfiguration der "XML Filter" (XSLT-Filter) in OOo 1.9.69 (Beta)

Aus Anwendersicht fügen sich die installierten XSLT-Filter in die vertrauten Funktionalitäten ("Öffnen…", "Speichern unter…") ein und mischen sich dort mit den nach wie vor zahlreichen, fest eingebauten Binärformat-Filtern. Die Wahl des richtigen Importfilters für eine gegebene Datei mit der sehr unspezifischen Namensendung *.xml erfolgt automatisch anhand des deklarierten Dokumenttyps. Als Teil einer Importfilter-Konfiguration kann zusätzlich ein Dokumenten-Template identifiziert werden, dessen (Formatierungs-) Styles automatisch auf das importierte Dokument angewendet werden, gesteuert durch entsprechende Zuweisungen des (Import-) Stylesheets.

[1] http://www.oasis-open.org

Bild 44: "XML Filter" präsentieren sich dem Anwender als weiterer Dateityp.

Sollen XML-Dokumente als solche bearbeitet (und nicht importiert) werden, bietet OOo/SO einen integrierten XML-Formulareditor an. Er verwendet intern das XForms-Modell (einschließlich der Instanzen) wie in Kapitel 3.9.3.1 vorgestellt, definiert die Controls der Benutzerschnittstelle allerdings nicht mit den generischen XForms-Elementen, sondern verwendet an ihrer Stelle die traditionellen, in der OpenDocument-Spezifikation beschriebenen Controls der Suite. Auch fehlen in der Version 1.9.69 (Beta) noch einige durchaus nützliche XForms-Features wie beispielsweise das Repeat-Element. Sie sollen erst in einer späteren Version als 2.0 realisiert werden.

3.13.5.4 Einschränkungen bei den Konvertierungs(Import)filter

Zur Konvertierung von Datei-Formaten sind in OOo/SO verschiedene Konverter (Filter) integriert, über welche MS Office Dokumente in OOo/SO geöffnet, bearbeitet und wieder als MS Office Dokument gespeichert werden können. Darüber hinaus ist es möglich, auch MS Dokumentenvorlagen zu importieren und zu bearbeiten. Dateien können entweder im MS Office 97/2000/XP-Format oder im OOo/SO Format gespeichert werden. Im Folgenden wird bei den Betrachtungen nur auf die Konvertierung aus einem abzulösenden Format eingegangen. Dies betrifft bei Office 97/2000 (siehe Ausgangslage) nur die bisher verfügbaren binären Dateiformate von Microsoft Office. Auf die Konvertierung von XML-Dateiformaten wurde im vorhergehenden Kapitel im Zusammenhang mit der Thematik der Interoperabilität eingegangen.

Im Allgemeinen erfolgt die Konvertierung in einer akzeptablen Qualität, sofern es sich nicht um komplexe Dokumente mit Makros und speziellen Format-Features (siehe Tab.: 41) handelt. Hier gibt es einige Layouteigenschaften und Formatierungsattribute in MS Office, die in OOo/SO nicht unterstützt oder anders behandelt werden. Infolgedessen ist es erforderlich, die durchgeführte Konvertierung in einem gewissen Grad manuell nachzubearbeiten, um ein dem Ausgangsdokument entsprechendes Format zu erhalten. Insbesondere bei komplexen und sehr produktspezifischen Dokumenteneigenschaften, wie Indizes, Felder, Frames und Tabellen, können keine 100%igen Konvertierungen erwartet werden. Weiterhin kann es auch in einigen Fällen bei der Konvertierung von Basis-Attributen und –Formatierungen, wie Seitenrändern oder Leerräumen zwischen Absätzen zu

Unterschieden zwischen dem Original und dem konvertierten Dokument kommen.

In der folgenden Tabelle werden die MS Office Eigenschaften aufgelistet, für die eine manuelle Nachbearbeitung der automatischen Konvertierung in Frage kommen kann.

Tab.: 41: Problematische MS Office Eigenschaften hinsichtlich der Konvertierung nach OOo/SO[1]

Anwendung	Eigenschaften
Microsoft Word	❍ AutoShapes ❍ Revision marks ❍ OLE Objekte ❍ Einige Kontroll- und Formular-Felder ❍ Indizes ❍ Tabellen, Rahmen und Multi-Spalten-Formatierung ❍ Hyperlinks und Bookmarks ❍ WordArt-Grafiken ❍ Animierter Text
Microsoft Excel	❍ AutoShapes ❍ OLE Objekte ❍ Pivot Tabellen ❍ Neue Chart-Typen ❍ Formatierungen abhängig vom Inhalt ❍ Einige Funktionen und Formeln
Microsoft PowerPoint	❍ AutoShapes ❍ Tab-, Zeilen- und Absatz-Zwischenräume ❍ Hintergrundgrafik des Masters ❍ Gruppierte Objekte ❍ Einige Multimediaeffekte

Insgesamt kann festgehalten werden, dass sich die Probleme in all den zuvor aufgeführten Bereichen deutlich verringert haben.

3.13.5.5 Funktionale Unterschiede

Konzeptionell gibt es keinen grundlegenden Unterschied zwischen Microsoft Office und OOo/SO. Beide Systeme basieren auf einer 3-Ebenen Architektur, die aus der Anwendung selbst, den Dokumenten-Vorlagen und den Dokumenten besteht. Auf der untersten Ebene befindet sich die Anwendungsschicht, welche die Werkzeuge und die Eigenschaften für die Erstellung von Dokumenten und Vorlagen liefert. Auf der nächsten Ebene liegen die Vorlagen, die eine Vielzahl von Objekten, Makros, Formatierungen und Einstellungen enthalten können, mit deren Hilfe die Erstellung neuer Dokumente vereinfacht wird. Letztendlich betrifft

[1] StarOffice 7™ Migration Guide; http://se.sun.com/edu/staroffice/so_migration_guide_0104.pdf

das die Dokumente, die auf der obersten Ebene ebenfalls weitere Objekte, Makros, Formatierungen und Anwender-Einstellungen enthalten können, welche die Funktionalität aus den Vorlagen erweitern.

Worin sich die beiden Office Suites unterscheiden, sind die Eigenschaften und Funktionen, die sie zur Verfügung stellen und unterstützen. In vielen Fällen können diese Unterschiede der Designwahl und den unterschiedlichen Objektmodellen zugeschrieben werden, auf denen die Anwendungen aufbauen. Zum überwiegenden Teil gibt es in den beiden Suiten jeweils Entsprechungen zu den einzelnen Eigenschaften und Funktionen des anderen Produktes.

Die nachfolgende Tabelle (Tab. 42) stellt einen Überblick über die verfügbaren Vorlagen- und Format-Typen in MS Office und OOo/SO nach Anwendungen kategorisiert, dar.

Tab. 42: Gegenüberstellung der verfügbaren Vorlagen- und Format-Typen

Typ	MS-Word	OOo/SO-Writer	MS-Excel	OOo/SO-Calc	MS-Power Point	OOo/SO Impress
Standard-Dokumentvorlage	normal.dot	verschiedene	bOOok.xlt sheet.xlt	hardcoded	blank.pot	hardcoded
Dokumentenvorlage	verschiedene	verschiedene	verschiedene	verschiedene	Inhalts-/ Design-Vorlagen	Inhalts-/ Design-Vorlagen
Styles	N/a Absatz Zeichen Liste N/a Tabelle	Seite Absatz Zeichen Nummerierung Rahmen Tabelle	Seite/ Blatt Zelle	Seite/ Blatt Zelle	N/a[1] N/a	Grafik-Vorlagen Präsentation

In der folgenden Tabelle (Tab. 43) sind die Unterschiede in den Schlüsselfunktionen zusammengefasst. Weitere funktionale und sonstige Unterschiede werden im „StarOffice 7.0 Migration Guide“[2] ausführlich beschrieben.

Tab. 43: Unterschiede in den Schlüsselfunktionalitäten

[1] PowerPoint liefert ein vordefiniertes Farb- und Animationsschema, welches für die gesamte Präsentation gilt. Demgegenüber verwendet Impress Styles zur Definition des grafischen Erscheinungsbildes und der Darstellung einzelner Objekte.

[2] http://se.sun.com/edu/staroffice/so_migration_guide_0104.pdf

Eigenschaft	Bemerkung
Dokumentenbasierte Makros	OOo/SO unterstützt aufgrund der Unterschiede in den beiden Objektmodellen keine VBA-Makros. Alle VBA-Makros müssen für eine Weiterverwendung (manuell) umgewandelt werden. OOo/SO Dokumente können aber Makros der eigenen Programmiersprache (StarBasic) enthalten. OOo 1.1 und SO 7 enthalten gegenüber ihren Vorgängerversionen jetzt auch einen Makrorekorder[1]. Die VBA-Makros gehen beim Im- und Export nicht verloren.
3D Grafik[2]	MS Office verwendet die „Escher 3D Graphic-Engine“, die nicht identisch mit der OOo/SO 3D-Engine ist. Infolgedessen können kleine Unterschiede in der Darstellung von 3D-Objekten entstehen, wenn 3D-Objekte aus MS-Office importiert werden. Die in OOo/SO verfügbaren Filter unterstützen nicht den Export von 3D-Objekten in das Escher 3D Format.
Tabelle (MS Word)	OOo/SO und MS verwenden unterschiedliche Tabellen-Modelle, was dazu führen kann, dass es zu leichten Unterschieden in der Darstellung kommen kann. Die folgenden MS-Features werden in OOo/SO nicht unterstützt. ❍ Seitenwechsel innerhalb einer Zeile[3] ❍ Hintergrundmuster innerhalb von Zellen Die Darstellung von Rahmen kann nach der Umwandlung unterschiedlich sein, da OOo/SO nicht alle MS-Word Linetypen unterstützt.
Zeichenformate (MS Word)	In Word ist es möglich, das Format für die Listenzeichen anders zu wählen als das des Listeninhalts. Dies wird in Writer über die Zuweisung eine eigenes Zeichenformats für das Listenzeichen erreicht.
Zeichen- und Abstandsmetrik (MS Word)	I.d.R. sind die Zeichenabstände in Word etwas geringer als in Writer. Durch die Einführung des Druckerunabhängigen Layouts wurde dieser Unterschied in OOo1.1/SO7 erheblich verringert[4]. Beide Anwendungen benutzen auch unterschiedliche Maßeinheiten für vertikale Abstände (Word = Punkte, OOo/SO = Inch). Dadurch kann die Anzahl der Zeilen zwischen den Anwendungen beim gleichen Dokument variieren.
Arbeitsblattgröße (MS Excel)	Ein einzelnes Arbeitsblatt in Calc kann maximal 32.000 Zeilen enthalten[5]. Excel hat dagegen ein Limit von 65.536 Zeilen. Bei einem Import eines Excel-Blattes mit mehr als 32.000 Zeilen verteilt Calc die Einträge auf mehrere Arbeitsblätter.

1 Makros sollten aber aufgrund der erheblichen Probleme, die sie für eine Migration darstellen, nur sehr restriktiv verwendet werden. Dies gilt sowohl für OOo/SO als auch für MS Office.

2 Laut Sun sollen 3D-Grafiken in OOo2.0/SO8 mit MS Office kompatibel sein.

3 Ist laut Sun ab OOo2.0/SO8 möglich

4 Laut Sun soll es ab OOo2.0/SO8 hier keine Unterschiede mehr geben.

5 Laut Sun wird die maximale Anzahl Zeilen in OOo2.0/SO8 auf 65536 erhöht.

Eigenschaft	Bemerkung
Pivot-Tabellen (MS Excel)	Excel unterstützt Pivot-Tabellen für komplexe Datenanalysen. In Calc gibt es hierfür ein vergleichbares Tool, „Datapilot“, welches aber weniger Analysefunktionen und keine dynamische Chart-Erstellung unterstützt. Bei einem Import eines Excel-Dokuments, in dem ein starker Gebrauch von Pivot-Tabellen gemacht wird, werden Funktionalitäten verloren gehen.
Chart-Typen (MS Excel)	Die Chart-Engine in Calc ist bei weitem nicht so leistungsfähig wie die in Excel. Für eine Reihe von Chart-Typen in Excel gibt es keine Entsprechungen in Calc. Beim Import entsprechender Dokumente versucht Calc einen möglichst ähnlichen Chart-Typ auszuwählen.
Merge Documents (MS Word)	Writer und Word unterstützen beide die Verwendung von sogenannten „Merge Documents“, hierbei handelt es sich um die Verknüpfung von z.B. Excel-Arbeitsblättern mit einem Word-Dokument. Diese Funktionalität ist bei Word etwas anders implementiert als in Writer und die verfügbaren Filter unterstützen diese Funktionalität nicht. Entsprechende Dokumente werden zwar mit den verknüpften Feldern importiert, allerdings muss die Verknüpfung mit der Datendatei manuell hergestellt werden.

3.13.5.6 Wichtige Untersuchungskriterien einer Bestandsanalyse

Bevor eine grundlegende Entscheidung für oder gegen eine Migration und daran anschließend eine detaillierte Planung möglich ist, muss im Rahmen einer Bestandsanalyse geprüft werden:

- was zu migrieren ist
- ob eine Migration möglich ist und
- welcher Aufwand damit verbunden sein wird.

Bei der Bestandsanalyse sollten die Dokumente auf folgende Kriterien hin untersucht und ggf. kategorisiert werden:

- Verfügbarkeit der Dokumente
  - Dokumente, die evtl. weiter zu bearbeiten sind
    Für diese Dokumente kann eine Konvertierung sinnvoll sein.
  - Dokumente, die maximal noch gelesen werden sollen
    Für diese Dokumente sollte, zumindest im Migrationsfall, eine Archivierung bzw. eine Konvertierung nach PDF oder beides in Erwägung gezogen werden. Hierdurch wird der Migrationsaufwand vermindert.
- Komplexität der Dokumente
  - einfache Dokumente
    Diese enthalten keine Makros, proprietäre Grafiken (wie z.B. WordArt), Vektorgrafiken, komplexe Formatierungen oder Elemente wie Fußnoten, Tabellen oder Indizes. Sie lassen sich am besten über eine Batch-

Konvertierung umwandeln (siehe Abschnitt „Konvertierungsverfahren“ im Kapitel 3.13.5.8).

- komplexe Dokumente
  Diese enthalten Makros, gemeinsame Komponenten, Absatz- und Seitenformatierung, proprietäre und Vektorgrafiken, viele Links und Querverweise, OLE-Objekte, Rahmen, Text-Boxen, Fußnoten, aktive Komponenten, Formularfelder, Formular-Controls, Formulare oder Tabellen, also eine Fülle verschiedenster Formatierungen und Elemente. Diese Dokumente erfordern in der Regel zusätzliche Planungen und sollten einzeln ausgewertet und umgewandelt werden.

❍ Komplexität der Vorlagen

- einfache Vorlagen
  Einfache Vorlagen bestehen aus generischem Text und entsprechender Formatierung, die als Ausgangspunkt oder grober Entwurf für neue Dokumente dienen. Gute Beispiele hierfür sind z.B. Modellbriefe, grundlegende Reports oder Protokolle. Für einfache Vorlagen bestehen die gleichen Konvertierungsoptionen wie für einfache Dokumente.
- komplexe Vorlagen
  Komplizierte Vorlagen enthalten Formfelder und Makros, die nicht immer leicht umzuwandeln und mit Hilfe der Entwicklungsumgebung von OOo/SO neu erstellt werden müssen oder gar einem Reengineering zu unterziehen sind.

❍ Verwendung von externen Datenquellen
Diese müssen in der Regel neu angebunden werden. Das ist grundsätzlich recht problemlos möglich. Zu diesen Datenquellen zählen u.a. Datenbanken und Excel-Dokumente.

❍ Integration externer Software
Hierbei gilt es zum einen den Umfang der Integration und die Anzahl der betroffenen Anwendungen zu untersuchen und zum anderen muss mit Blick auf Integration in OOo/SO die Verfügbarkeit des Quelltextes geprüft werden. Verwendet eine externe Software MS Office mittels der OLE/COM-Automation Schnittstelle, so kann stattdessen auch OOo/SO über diese Schnittstelle angebunden werden. Die aufgerufenen MS Office Funktionen müssen in entsprechenden OOo/SO Aufrufe übertragen werde

3.13.5.7 Vorbereitung der Konvertierung

Word-Dokumente

Viele Unterschiede beim Layout nach einer Konvertierung lassen sich auf „unsachgemäße“ Formatierungstechniken zurückführen. Um die Treue des Dokumentenlayouts zu erhöhen, sollte sichergestellt werden, dass der ursprüngliche Text „richtig“ formatiert wird bzw. wurde. Die folgenden Hinweise sollten bei der

täglichen Arbeit beachtet werden, auch wenn die Migration zum heutigen Zeitpunkt noch nicht stattfindet:

- Verwenden Sie Zeichen- und Absatz-Formatvorlagen anstelle von direkter Formatierung
- Entfernen Sie unnötige (Hard-)Returns zwischen Listeneinträgen zur Erzeugung zusätzlichen Leerraums zwischen einzelnen Bullets. Diese erzeugen bei der Konvertierung zusätzliche Bullets ohne Inhalte (leerer Listeneintrag).
- Erstellen Sie Tabellenspalten nicht mit Hilfe von Mehrfach-Tabs. Definieren Sie Tab-Stops, so dass nur ein Tab den Text zwischen zwei Spalten separiert. Alternativ kann das Tool zur Erstellung von Tabellen verwendet werden. Bei der Verwendung von Mehrfach-Tabs kann es vorkommen, dass eine Tabelle nach einer Konvertierung „out of range“ ist, weil die beiden Anwendungen unterschiedliche Default-Tabs verwenden.
- Überprüfen Sie, dass das Seitenformat im Dokument identisch mit der Druckerseitengröße ist. OOo/SO nimmt keine automatische Justierung vor, um eine korrekte Druckausgabe sicherzustellen.

Excel-Dokumente

Große und komplexe Spreadsheets bedürfen einer genauen Überprüfung hinsichtlich evtl. verwendeter besonderer Formatierungstechniken und enthaltener Logik (Formeln, Add-Ins), um sicherzustellen, dass diese korrekt umgewandelt werden können. Dies betrifft insbesondere 3rd-Party - und Standard-Excel - Add-Ins.

Einige der betroffenen Bereiche werden im Folgenden kurz aufgeführt und erläutert:

- Überprüfen Sie die Einstellungen für Datenquellen von Charts. Grundsätzlich ist Excel sehr viel flexibler hinsichtlich der Datenbereiche von Charts als dies Calc ist. OOo/SO verlangt z.B., dass die Label immer in der ersten Zeile oder Spalte angeordnet sind. Ist dies nicht der Fall, werden in der Regel die Charts ohne Labels importiert.
- Liegt ein Passwortschutz für Dokumente vor? Calc kann keine passwortgeschützten Excel-Spreadsheets öffnen[1]. Vor der Konvertierung muss der Schutz also aufgehoben werden.
- Vermeiden Sie Array-Konstanten in Formeln. Calc unterstützt in Formeln keine Array-Konstanten wie in Excel (z.B. {1,2;3,4}) sondern nur Zellenbereiche die ein Array spezifizieren (z.B. {A1:B2}).

[1] Laut Sun ab der nächsten Version möglich.

- Vermeiden Sie Sonderzeichen in den Namen von Arbeitsblättern. Excel unterstützt mehr Sonderzeichen in der Bezeichnung von Arbeitsblättern als Calc.
- Vermeiden Sie Arbeitsblätter mit mehr als 32.000 Zeileneinträgen und Spreadsheets mit mehr als 256 Arbeitsblättern, da Calc derzeit nicht mehr Einträge unterstützt (siehe auch 3.13.5.4).
- Vermeiden Sie unterschiedliche Ansicht-Einstellungen für verschiedene Arbeitsblätter, die von Excel unterstützt werden. In Calc können solche Einstellungen nur global für das gesamte Dokument vorgenommen werden.
- Prüfen Sie die Zellengröße hinsichtlich rechts ausgerichteten Textes, dieser wird, wenn die Zelle zu klein ist, nicht nach links über die Zelle hinaus verlängert[1].

PowerPoint-Dokumente

Einfache PowerPoint-Präsentationen werden normalerweise ohne Probleme durch Impress korrekt übernommen. Präsentationen, die erweiterte Layoutfunktionen und Effekte verwenden, führen in der Regel zu einer unterschiedlichen Darstellung im konvertierten Dokument.

Die nachfolgend aufgelisteten Maßnahmen sollen helfen, die ursprüngliche Formatierung zu erhalten:

- Vermeiden, entfernen oder ändern Sie Schatten-Objekte, die nicht durch Impress unterstützt werden. Impress unterstützt nicht alle Schatten-Formate aus PowerPoint. Die Abbildung (Bild 45) zeigt die Konvertierung der Schatten aus PowerPoint nach Impress.
- Vermeiden, entfernen oder ändern Sie die Objektattribute
  - dreifarbiger Farbverlauf
  - doppelt und dreifach linierte Ränder.

  Diese werden durch Impress nicht unterstützt. Für eine Konvertierung sollten diese in
  - zweifarbigen Farbverlauf
  - einfach linierte Ränder

  abgeändert werden. Die abgerundeten Ränder werden automatisch in eckige Ränder umgewandelt.
- Fehlende Informationen in den Dokumenteneigenschaften.
  Anders als in PowerPoint wird in Impress nicht das Datum des letzten Zugriffs gespeichert. Außerdem werden die PowerPoint Dokumentenei-

[1] Ab OOo2.0/SO8 bedarf dieser Punkt keiner Beachtung mehr.

genschaften nicht mit in das konvertierte Dokument importiert. Beide Mängel können, wenn der Bedarf besteht, mittels Makros nachgebildet bzw. umgangen werden.

- Fehlende Unterstützung hinsichtlich „Erzählung aufzeichnen“
  Impress unterstütz kein „Erzählung aufzeichnen“ wie in PowerPoint. In Impress kann zu jedem Slide ein eigenes Soundfile angelegt werden. Um die Aufzeichnungen aus PowerPoint weiter nutzen zu können, müssen diese entweder neu aufgezeichnet oder über ein Splittingverfahren[1] konvertiert werden.

Bild 45: Schatten-Objekte PowerPoint und Impress[2]

3.13.5.8 Durchführung der Konvertierung

Konvertierungsverfahren

Die Konvertierung der MS Office Dokumente nach OOo/SO kann mit der Software entweder als Einzel- oder als Batch-Konvertierung durchgeführt werden:

- Einzelkonvertierung
  Das MS-Dokument wird mit OOo/SO geöffnet und als OOo/SO-Dokument gespeichert.
- Batch-Konvertierung
  Die betroffenen Dokumente werden in ein entsprechendes Verzeichnis (sollte speziell hierfür angelegt werden) kopiert. Über die OOo/SO-Funktion „Datei/Autopilot/Dokumentenkonverter“ kann dann der Batch-Prozess initiiert werden. Hier wird zunächst das Quellformat (MS oder OOo/SO) gewählt (siehe Bild 46) und anschließend definiert, ob es sich

[1] Nachzulesen im „StarOffice 6.0 Software Migration Guide“ Seite 47 „Re-record or split narration“.

[2] Quelle: StarOffice 7™ Migration Guide; http://se.sun.com/edu/staroffice/so_migration_guide_0104.pdf

um Dokumente oder Vorlagen handelt und in welchem Quellverzeichnis diese zu finden sind. Ferner ist festzulegen, in welchem Zielverzeichnis die konvertierten Dokumente abgelegt werden sollen (siehe Bild 47). Abschließend werden alle MS-Dokumente des Quellverzeichnisses konvertiert und als OOo/SO-Dokumente im Zielverzeichnis abgelegt.

Bild 46: Dokumentenkonverter: Auswahl des Quellformats

Bild 47: Dokumentenkonverter: Auswahl des Quell- und Zielverzeichnisses

Wie aus der vorhergehenden Abbildung (Bild 47) zu ersehen ist, kann der Dokumentenkonverter zwischen Dokumenten und Dokumentenvorlagen unterscheiden. Der wesentliche Unterschied dabei ist, dass die MS Office Vorlage auch als OOo/SO-Vorlage gespeichert wird.

Welche Konvertierungsform zu einem bestimmten Zeitpunkt die Günstigste ist, ist abhängig von der Komplexität der Dokumente oder der Vorlagen (siehe Kapitel 3.13.5.6).
Außerdem ist jene Situation näher zu betrachten, in der Makros, OLE/COM-Steuerung oder die Integration externer Anwendungen, betroffen sind. Diese müssen dann neu erstellt werden.

Konvertierungsoptionen

Zur Optimierung der Batch- oder Einzelkonvertierung gibt es in OOo/SO noch Kompatibilitätseinstellungen in den Optionen, die vorzunehmen sind[1].

Überprüfung der konvertierten Dokumente

Nach einer Konvertierung ist es sinnvoll, die konvertierten Dokumente auf die Übernahme folgender Einstellungen zu überprüfen:

- Ränder
- Tabs
- Einrückungen
- Zeilenlängen (Text pro Zeile)
- Zeilenabstände innerhalb von Absätzen
- Abstände zwischen Absätzen
- Tabellen
- Kopf- und Fußzeilen
- Listen
- Grafiken.

Sonstige Konvertierungsmaßnahmen

Neben der grundsätzlichen Konvertierung von bestehenden Dokumenten und Vorlagen besteht evtl. der Bedarf, die bestehenden Autotexteinträge sowie die über lange Zeit erstellten Benutzerwörterbücher mit in das neue System zu übernehmen.

Die Überführung der Autotexteinträge aus den vorhandenen Vorlagen nach OOo/SO kann automatisiert vorgenommen werden[2].

---

1 Siehe „StarOffice 7™ Migration Guide" Seite 39 - 540; http://se.sun.com/edu/staroffice/so_migration_guide_0104.pdf"

2 Im Einzelnen wird dies im „StarOffice 7™ Migration Guide", Seiten 55 – 56 beschrieben.

Sowohl MS Office als auch OOo/SO unterstützen die Erstellung und Verwaltung von Benutzerwörterbüchern. In beiden Anwendungen haben Wörterbücher die Endung „.dic“, sind aber nicht kompatibel zueinander. MS Office speichert seine Wörterbücher als einfache Text-Dateien, wohingegen die Wörterbücher in OOo/SO in einem proprietären Format abgelegt werden. Eine automatisierte Übernahmeroutine gibt es hierzu bisher noch nicht.

3.13.5.9 Integration externer Anwendungen

Bei den externen Applikationen spielt mit Blick auf eine mögliche Migration nach OOo/SO der Grad der Integration in die MS Office Suite eine wichtige Rolle. Viele der heute in den Behörden eingesetzten Fach- und Standardanwendungen sind speziell für einen Einsatz in einer MS Windows geprägten Systemumgebung konzipiert und machen starken Gebrauch von den proprietären Windows API-Modulen wie:

- MAPI
- COM
- DDE
- ...

Der Grad der Integration in die Windowsumgebung kann hierbei ganz unterschiedlich sein. Eine einfache und noch recht unproblematische Integration ist die Nutzung der MAPI-Schnittstelle, um aus einer Anwendung heraus auf den Standard E-Mail-Client zuzugreifen. Ein weitaus höherer Grad an Integration liegt sicherlich dann vor, wenn eine externe Anwendung nur bestimmte MS Anwendungen zulässt bzw. diese sogar zwingend benötigt werden, um die volle Funktionalität dieser Anwendung nutzen zu können.

Diese Unterschiede im Grad der Integration von externen Anwendungen in Windows und in die MS Office Suite erfordern eine genaue Prüfung, ob eine Migration technisch machbar und welcher Aufwand damit verbunden ist. Sofern der Source Code der externen Anwendung verfügbar ist, muss im Einzelfall geprüft werden, ob eine Integration in OOo/SO über die von OOo/SO bereitgestellte Schnittstelle UNO[1] (Universal Network Objects) möglich ist.

3.13.5.10 Migration von Makros und OLE/COM-Steuerungen

Makros und OLE/COM sind eine intensiv genutzte Methode zur Erweiterung der Office-Funktionalitäten und zur Office-Automation unter Windows (siehe Kapitel 3.13.4.2). Die Nutzung geht hin bis zur Automation von ganzen Workflows innerhalb einer Organisation zwischen einzelnen Abteilungen. Da die Makros und Scriptings in erster Linie auf VBA basieren, lassen sich diese unter OOo/SO nicht ausführen. Für eine automatisierte Migration nach OOo/SO gibt es verschiedene Werkzeuge, welche die vorhandenen Dokumente und Vorlagen analysieren und

[1] Mehr zu UNO findet sich unter http://udk.openoffice.org/common/man/uno.html .

weitestgehend automatisiert die vorhandenen Makros aus MS Office nach StarBasic konvertieren. Leider stehen diese Werkzeuge nicht als freie Software zur Verfügung. Es ist sogar so, dass diese Werkzeuge noch nicht einmal frei auf dem Markt erworben werden können. Sun stellt diese Werkzeuge nur über seine Migrationspartner zur Verfügung. Daher ist es notwendig genau zu prüfen welcher Weg wirtschaftlicher ist,

- die manuelle Überführung bzw. neu Erstellung oder
- die Beauftragung eines Migrationpartners von Sun.

Grundsätzlich sollte zuvor genau geprüft werden, welche der bestehenden Makroprogrammierungen weiterhin zwingend benötigt wird bzw. ob es nicht andere Lösungen gibt, die flexibler und plattformunabhängiger sind.

Dies bietet gleichzeitig die Möglichkeit einer Konsolidierung der Makro- und OLE/COM-Anwendungen sowie einer Neuorientierung in der IT-strategischen Ausrichtung hinsichtlich der Büroautomation. In diesem Zusammenhang folgt an dieser Stelle ein kleiner Exkurs, in dem eine beispielhafte Lösung vorgestellt wird, die im Rahmen des Migrationsprojektes „OSS-Desktop“ entwickelt wurde.

Exkurs Dokumentgenerator

Im Rahmen des Pilotprojektes „OSS-Desktop“ wurde für das Bundesministerium der Justiz eine Anwendung entwickelt, die zur standardisierten, IT-gestützten Erzeugung von Dokumenten dient. Der Dokumentgenerator automatisiert die Nutzung von Adressen, sowie die Erstellung von Verarbeitungs- und Inhaltsbereichen innerhalb von Dokumenten. Der Dokumentgenerator löste eine auf VBA-Makros basierende Anwendung ab. Da die ursprüngliche Altanwendung keine Unterstützung von OpenOffice bzw. StarOffice bot, war in einer heterogenen Office-Umgebung nicht einsetzbar und musste somit abgelöst werden. Der Dokumentgenerator wird unter einer GPL Lizenz entwickelt und steht somit allen Interessenten frei zur Verfügung. Die Anwendung wurde von der tarent GmbH[1] entwickelt.

Der Dokumentgenerator dient zur Erstellung und Bearbeitung unterschiedlicher Dokumenttypen, wie sie für die tägliche Arbeit benötigt werden. Im BMJ werden beispielsweise Verfügungen und Reinschriften in unterschiedlicher Ausprägung erstellt, entweder als Vermerk, Verfügung, Ministervorlage oder Staatssekretärvorlage.

Gegenüber anderen Lösungen, die ausschließlich die Skript und Makroschnittstellen von Microsoft Word oder OpenOffice.org/StarOffice nutzen, wurde der Dokumentgenerator in Java geschrieben und stellt damit eine einheitliche Lösung sowohl für Linux- als auch Windowsbasierte Clientsysteme dar. Der Dokumentgenerator unterstützt weiterhin die Textverarbeitungsanwendungen OpenOffice.org/Staroffice als auch Microsoft Office. Die folgende Auflistung gibt die vom Dokumentgenerator unterstützten Officesuiten wieder:

[1] Maintainer des Dokumentgenerators: www.tarent.de

- Staroffice 7
- OpenOffice.org 1.x
- Microsoft-Office 97, 2000, 2002 und 2003

Der Dokumentgenerator ist in Java implementiert und benötigt für die Nutzung eine entsprechende Laufzeitumgebung (Java-Laufzeitumgebung ab Version 1.4) auf den jeweiligen Clientsystemen. Die Anwendung ist in die jeweiligen Office-Oberflächen (Menü, Symbolleisten) mit den jeweils officespezifischen verfügbaren Technologien integriert (StarBasic/VBA). Da es sich hierbei in der Regel nur um die Aufrufe der Anwendungsdialoge handelt, ist diese Integrationsschicht sehr klein und damit auch in der Pflege unkritisch. Der Dokumentgenerator realisiert die gesamte Logik und Automatismen, die ursprünglich durch die Verwendung von VBA-Makros implementiert wurden. Er verwendet einfache Dokumentvorlagen der jeweiligen Officesuiten zur Bereitstellung des Enddokuments. Die Anwendung trennt deutlich zwischen Anwendungslogik und Präsentationsschicht, somit wird eine Unabhängigkeit von der jeweiligen Officeumgebung erreicht und auf den spezifischen Einsatz von Makros kann verzichtet werden. Die noch benötigen Dokument-Vorlagen können vom Anwender oder den Administratoren mit Hilfe von Platzhaltern und Formatvorlagen selbst gestaltet und den jeweiligen Anforderungen angepasst werden. In der folgenden Abbildung wird die grundsätzliche Architektur des Dokumentgenerators dargestellt.

Bild 48: Architektur des Dokumentgenerators

Der Nutzer führt die Erstellung der jeweiligen Dokumente mit seinem gewohnten Office-Programm durch und empfindet den Dokumentgenerator durch die Integration in die jeweiligen Office-Oberflächen als Teil der Officelösung. Der Nutzer kann den Dokumentgenerator über eine eigene Symbolleiste oder über das An-

wendungsmenü bedienen. Die Dialoge des Dokumentgenerators erscheinen als „Kindfenster“ der jeweiligen Textverarbeitung und sind mit dieser fest verbunden.

Bei der Erstellung von Dokumenten, insbesondere Anschreiben, können die Adressaten der Schreiben aus Adresskatalogen ausgewählt werden. Die Adresskataloge können über Dialoge des Dokumentgenerators gepflegt werden. Bei den Adresskatalogen werden zum einen persönliche Kataloge, diese sind durch den Nutzer frei bearbeitbar, und zum anderen schreibgeschützte Kataloge, die von zentraler Stelle bereitgestellt werden, unterschieden. Die Bereitstellung der Adressdaten kann sowohl über einfache Textdateien als auch mittels Datenbanksysteme erfolgen. Die Textdateien verfügen unter Windows- als auch Linux-basierten Systemen über das gleiche Datenformat. Als weiteres Format kann der Dokumentgenerator Adressen im vcard-Format verwenden, wie sie zum Beispiel aus verschiedenen Groupwarelösungen oder Microsoft Outlook exportiert werden können. Eine weitere Variante ist die Nutzung eines zentralen LDAP Verzeichnisdienstes für die Bereitstellung von Adressinformationen.

3.13.5.11 Programmierumgebung von OOo/SO

OOO/SO besitzt genau wie MS Office auch eine API[1]. Das OOo/SO API ist unabhängig von einer Programmiersprache oder einem Betriebssystem formuliert. Derzeitig lässt sich OOo/SO in den Programmiersprachen Java, C++, StarBasic und unter Windows mittels OLE/COM-Steuerung programmieren. Alle Programmiersprachen verwenden dabei das gleiche API, d.h. es sind die gleichen Aufgaben möglich. Sowohl Java als auch C++ erlauben außerdem die Entwicklung von Komponenten, die als Plug-In innerhalb von OOo/SO verschiedenste Aufgaben erfüllen können:

- Neue Chart-Typen
- Neue Calc Funktionen
- Wizards
- Zusätzliche Funktionalität für den Benutzer
- StarBasic Erweiterung.

StarBasic ist die integrierte modulare Skriptsprache in OOo/SO und folgt gleichen Prinzipien wie VBA. Struktur und Syntax beider Sprachen sind in großen Teilen sehr ähnlich, so dass ein versierter VBA-Programmierer keine größeren Schwierigkeiten bei der Übertragung von VBA-Makros haben wird.

Neben der API stellt OOo/SO genau wie MS Office eine Entwicklungsumgebung (Integrated Development Environment (IDE)) zur Verfügung, deren Benutzer-

[1] Alle wesentlichen Informationen hierzu sind unter folgender Web-Adresse zu finden http://api.openoffice.org/ (Onlinedokumentation). Die Spezifikation der Schnittstelle kann unter der URL http://udk.openoffice.org/ nachgelesen werden.

schnittstelle sehr an die der Entwicklungsumgebung von MS Office angelehnt ist[1].

3.13.6 Fortführende Migration

Bei der fortführenden Migration muss in erster Linie die Migration von Office 97 nach Office 2003 betrachtet werden, da zwischen diesen beiden Versionen die für eine Migrationsbetrachtung wesentlichen Änderungen vollzogen wurden. Bei einem Wechsel von Office 2000 nach Office 2003 sind die zu betrachtenden Änderungen nicht mehr so markant bzw. wurden bereits vollzogen und werden bei einer Betrachtung der Migration von Office 97 nach Office 2003 mit berücksichtigt. Versionen von MS Office vor der Version Office 97 werden hier nicht weiter betrachtet.

Die Neuerungen in Microsoft Office 2003 gegenüber Office 2000/97 liegen insbesondere im Bereich der Benutzerschnittstelle, der XML-Unterstützung (siehe Kapitel 3.13.6.3) sowie im Bereich Teamarbeit, wobei dieser Teil der zusätzlichen Funktionen in erster Linie Groupware-Funktionalitäten abdeckt bzw. erweitert, die bereits mit anderen Anwendungen abgedeckt werden[2]. Für die tägliche Arbeit ergeben sich dadurch nur in einigen Anwendungsfällen Änderungen. Auf die neuen Funktionalitäten von Office 2003 wird daher nur in ausgewählten Zusammenhängen eingegangen. Im Besonderen sind dies:

- Konvertierung vorhandener Dokumente
- XML-Implementierung in Office 2003
- Smarttags und ihre Erweiterungen in Office 2003
- Besonderheiten der Windows Sharepoint Teamservices

Eine weitere Neuerung in den Office 2003 Paketen ist die neue Einzelanwendung InfoPath (siehe Kapitel 3.9.3.2). InfoPath dient zur formularorientierten Bearbeitung von XML-Dokumenten. Es wird von Microsoft genau wie Project und Visio als Spezialanwendung[3] von Office 2003 eingestuft und daher an dieser Stelle nicht weiter betrachtet.

Erwähnenswert ist die Aufnahme von InfoPath in die Office-Produktpalette allerdings in strategischer Hinsicht. Sie unterstreicht die wachsende Bedeutung der Office-Suiten als Desktop- bzw. Client-Komponente zentralisierten Backend-Prozessen (siehe Kapitel 3.9 und 3.13.3). In diesem Zusammenhang wird InfoPath näher vorgestellt (siehe Kapitel 3.9.3.2).

---

1 Weitere Hinweise zum Umgang mit der Programmier- und Entwicklungsumgebung sind im "StarOffice 6.0 Migration Guide" Seiten 79 –90 zu finden.

2 Einzelheiten zu den neuen Features im Vergleich zu früheren Versionen finden sich unter http://www.microsoft.com/germany/office/editionen/verbesserungen/vergleich.mspx

3 http://www.microsoft.com/germany/office/editionen/default.mspx

3.13.6.1 Konvertierung vorhandener Dokumente

An den binären Dateiformaten hat sich im Wesentlichen nichts geändert. Diese können einfach mit den entsprechenden Office 2003 - Anwendungen geöffnet werden. Allerdings gibt es keine verlässlichen Erfahrungswerte, die bestätigen, dass dies für alle Formatierungen, Vorlagen, Makros und Scriptings reibungsfrei funktioniert. Insbesondere die Änderungen im Objektmodell (siehe 3.13.6.2) führen dazu, dass es zu Problemen bei der Konvertierung von Dokumenten aus Office 97 nach Office 2003 kommen kann.

Genau wie bei OOo/SO gibt es auch in Office 2003 die Möglichkeit einer Batch-Konvertierung, die mit Hilfe des „Stapelkonversions-Assistenten“ durchgeführt wird. Neben dem Standard-Konvertierungsfilter bietet Microsoft noch ein „Office Konverter Pack“[1] als weitere Unterstützung an.

Kompatibilät zu früheren Versionen

Die binären Dateiformate von Office 97, 2000, XP und 2003 sind grundsätzlich kompatibel, alle Dokumente können im Allgemeinen in jeder Version geöffnet, bearbeitet und wieder gespeichert werden.

Wenn Office 2003 Dokumente mit Office 97 geöffnet werden, kann es zu Darstellungsproblemen kommen. Einzelne neue Funktionen und Formatierungsmöglichkeiten aus Office 2003 werden dann in Office 97 nicht dargestellt. Diese gehen aber laut Whitepaper „Microsoft Office 2003 and File Sharing in a Heterogeneous Office Environment“[2] bei einer Bearbeitung mit Office 97 nicht verloren und können beim nächsten Öffnen in Office 2003 weiterverwendet werden.

3.13.6.2 Programmierumgebung

Neuerungen

VBA-Versionen

Gegenüber Office 97 hat es einige wesentlichen Änderungen in der Programmierumgebung von Microsoft Office 2003 gegeben. Eine der wichtigsten Änderungen ist dabei der Wechsel von VBA Version 5 nach Version 6. Mit diesem Versionswechsel, der schon mit Office 2000 vollzogen wurde, hat auch eine deutliche Änderung im „Object Model“ stattgefunden. Dies hat nicht unerhebliche Auswirkungen auf die Migration von Makros, Scriptings und Integrationen externer Anwendungen, die noch auf dem Object Model der Version 5 basieren. Wer die Migration von Office 97 nach Office 2000 schon vollzogen hat, hat damit bereits die entscheidende Hürde überwunden. Mit Office XP und Office 2003 gab es zwar weitere Wechsel in den VBA-Versionen, nämlich zu Version 6.3 in XP und Version 6.4 in 2003, die jedoch nicht das Object Model berührten.

---

1 http://office.microsoft.com/en-us/assistance/HA011513581033.aspx

2 Microsoft Office 2003 and File Sharing in a Heterogeneous Office Environment
www.microsoft.com/technet/prodtechnol/office/office2003/operate/o03flshr.mspx

.NET-Lösungen mittels Visual Studio Tools für Office[1]

Mit Office 2003 gibt es auch die Möglichkeit, von Microsoft als „intern“ bezeichnete[2] auf .NET basierende Lösungen (Office-Automatisierungen) zu entwickeln und zu nutzen. Microsoft .NET basierende Office-Automatisierungen können schon länger erstellt werden, allerdings nur als „externe“ Automatisierungen, Microsoft meint hiermit Lösungen, die Office-Anwendungen nur aufrufen, wenn Sie deren Funktionen nutzen wollen. Mit den Visual Studio Tools für Office bietet sich nun die Möglichkeit, .NET-Programm-Code mit einem bestimmten Dokument zu verknüpften und ihn auszuführen, wenn bestimmte Bearbeitungsereignisse eintreten. Möglich ist dies für Word- und Excel-Dokumente.

In der einfachsten Form bestehen solche Lösungen, die mit den Microsoft Visual Studio-Tools für Microsoft erstellt wurden, aus zwei Dateien,

- einem Word- bzw. einem Excel-Dokument und
- einer .NET-Assembly (siehe Kapitel 3.9.5), die von Visual Studio .NET als DLL-Datei kompiliert wird.

Mit einen Word- oder Excel-Dokument verknüpft werden diese beiden Dateien mit Hilfe benutzerdefinierter Eigenschaften im Dokument. Damit besteht auch die Möglichkeit „Managed Code“ (siehe Kapitel 3.9.5) in der Office-Automatisierung zu verwenden. Die nachfolgende Abbildung (Bild 49) zeigt die typische Architektur einer solchen Lösung.

Bild 49: Typische Architektur einer Visual Studio Tools für Office Lösung[3]

---

1 Die nachfolgenden Darstellungen basieren auf Informationen von Microsoft, die unter „MSDN Home > Visual Studio .NET > Visual Basic und Visual C# verfügbar sind: http://msdn.microsoft.com/library/deu/default.asp?url=/library/DEU/dv_wrcore/html/oriIntegratingOfficeComponents2.asp

2 Neues bei der Programmierung mit Office

3 Quelle: Microsoft http://msdn.microsoft.com/library/deu/default.asp?url=/library/DEU/dv_wrcore/html/wrconwhiterabbitarchitecture.asp

Der offensichtliche Unterschied zu vielen VBA-Lösungen liegt nun darin, dass der Programm-Code selbst nicht Bestandteil des Word- oder Excel-Dokumentes ist, sondern vom Dokument lediglich referenziert wird (einige weitere Unterschiede werden später angesprochen).

Der Ablauf beim Ausführen einer solchen Lösung sieht wie folgt aus: Mit dem Öffnen des jeweiligen Office-Dokumentes wird durch das Ladeprogramm in Word oder Excel die .NET-CLR (siehe Kapitel 3.9.5) gestartet. Diese wiederum lädt die Assembly.

Mit Hilfe der CLR kann Managed Code genutzt werden, der in einer beliebigen vom Microsoft .NET Framework unterstützten Sprache verfasst wurde. Die Entwicklungsunterstützung in den Visual Studio Tools für Office 2003 beschränkt sich jedoch noch auf Microsoft Visual Basic® .NET and Microsoft Visual C#® .NET[1].

Die wesentlichen Vorteile gegenüber VBA sind die Folgenden:

- Wie bereits erwähnt liegt der Code nicht mehr direkt im Office-Dokument.
- Die Entwicklerumgebung ist nicht Bestandteil von Microsoft Office 2003. Sie muss separat erworben werden und steht damit i.d.R. nicht jedem Benutzer automatisch zur Verfügung. Dies lässt hoffen, dass zukünftig weniger unkontrolliert und unkoordiniert Office-Automatisierungen erstellt und genutzt werden.
- Die Sicherheitsumgebung (CAS) (siehe Kapitel 3.9.5) des .NET-Frameworks sorgt dafür, dass Code nicht mehr unkontrolliert ausgeführt werden kann. Damit verringert sich auch die Gefahr von Makroviren, insbesondere, wenn zugleich auf die Nutzung von VBA-Automatisierungen vollständig verzichtet wird.
- Das traditionelle „Object Model“ kann auch mit diesen Lösungen genutzt werden. Der Managed Code kommuniziert mit den Office-COM-Komponenten durch die so genannten Primary Interop Assemblies (PIA).

Die Entwicklung der Visual Studio Tools für Office steht noch am Anfang, und Microsoft wird auch VBA vorläufig noch weiter unterstützen[2]. Grundsätzlich scheint der Weg aber weiter in Richtung .NET zu gehen.

Migration von Makros, Scriptings und der Integration externer Anwendungen

Die Hauptschwierigkeit bei einer Migration nach Office 2003 liegt in den Änderungen innerhalb der Programmierumgebung von Office. Dabei ist insbesondere der Wechsel im „Object Model“ ausschlaggebend. Vor allem die Änderung in der

---

1 Quelle: http://msdn.microsoft.com/vstudio/office/officetools.aspx

2 http://msdn.microsoft.com/office/understanding/vsto/articles/default.aspx?pull=/library/en-us/dno2k3ta/html/odc_ofcomparevba6andvsto.asp#odc_ofcomparevba6andvsto_isvba60goingaway

Methode zur Einbindung von Objekten hat Auswirkungen auf die Kompatibilät zu früheren Versionen und damit auf die Migration.

Grundsätzlich ist davon auszugehen, dass Officeanwendungen (Makros, Scriptings, externe Anwendungen), die in der Programmierumgebung von Office 97 entwickelt wurden, problemlos auch in einer Office 2003-Umgebung eingesetzt werden können, ohne dass Anpassungen vorzunehmen sind. Trotz einer grundsätzlich vorhandenen Abwärtskompatibilität schließt auch Microsoft nicht aus, dass es Ausnahmen geben kann, die eine Anpassung erforderlich machen[1].

Ungleich problematischer stellt sich dies in einer umgekehrten Situation dar. Das heißt, dass neuere Anwendungen, die für Office 2003 entwickelt wurden, nur schwerlich in einer Office 97-Umgebung fehlerfrei genutzt werden können. Dies gilt insbesondere für Makros und muss beachtet werden, wenn innerhalb einer Organisation keine vollständige bzw. eine sukzessive Umstellung erfolgt und beide Office-Versionen eingesetzt werden.

Aufgrund der Unsicherheit, ob denn auch alle Officeanwendungen weiterhin genutzt werden können bzw. ob Anwendungen ggf. anzupassen sind, macht es erforderlich, analog zur ablösenden Migration eine genaue Bestandsanalyse der vorhandenen Makros, Scriptings und externen Anwendungen durchzuführen.

3.13.6.3 Das XML-Dateiformat in Office 2003

Die Office 2003-Versionen von Word und Excel bieten die Möglichkeit, ihre Dokumente als XML-Dateien zu speichern. Diese Funktionalität unterliegt allerdings drastischen Einschränkungen. Beispielsweise gehen beim Speichern einer Excel-Mappe in einer XML-Datei die Diagramme verloren. Werden darüber hinaus Word-Dokumente mit eingebetteten Excel-Arbeitsblättern als XML-Datei gespeichert, dann enthalten diese nicht einmal das Arbeitsblatt als XML, sondern stattdessen einen druckbar kodierten Binärblock (Auszug):


```
<w:docOleData><w:binData w:name="oledata.mso">
EAAAAgAAAAEAAAD+////AAAAAAAAAAAD/////////////////////////////////////////////
/////v////7///8EAAAABQAAAAYAAAD+/////////////////////////////////////////////
AAAAAAAWAAUA/////////8BAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAFAUqEb09sQB
AwAAAMAHAAAAAAAAXwAxADEANgA2ADgANQA3ADAAMAAzAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
W/4qSGgXHcISgQ9Pn5oRjL8BMAf8skd8x0gp3wsrz82hCyWf5R3rQ9bDvsagN81jsvedI96He9jP
rGndHg5cLaoXHVoV69CHsS5HTtFz4I6h7+BGjz8gsW3uZNGySJ7F8nxD3vlQnstR80VyHnWUeQqX
xaQ2oVk52OmU5jpLq+wt7D6CSINpa0Py9JvbcGBZkEnoJryUTWSq/kqBg+tscXvx/op04tzTkUls
XdXdoGuM/gbBLTCfAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA==
</w:binData></w:docOleData>
```


Standard-Dateiformat beider Anwendungen ist weiterhin das bekannte Binärformat (*.doc, *.xls etc.). Die Speicherung als XML-Dokument kann fallweise gewählt werden, aber auch per Konfiguration als Standard eingestellt werden.

[1] "Microsoft® Office Resource Kit, Technischer Artikel (Whitepaper), Probleme bei der Migration von Microsoft Office 97 zu Microsoft Office 2003" (Office_97-03_Delta.doc).

Die verwendeten XML-Schemata sind Microsoft-spezifisch und werden als "Office 2003 XML Reference Schemas" bezeichnet. Sie umfassen eine Reihe einzelner Schemata: WordProcessingML (früher WordML), SpreadsheetML, DataDiagrammingML (Visio, kein Bestandteil von Office 2003) und FormTemplate XML-Schemas (InfoPath, siehe Kapitel 3.9.3.2). Die Schemata sind nach Aussage von Microsoft vollständig dokumentiert und stehen auf der Microsoft-Website zum Download bereit[1]. Bereitgehalten werden sie allerdings lediglich als selbstextrahierende, ausführbare Dateien für Windows 2000 Service Pack 3, Windows Server 2003 und Windows XP. Nutzer anderer Betriebssysteme werden von Microsoft auf die Website der OIO-Infostructurebase des dänischen Technologieministeriums verwiesen[2].

Die Office 2003-Schemata nebst Dokumentation können indes unter Auflagen von Jedermann weiterverbreitet werden. Anwendungen, die Office 2003-kompatible XML-Dateien lesen und/oder schreiben, können unter einer so genannten Patent-Lizenz entwickelt und vertrieben werden, die ihrerseits Auflagen enthält. Allgemein herrscht eine gewisse Unklarheit über die Stichhaltigkeit und mögliche Konsequenzen dieses Lizenzmodells, insbesondere darüber, ob es die Implementationen von Office 2003-kompatiblen Anwendungen unter Open Source-Lizenzen behindern kann[3]. Microsofts sagt zu, Updates der Office 2003-Schemata sowie "künftige Versionen dieser Spezifikationen" zu den gleichen Bedingungen zugänglich zu machen. Für die Schemata künftiger Office-Generationen behält sich Microsoft ausdrücklich eine andere Lizenzgestaltung vor.

Ergänzende XML-bezogene Funktionalitäten in Office 2003

Wie beschrieben, bieten Word und Excel eingeschränkte Möglichkeiten, ihre Dokumente in XML-Dateien zu speichern. Darüber hinaus bieten beide Anwendungen die Möglichkeit, Passagen im Dokument mit benutzerdefinierten XML-Schemata auszuzeichnen. Dieses Leistungsmerkmal ist jedoch auf die selbständigen Versionen sowie auf die in der Office 2003 Professional Edition enthaltenen Versionen der Anwendungen beschränkt.

Die Funktionalität ist in beiden Anwendungen unterschiedlich ausgestaltet. Word 2003 verwaltet eine so genannte Schemabibliothek, in die alle benutzerdefinierten Schemata eingefügt werden. Einem Dokument kann eines oder mehrere dieser Schemata zugeordnet und die zugeordneten Schemata für die Auszeichnung verwendet werden. Die folgende Abbildung (Bild 50, S. 311) zeigt ein Word 2003-Dokument, das mit dem eingangs vorgestellten Telefonbuch-Schema assoziiert ist. Wie bei XML-Editoren üblich zeigt der "XML-Struktur"-Aufgabenbereich rechts dem Benutzer einerseits die Struktur der eingefügten Auszeichnungen und weist

1 http://www.microsoft.com/office/xml/default.mspx

2 http://isb.oio.dk/info

3 Microsoft hat eine Reihe von Klarstellungen veröffentlicht und auch die Lizenz in diesem Sinne erweitert, ohne jedoch die genannten Fragen klar zu beantworten.

ihn auf Schema-Verletzungen hin, andererseits unterstützt er ihn kontextsensitiv bei der Auswahl möglicher Auszeichnungen.

Häufig wird unterschieden zwischen technisch-semantisch unstrukturierten herkömmlichen Office-Dokumenten und konsequent strukturierten Daten, wie sie mit InfoPath bearbeitet werden (siehe Kapitel 3.9.3.2). Wie die Abbildung zeigt, eröffnet Word 2003 einen dritten Weg: in beliebig gestaltbare, unstrukturierte Textdokumente werden einzelne Inseln mit ausgezeichneter Struktur eingebettet.

Die Komplexität von Schemata, die sich für die unmittelbare, interaktive Verwendung durch einen menschlichen Benutzer eignen, hat schon aus ergonomischen Gründen durchaus Grenzen. Auch auf der technischen Ebene macht Word dem Anwender allerdings schnell deutlich, dass beispielsweise beim Import modularisierter oder abhängiger Schemata der Teufel im Detail steckt.

Bild 50: Verwendung benutzerdefinierter Schemata in Word 2003

Dokumenten mit benutzerspezifisch ausgezeichneten Daten können auf zweierlei Weise gespeichert werden: als WordProcessingML-Datei mit eingebetteten benutzerspezifischen Elementen, oder als rein benutzerspezifische XML-Datei. Im zweiten Fall werden nur die mit dem benutzerspezifischen Schema ausgezeichneten Daten gespeichert, das umkleidende Office-Dokument hingegen nicht. Auf Wunsch validiert Word 2003 die benutzerspezifisch ausgezeichneten Teile des Dokumentes vor dem Speichern.

Bild 51: Schema-Verwaltung von Word 2003: nicht immer selbsterklärend

Mit jedem Dokument kann ein XSL-Stylesheet als Exportfilter definiert und beim Speichern als XML-Datei auf die vollständige WordProcessingML-Repräsentation des Dokumentes angewendet werden. Diese Transformation steht auch dann zur Verfügung, wenn das Dokument nicht mit einem benutzerdefinierten Schema assoziiert wurde. Die Assoziation mit einem Export-Stylesheet kann auch in Dokumentvorlagen abgelegt werden.

Ebenso ist es möglich, beim Öffnen einer XML-Datei ein Stylesheet zu identifizieren, anhand dessen das Dokument transformiert werden soll. Eine Assoziation des Stylesheets mit der Datei findet in diesem Fall jedoch nicht statt.

Bild 52: Einbindung von Transformations-Stylesheets in Word 2003 beim Laden (oben) und Speichern (unten)

Mit Hilfe der Stylesheets, die mit StarOffice/OpenOffice.org geliefert werden, kann Word 2003 auf diesem Wege Dokumente erzeugen, die gegen das OASIS OpenDocument-Schema-validierbar sind, und diese auch wieder importieren[1].

Eine weitere Importfilter-Funktionalität ist in der Schemabibliothek verankert. Sie bietet die Möglichkeit, mit einem Schema eines oder mehrere Stylesheets als so genannte "Solutions" zu assoziieren; beim Laden einer XML-Datei, die das fragliche Schema referenziert, wählt der Anwender eine dieser Solutions aus. Prinzi-

[1] Diese Möglichkeit wurde anhand sehr einfacher Dokumente mit Hilfe der Stylesheets verifiziert, die mit OpenOffice.org 1.9.65 zur Verfügung gestellt wurden. Das unmittelbare Öffnen der erzeugten Dateien mit einen frisch installierten OpenOffice.org 1.9.65 gelingt jedoch nicht, da die OpenDocument-Dateien kurz gesagt in einem Format geschrieben werden, das normalerweise für den OpenOffice.org-internen Gebrauch bestimmt ist.

piell sollte dieser Mechanismus in der Lage sein, OpenDocument-Dateien automatisch zu importieren; diese Möglichkeit kann im Rahmen des Leitfadens jedoch nicht verifiziert werden[1].

Excel kennt im Gegensatz zu Word keine Schemabibliothek. Vielmehr werden Assoziationen von Schemata mit einem Dokument jeweils individuell hergestellt. Die Speicherung von SpreadsheetML-Dateien und reinen benutzerdefinierten XML-Dateien werden als zwei verschiedene Dateiformate behandelt. Stylesheet-gesteuerte Transformationen beim Laden oder Speichern von XML-Dateien sind nicht verfügbar. Eine Reihe von Schema-Konstrukten werden nicht unterstützt:

Bild 53: Nicht unterstützte Schema-Konstrukte in Excel

Während Textdokumente eine mehr oder wenige klare sequenzielle Struktur haben, sind „Vorn“ und „Hinten“ in Spreadsheets eine Frage der Interpretation. Dementsprechend bietet XML bei der benutzerdefinierten Auszeichnung von Daten Freiheiten, die über die von Word hinausgehen. Zugleich orientiert sich Excel an einem Datenbank- bzw. Datenblock-haften Blickwinkel. Dem entsprechend stellen sich die gleichen benutzerdefinierten Auszeichnungen in Excel anders dar als in Word (siehe Bild 54, S. 314).

[1] Word 2003 versteht keine Relax NG-Schemata, das OpenDocument-Schema ist jedoch in Relax NG formuliert. Eine automatische Konvertierung nach W3C Schema ist mit dem OpenDocument-Schema jedoch nicht möglich.

Bild 54: Verwendung benutzerdefinierter Schemata in Excel 2003

3.13.6.4 Weitere zu betrachtende neue Funktionalitäten

Smarttags

Die Einführung von so genannten Smarttags erfolgte bereits mit Office XP. In Office 2003 wurde die Funktionalität um einige Punkte erweitert.

Smarttags sind eine weitere Möglichkeit der Automatisierung durch kontextsensitive Unterstützung der Nutzer. Ein Smarttag löst auf Basis einer Eingabe (z.B. ein vorbestimmtes Wort oder eine bekannte Zahl) eine Funktion aus. So lassen sich mit Hilfe von Smarttags auch Funktionen in anderen Anwendungen nutzen, z.B. öffnen von weiteren Dokumenten[1]. Unterschieden wird zwischen einfachen Smarttags und COM-basierten Smarttags. Einfache Smarttags werden in XML-Listen verwaltet, die an einer zentralen Stelle im Rechner-Netzwerk abgelegt werden und dann allen Anwendern zur Verfügung stehen. COM-basierte Smarttags werden als so genannte Smarttag-Add-Ins eingesetzt. Der Nutzen der Smarttags ist allerdings umstritten, sicherlich können geeignete Smarttags dem Neueinsteiger die Arbeit erleichtern, indem sie ihn an geeigneter Stelle auf verfügbare Funktionalitäten und Formatierungshilfen hinweisen. Genauso gut kann dies einen Neueinsteiger aber auch völlig verwirren, wenn er mit den angebotenen Funktionalitäten nichts anfangen kann. Um dies zu vermeiden, ist es notwendig die Benutzer bei einer Umstellung auf Office 2003 in ausreichendem Maße auf diese neue Funktionalität zu schulen, sofern man diese Funktionalität nutzen möchte. Es besteht auch die Option diese Funktionalität über „Extras/Autokorrektur/Smartags“ zu deaktivieren.

[1] Siehe Beispiel Office 2003 und Domea

Mit Blick auf die Zukunft stellen Smarttags eine weitere anwendungsspezifische Automation dar, die nur im Zusammenhang mit MS Office verwendet werden kann. Der verstärkte Einsatz führt letztendlich zu einem noch höheren Umstellungsaufwand bei einer Ablösung von MS Office bzw. kann dazu beitragen, dass eine Ablösung aus wirtschaftlichen Gründen abzulehnen ist.

Unterstützung der Zusammenarbeit und Bereitstellung von Dokumenten

Kern dieser Unterstützungsfunktionalitäten sind die so genannten „Windows SharePoint Services“[1] (WSS). Im Wesentlichen handelt es sich hierbei, wie bereits erwähnt, um erweiterte Groupware-Funktionalitäten, die in der einen oder anderen Weise schon mit Groupware-Lösungen und anderen Anwendungen, wie z.B. Dokumenten-Management-Systemen oder Content-Management-Systemen weitgehend abgedeckt werden.

Microsoft selbst hebt dabei drei funktionale Möglichkeiten hervor[2], die diese nochmals verdeutlichen sollen:

- „*Gemeinsame Bearbeitung von Dokumenten. Steuern Sie den Zugriff auf Ihre Dokumente, verfolgen Sie Versionen und Aktualisierungen und sammeln Sie Rückmeldungen anderer Teammitglieder*“.
- „*Verwalten von Teams und Projekten. Koordinieren Sie die Aktivitäten Ihrer Teammitglieder, und verwalten Sie Statusberichte, aktuelle Daten, Aufgaben, Teamkalender und mehr*“.
- „*Effektivere Durchführung von Besprechungen. Planen und verwalten Sie Teambesprechungen mit den Teammitgliedern vor Ort und an anderen Standorten*“.

Viele der von Microsoft hervorgehobenen Neuerungen von Office 2003 lassen sich u.a. nur mit den WSS in vollem Umfang nutzen. Die WSS sind allerdings nicht Bestandteil von Office 2003 sondern Teil von Windows Server 2003 und werden derzeit als separates Add-On kostenlos zur Verfügung gestellt.

Information Rights Management (IRM) und Rights Management Services (RMS)

Weitere Features, die auch im Zusammenhang mit WSS genannt werden, sind die von Microsoft als „sicherheitsrelevante Methoden, der Zusammenarbeit“[3] benannten Funktionen. Diese sind Möglichkeiten, für die Zusammenarbeit, Kommunikation und Informationensbereitstellung feingliedrige personen- und gruppenbezogene Sicherheitsrichtlinien festzulegen. Voraussetzungen, um diese nutzen zu können, sind:

---

1 Ehemals „SharePoint Team Services“

2 http://www.microsoft.com/germany/office/ueberblick/zusammenarbeit/wss/default.mspx

3 “Microsoft® Office Resource Kit, Technischer Artikel (Whitepaper), Probleme bei der Migration von Microsoft Office 97 zu Microsoft Office 2003” (Office_97-03_Delta.doc Abschnitt „Basisanforderungen“).

- Betriebssysteme wie Windows® 2000, Windows XP oder Windows Server 2003,
- die Verfügbarkeit der Windows-Authentifizierung und –Rechteverwaltung für Windows Server 2003 (RMS),
- die Nutzung von Active Directory,
- die Bereitstellung von Passport-fähige Benutzerkonten, insbesondere die Verwaltung von Informationsrechten (IRM) sowie
- beim Einsatz im Netzwerk "das Erstellen von Servern [...], die ausschließlich der Verwaltung der erstellten SharePoint-Websites dienen“.

Diese so genannten Basis-Anforderungen zeigen, dass die Nutzung dieser neuen Funktionalitäten nur in einer abgeschlossenen Windows-basierten Infrastruktur in vollem Umfang nutzbar sind, da die Office-Komponenten dazu sehr eng mit dem Authentifizierungs- und Zugriffsberechtigungsmanagement verwoben werden.

Basis der gesamten Architektur sind die Rights Management Services (RMS)[1], nicht zu verwechseln mit DRM, dem Windows Media Digital Rights Management, das zur Beschränkung des Zugriffs auf Medieninhalte dient. RMS ist vielmehr ein weiteres Add-On für Windows Server 2003 und ergänzt dessen Sicherheitsarchitektur um eine weitere Schicht. RMS in Kombination mit AD ermöglicht es, Dateien personen- oder gruppenbezogen mit zusätzlichen Zugriffseinschränkungen wie etwa "Read only" oder "Do not forward" zu belegen. Damit soll u.a. sichergestellt werden, dass sensible Daten auch außerhalb eines abgeschlossenen Systems (außerhalb von Firewalls) nicht in unberechtigte Hände fallen. Die Berechtigungsüberprüfung erfolgt anhand von Zertifikaten, die durch den RMS-Server zunächst bereitgestellt und später überprüft werden. Damit eine Anwendung die zusätzlichen Zugriffsbeschränkungen überhaupt berücksichtigen und auswerten kann, benötigt sie als Schnittstelle zum RMS-Server einen entsprechenden RMS-Cient. Für Office 2003 heißt diese Client-Implementierung IRM (Information Rights Management).

Mit IRM kann für jede Datei festgelegt werden, dass einzelne Benutzer oder Benutzergruppen vollständigen Zugriff haben, andere Benutzer dagegen die Datei nur ausdrucken oder nur lesen dürfen. Im weitesten Sinne ist dies in etwa vergleichbar mit den Sicherheitseinstellungen, die für einzelne PDF-Dokumente mit Adobe Acrobat festgelegt werden können, die dann vom Reader ausgewertet werden. Bei den PDF-Dokumenten gelten diese Regeln aber immer für alle Benutzer, unabhängig davon wo und in welcher Systemumgebung diese das Dokument verwenden. Ein weiterer Unterschied liegt darin, dass Office 2003 Dokumente durch IRM verschlüsselt werden. Damit die zusätzlichen Zugriffregeln für Office 2003 Dokumente auch personenbezogen überprüft werden können, ist es

[1] Microsoft Office 2003 - Informationen schützen mit den Diensten für die Windows-Rechteverwaltung und der Verwaltung von Informationsrechten (rmsirm.doc)

notwendig, dass eine entsprechende Windows-Umgebung mit RMS-Server zur Verfügung steht. Was passiert aber, wenn ein mit Einschränkungen versehenes Dokument geöffnet werden soll und keine Verbindung zu einem RMS-Server besteht? Laut Microsoft gilt folgendes[1]:

> *„Für Autoren von Dokumenten, Arbeitsmappen und Präsentationen mit Zugriffseinschränkung ist es stets erforderlich, dass Sie eine Internetverbindung herstellen, um Ihre Anmeldeinformationen zu bestätigen und zu überprüfen, ob Ihnen die Berechtigung zum Lesen des Inhalts erteilt wurde. Wenn Sie Ihre Anmeldeinformationen für ein Dokument, eine Arbeitsmappe oder eine Präsentation erstmalig bestätigt haben, können Sie das Dokument, die Arbeitsmappe oder Präsentation später, auch wenn Sie offline arbeiten, möglicherweise ohne Internetverbindung öffnen. Es kann jedoch vorkommen, dass Autoren für jedes Öffnen eines Dokuments, einer Arbeitsmappe oder Präsentation mit Zugriffseinschränkung anfordern, dass Sie Ihre Berechtigung über eine Internetverbindung bestätigen.“*

Bild 55: Ausschnitt der Web-Site von Microsoft zur Unterstützung im Umgang mit IRM-geschützten Dokumenten

Diese Bedingungen gelten nicht nur für Autoren, sondern für jegliche Nutzer, die auf eine solche Datei zugreifen wollen. Will man ein RMS-geschütztes Dokument

[1] http://office.microsoft.com/de-de/assistance/HP010378611031.aspx

jemanden außerhalb der eigenen Organisation zum Lesen oder für eine gemeinsame Bearbeitung zur Verfügung stellen, dann muss diese Person dem RMS bekannt sein. Dies kann über das Organisationsnetzwerk hinaus über das Internet mittels so genannter Passport-fähiger Benutzerkonten ermöglicht werden.

Die durch RMS geschützten Dateien können nur noch mit RMS-fähigen Anwendungen und einer Verbindung zum RMS-Server genutzt werden. Von solchen Anwendungen gibt es heute noch nicht sehr viele, so dass diese Feature nur in reinen Windows- und Office 2003-Umgebungen zum Einsatz kommen kann. Noch ist nicht absehbar, inwieweit andere Software-Hersteller RMS unterstützen werden. Mit der aktuellen und folgenden Version von OOo/SO können RMS-geschützte Dateien nicht geöffnet werden.

Was eine große Zahl von solchermaßen behandelten Dateien für eine spätere Migration bedeutet, ist leicht vorstellbar. Insbesondere eine ablösende Migration, nach der alte Dokumente weiter verwendet werden sollen, ist nur mit sehr viel Aufwand zu betreiben, da bei allen weiter zu verwendenden Dateien die ursprünglichen Einschränkungen wieder aufgehoben werden müssten. Dateien auf die lesender Zugriff möglich sein soll, müssten zumindest in ein anderes lesefähiges Format (z.B. PDF) umgewandelt werden. Die damit verbundenen Aufwendungen verhindern vermutlich jede ablösende Migration schon aus wirtschaftlichen Gründen.

Die hier vorgestellte Technologie von Microsoft ist in dieser Form derzeit sicherlich ein Alleinstellungsmerkmal. Aus Sicht der Autoren des Migrationsleitfadens gibt es aber alternative Konzepte, die mit Hilfe plattformunabhängiger Lösungen und losgelöst von bestimmten Anwendungen zur Erstellung und Bearbeitung von Dokumenten die gleichen Sicherheitsanforderungen, also der Verschlüsselung von Dokumenten, dem gesicherten Austausch und der Bereitstellung mit definierten Zugriffsrechten, erfüllen können und gleichzeitig der Behörde die freie Wahl des Office-Anwendung erhalten.

Abschließend muss noch deutlich hervorgehoben werden, dass IRM nur im Zusammenhang mit den bisherigen binären Formaten von Microsoft Office (.doc, .xls usw.) genutzt werden kann. Mit Nutzungseinschränkungen belegte Dateien können logischerweise nur noch von Benutzern in ein XML-Dateiformat konvertiert werden, welche die vollen Rechte an dem so geschützten Dokument haben. Bei der Konvertierung gehen die festgelegten Nutzungseinschränkungen verloren.

Zusammenfassend ist festzuhalten, dass Microsoft mit IRM und RMS eine Technologie bereitstellt, die sicherlich ihre sinnvollen Einsatzszenarien findet. Jeder Nutzer sollte sich jedoch vor der Einführung dieser Technologie die damit verbundenen Konsequenzen hinsichtlich Interoperabilität und vor allem hinsichtlich der Option auf eine spätere Ablösung von MS Office und den damit verbundenen Aufwendungen bewusst machen. Interoperabilität ist nur mit Anwendungen gegeben, welche ebenfalls diese Technologie integriert haben, also über eine RMS-Client-Implementierung verfügen und Zugriff auf die Authentifizierungs- und Auto-

risierungsinfrastruktur besitzen. Bei einer möglichen späteren Ablösung von MS Office müssen bei allen Dokumenten, die weiter genutzt werden sollen, die erweiterten Sicherheitseinstellungen zurückgenommen werden.

3.13.7 Bewertung der Office-Migrationspfade

Auf Basis der zuvor durchgeführten Betrachtungen werden nachfolgend zunächst die Ablösung von Office 97 bzw. Office 2000 durch Office 2003 oder durch OOo/SO bewertet. Diese Bewertungsergebnisse bilden die Grundlage für eine Bewertung der Möglichkeiten zur Ablösung des Microsoft-Desktop durch einen Linux-Desktop.

3.13.7.1 Dateiformat-unabhängige Interoperabilitätsaspekte

Aus dem vorangegangenen Kapitel wird deutlich, dass eine 100%ige Kompatibilität mit MS Office nicht besteht. Da die Inkompatibilitäten auf der Ebene des Dokumentenmodells angesiedelt sind, können sie auch durch den Datenaustausch auf der Basis von XML-Dateien nicht behoben werden sondern sind unabhängig vom verwendeten Dateiformat. Was bedeutet dies hinsichtlich des Austausches von Dokumenten zwischen Benutzern von OOo/SO und Benutzern von MS Office? Die Beantwortung dieser Frage muss auf zwei Betrachtungsebenen vorgenommen werden.

1. Der Zweck des Dokumentenaustausches ist zu berücksichtigen.
2. Die Komplexität der Dokumente, die ausgetauscht werden sollen, ist ebenfalls zu berücksichtigen.

Der Dokumentenaustausch erfolgt zu reinen Informationszwecken

In diesem Fall spielt die Komplexität der auszutauschenden Dokumente keine Rolle. Die auszutauschenden Dokumente sollten in das PDF-Format konvertiert werden. Ein PDF-Reader steht jedem Benutzer zur Verfügung bzw. kann kostenfrei aus dem Internet bezogen werden. Das PDF-Format wird den Bundesbehörden schon seit längerem als Austauschformat empfohlen.

Der Dokumentenaustausch erfolgt zum Zweck der gemeinsamen Bearbeitung

In diesem Fall spielt die Komplexität der Dokumente, wie aus den vorgehenden Betrachtungen deutlich geworden ist, ein sehr wichtige Rolle.

1. Handelt es sich um einfache Dokumente, dann kann eine gemeinsame Bearbeitung ohne größere Probleme erfolgen. Die Überarbeitungsfunktionen in OOo/SO und MS Office sind interoperabel.
2. Handelt es sich jedoch um komplexe Dokumente, dann müssen bei der gemeinsamen Bearbeitung deutliche Einschränkungen in Kauf genommen werden.
    - Hinsichtlich Textverarbeitung und Tabellenkalkulation kann die gemeinsame Bearbeitung weiterhin nur auf der rein inhaltlichen Ebene

empfohlen werden. Die Verantwortung für die Formatierung sollte eindeutig auf einer Seite definiert sein und erst nach Fertigstellung des Inhaltes durchgeführt werden. Beide Seiten müssen sich über das Vorgehen einig sein.

- In Tabellenkalkulationen können, aufgrund der Unterschiede in den Chart-Engines, die Charts ebenfalls erst nach Fertigstellung der Dateninhalte erzeugt werden. Sollen die Charts mit Calc erzeugt werden, dann müssen die Einschränkungen hinsichtlich der Labelerstellung beachtet werden (s.o.).
- Eine gemeinsame Bearbeitung von Pivot-Tabellen ist nicht möglich, da diese durch Calc nicht unterstützt werden.
- Eine gemeinsame Bearbeitung von komplexen Präsentationen kann nicht empfohlen werden.

Soll eine gemeinsame Bearbeitung von Dokumenten mit OOo/SO und MS Office stattfinden, dann sollten folgenden Regeln beachtet werden:

- Einigung auf ein Dokumenten-Format. Bei einer Wahl zwischen OOo und SO ist es zwingend notwendig, sich auf die MS Office-Formate festzulegen, da in MS-Office keine OOo/SO-Filter verfügbar sind. Wenn es ein Format gibt, das beide können, wie z.B. RTF, dann sollte dieses verwendet werden.
- Vermeidung von der so genannte „Round Trip“-Konvertierung.
- Formatierung erst in der letzten Stufe/Instanz, da das Mapping zwischen OOo/SO und MS Office nicht eins zu eins funktioniert.
- Keine Bearbeitung von Dokumenten im Mixed-Mode, die
  - von vielen gemeinsam genutzt werden und
  - evtl. noch mit Automatismen behaftet sind.
- Enddokumente in PDF-Format überführen.

3.13.7.2 Interoperabilität auf der Basis von XML-Dateien

Die im vorausgegangenen Abschnitt beschriebenen Inkompatibilitäten auf der Ebene der Dokumentenmodelle schränken die Interoperabilität zwischen OOo/SO und Microsoft Office ein, und wie in Kapitel 3.13.3.2 dargelegt, kann auch XML daran im Prinzip nichts ändern. Allerdings bietet der Einsatz offener Standards generell mehr Freiheit bei Wahl und Einsatz der Werkzeuge, und so lassen sich auf der Basis von XML-Dateiformaten manche Schwierigkeiten vielleicht wirksamer eindämmen als vorher. Insofern lohnt sich durchaus eine zusammenfassende Betrachtung der XML-Unterstützung in den aktuellen Office-Suiten speziell unter Interoperabilitätsgesichtspunkten, aber auch im Hinblick auf Hintergrund und Entwicklungsperspektiven der XML-Strategien hinter den Produkten.

Mit der Fokussierung auf XML geht vernünftigerweise das konkrete Ziel einher, Dateiformate zu normieren. Interoperabilität zwischen jeweils zwei Anwendungen in einer bestimmten Version auf Dateiformat-Ebene ist auch auf der Basis von Import- und Exportfiltern für Binärformate herstellbar. Ein XML-Dateiformat entfaltet seine Vorzüge erst dann völlig, wenn es als zentrales Format für *alle* in Frage kommenden Anwendungen und Anwendungsversionen eingesetzt wird. Beispielsweise sollte es nicht nur zwischen zwei Textverarbeitungen ausgetauscht, sondern auch von Dokumentenmanagement- und Geschäftsprozess-Systemen gelesen und verstanden werden können. Idealerweise sollte das normierte Dateiformat die Konstante sein, und die eingesetzten Anwendungen die Variablen.

Ausgehend von den in den vorausgegangenen Kapiteln vorgestellten Anwendungen ist daher in erster Linie die Eignung von OpenDocument bzw. der Microsoft-Schemata für normierte Dateiformate abzuwägen. Diese Abwägung steht im Mittelpunkt dieses Kapitels.

Die Normierung von Dateiformaten ist durchaus ein Selbstzweck, steht allerdings in einer Wechselbeziehung mit Produktentscheidungen. Zwar ist die Normierung ursprünglich dadurch motiviert, dass Interoperabilität zwischen verschiedenen Produkten hergestellt werden soll. Die Produkte müssen sich jedoch auch hinlänglich schlüssig und wirtschaftlich vertretbar in solche interoperablen Umgebungen integrieren lassen. Bieten sie diese Möglichkeit nicht – und irgendeine wie auch immer geartete XML-Unterstützung reicht dafür nicht – müssen sie abgelöst werden. Damit reduziert sich wiederum die Zahl der Produkte, zwischen denen Interoperabilität hergestellt werden muss. Dieses Kapitel geht daher auch der Frage nach, wie viel Interoperationsfreude sich in der XML-Unterstützung der Office-Suiten tatsächlich ausdrückt und wie sie noch zu steigern wäre.

XML-Unterstützung in OOo/SO und MS Office

Unabhängig von Interoperabilitätsfragen zeigen sich im Vergleich der XML-Unterstützung in OpenOffice.org 2 bzw. StarOffice 8 und Microsoft Office 2003 zahlreiche deutliche Unterschiede. Allerdings haben beide Suiten eine unterschiedliche Historie und Architektur. Microsoft Office ist eine Familie selbständiger Produkte, die sich unabhängig voneinander entwickelt und einen auch für den Anwender deutlich wahrnehmbaren eigenen Charakter haben. OOo/SO dagegen versteht sich seit vielen Jahren als eine einzige integrierte Lösung aus einem Guss.

Diese Unterschiede haben fast unausweichliche Konsequenzen für viele Aspekte der XML-Unterstützung. Die Verwendung eines einzigen, einheitlichen Dateiformats ist angesichts des monolithischen Zuschnitts von OOo/SO nahe liegend, drängt sich angesichts des weitaus lockereren Verbundes der Microsoft-Office-Anwendungen hingegen nicht unbedingt auf. Für OOo/SO käme eine uneinheitliche XML-Unterstützung in den Teilanwendungen einer Belästigung der Anwender gleich. Für Microsoft Office mag es dagegen durchaus schlüssig sein, anwendungsspezifisch zu entscheiden, ob, wie viel und welche XML-Unterstützung jeweils angezeigt ist.

OOo/SO speichert prinzipiell alles immer in XML-Dateien und kann ohne Zweifel für sich in Anspruch nehmen, die um Längen vollständigere, schlüssigere und konsequentere XML-Unterstützung zu bieten, zumindest was die Grundfunktionen der verschiedenen Teilanwendungen einer Office-Suite angeht. Microsoft Office dagegen bietet XML-Dateiformate nur für zwei der hier betrachteten Anwendungen an, und obendrein nur als Zweitformat. In doppelter Hinsicht: es ist nicht notwendigerweise vollständig, und (wohl auch deswegen) ab Werk nicht als Standard-Format voreingestellt.

Einen nicht zu unterschätzenden Einfluss dürfte auch haben, dass die Rolle von OOo/SO im Markt die des Herausforderers ist. Interoperabilität, besonders mit dem Markführer Microsoft Office, ist in dieser Position von überragender Bedeutung, und OOo/SO bringt dafür durchaus schmerzhafte Opfer[1]. In dieser Tradition steht die aus Anwendersicht praktisch nahtlose Integration der XSLT-Import- und Export-Filter in OOo/SO, neben der sich das auf Word beschränkte Microsoft-Pendant eher karg ausnimmt.

Allerdings haben Excel und vor allem Word mit der Integration benutzerdefinierter Schemata einen klaren Vorsprung darin, die Erweiterbarkeit beim Wort zu nehmen, die XML im Namen trägt. Dieses Leistungsmerkmal fordert einige Bedenken heraus. Einige dieser Bedenken sind technischer Art: die in dieser Weise erzeugten Dateien sind nicht mehr mit heutigen XML-Standardmitteln validierbar. Andere Bedenken sind rechtlicher Art: Programme, die diese nunmehr nichtkonformen Dateien lesen, stehen möglicherweise nicht mehr auf dem Boden der Patent-Lizenz. Und schließlich muss sich erweisen, welchen Anklang dieses Feature auf den Desktops der Anwender findet. Auf jeden Fall ist es ein wichtiges Signal, da dies über die bloße XMLisierung altbekannter Funktionalitäten hinaus geht und neue Möglichkeiten aufzeigt.

Nebeneinander betrachtet lassen die Suiten ahnen, welches Entwicklungs- und Innovationspotential die XML-Unterstützung in beiden Paketen noch bietet. Dies gilt (leider) in besonderem Maße für die Interoperabilität der Suiten untereinander und die Möglichkeit, Dateiformate zu normieren. Die folgenden drei Abschnitte fokussieren dieses Problem.

Technische Aspekte

Aufgrund der anwendungsspezifisch sehr unterschiedlichen XML-Unterstützung in Office 2003 müssen die Anwendungen auch im Hinblick auf normierte Dateiformate differenziert betrachtet werden.

Mit Blick auf die Textverarbeitung sind StarOffice/OpenOffice.org und Word technisch sehr weitgehend und unmittelbar interoperabel. Beide Anwendungen unterstützen XSL-Stylesheets für die Import-/Export-Funktionalität, und soweit sich

[1] "One (already resolved) example of this is the upper paragraph margin that exists in Microsoft Word and SO/OOo Writer. The latter, like many DTP and professional word processing applications, ignores this value for the first paragraph of a page. Microsoft Word does not. The result of this is that the documents look different, although exactly the same values are stored in both text engines." (http://development.openoffice.org/releases/q-concept.html)

dies anhand der aktuellen Entwicklerversion von OpenOffice.org ablesen lässt, können die dort bereitgestellten Stylesheets auch in Word eingesetzt werden. Damit steht ein Universalkonverter für die beiden beteiligten Formate zur Verfügung, und demonstriert die Vorzüge von XML-Standards.

Prinzipiell kann OOo/SO Writer WordProcessingML-Dateien schreiben und lesen, und Word kann Writer-Dateien schreiben und lesen, dank XSLT – und dank des Aufwandes, den OOo und Sun in die Entwicklung der Stylesheets investiert haben. Daher bieten sich auf den ersten Blick beide Dateiformate für eine Normierung an.

Abzuwarten bleibt allerdings, wie gut die von StarOffice/OpenOffice.org angebotenen Filter in ihrer endgültigen Version tatsächlich funktionieren, und ob sie womöglich sogar Roundtripping erlauben. Eine Rolle spielt dabei nicht nur die Qualität und Symmetrie der Stylesheets als solche, sondern nach wie vor auch die Kompatibilität und Abbildbarkeit der Dokumentenmodelle.

Damit verbunden ist die oben angesprochene Frage, ob die Produkte sich überhaupt in Interoperations-Szenarien auf der Basis von XML-Dateiformaten einfügen lassen. Sollen beispielsweise Textverarbeitungs-Dokumente mit eingebetteten Spreadsheets in reinen XML-Dateien abgelegt werden, kann Word prinzipiell nicht eingesetzt werden und WordProcessingML bietet sich nicht länger als normiertes Dateiformat an. Sollen Auszeichnungen mit benutzerdefinierten Schemata in ein Textdokument eingebettet werden, scheidet nicht nur das OpenDocument-Format aus, sondern auch StarOffice / OpenOffice.org als Produkt.

Mit Blick auf den erwähnten Universalfilter sind auch ergonomische Aspekte zu berücksichtigen. Während die Verwendung der Stylesheets in StarOffice/OpenOffice.org tief in die Funktionalität zum Laden und Speichern von Dateien integriert ist, hat sie bei Word – wie oben gezeigt – einen eher peripheren Charakter. Dadurch bietet sich zwar im Einzelfall mehr Flexibilität. Zugleich ist aber auch die Zahl der Handgriffe größer, die immer wieder für jedes Dokument vorgenommen werden müssen. So ist es für den Anwender wesentlich angenehmer, mit Writer WordProcessingML-Dateien zu bearbeiten, als umgekehrt mit Word auf OpenDocument-Dateien zuzugreifen. Allerdings ist dies kein Indiz für einen technischen Vorzug von WordProcessingML.

Schließlich ist das Universalfilter-Szenario technisch noch nicht ganz perfekt. Die Stylesheets transformieren nicht von bzw. in das normalerweise von StarOffice/OpenOffice.org tatsächlich verwendete OpenDocument-ZIP-Format, sondern in ein unkomprimiertes, flaches XML-Format. Es ist ebenfalls in der OpenDocument-Spezifikation definiert und kann auch von StarOffice/OpenOffice.org zum Speichern von Dokumenten verwendet werden, eine entsprechende Konfiguration vorausgesetzt. Daher eignet sich dieses flache XML-Format prinzipiell als normiertes Dateiformat. Allerdings werden Dateien in diesem Format sehr schnell sehr groß, etwa durch Text-kodierte eingebettete Grafiken. Das Gleiche gilt für die Verwendung von WordprocessingML als normiertem Dateiformat.

Unter diesem Gesichtspunkt ist es wünschenswert, das übliche, komprimierte OpenDocument-ZIP-Format zu normieren. Dazu reicht es nicht aus, die von Sun bereitgestellten XSL-Stylesheets in Word zu verwenden. Vielmehr muss sowohl für das Lesen wie für das Schreiben ein zweiter Konvertierungsschritt hinzukommen, der nicht allein mit XSL-Mitteln formuliert werden kann. Dadurch wird der Einsatz einer entsprechenden selbständigen Komponente benötigt. Diese Komponente muss sich nicht darauf beschränken, nur vom gezippten ins flache OpenDocument-Format zu konvertieren, sondern könnte sinnvollerweise gleich die gesamte Konvertierung nach WordProcessingML (und natürlich zurück) vollziehen.

Eingesetzt werden kann eine solche Komponente auf verschiedene Weise. Die technisch einfachste Lösung ist, sie dem Word-Benutzer zur Verfügung zu stellen, so dass er sie selbst nach Bedarf verwenden kann. Ebenfalls denkbar ist, diese Komponente von Skripten aus anzusprechen, die anstelle der normalen Funktionalitäten zum Lesen und Schreiben von Dateien verwendet werden. Verfügt eine Umgebung über ein wie auch immer geartetes zentrales Dokumenten-Repository, dann kann eine solche Komponente möglicherweise auch darin integriert werden. So könnte beispielsweise der (autoritative) OpenDocument-Datenbestand automatisch in einen (nicht-autoritativen) WordProcessingML-Datenbestand gespiegelt werden.

Um die Interoperabilität der Tabellenkalkulationen steht es im direkten Vergleich von vornherein deutlich schlechter. Zwar bietet StarOffice/OpenOffice.org auch für SpreadsheetML Tranformations-Stylesheets[1] an. Anders als Word bietet Excel jedoch keine Möglichkeit, diese Stylesheets beim Laden und Speichern zu verwenden. Um die Tabellenkalkulationen auf der Basis von OpenDocument interoperabel zu machen, ist also in jedem Fall ein Konvertierungsschritt außerhalb von Excel notwendig. Allerdings ist auch die SpreadsheetML-Unterstützung durch Excel selbst für viele typische Einsatzfälle so unzureichend, dass Interoperabilität auf der Basis von XML-Dateien grundsätzlich nur in merklich beschränktem Umfang möglich ist.

Mit Blick auf die Präsentations-Anwendungen kann eine Normierung nur auf der Basis von OpenDocument erfolgen, da Microsoft kein entsprechendes XML-Format anbietet.

Zugunsten des OpenDocument-Formates wird häufig ins Feld geführt, dass es alle Office-Funktionalitäten in einem Format vereint. Die damit verbundenen Vorteile wie Redundanzfreiheit sind allerdings auch mit mehreren, voneinander unabhängigen Schemata erreichbar. Ob der respektable Umfang des OpenDocument-Schemas seine weitere Verbreitung eher behindert als befördert, bleibt abzuwarten.

[1] Im Gegensatz zu den WordProcessingML-Stylesheets wurde die Funktionsfähigkeit der SpreadsheetML-Stylesheets im Rahmen des Leitfadens nicht verifiziert.

Aus technischer Sicht stellt sich die Situation insgesamt ermutigend dar, aber keineswegs befriedigend. Auf der Ebene der XML-Dateiformate deckt OpenDocument die gesamte Palette der Office-Anwendungen ab, enthält aber durch die Verwendung des Mehrdateien-ZIP-Archivs ein Konvertierungshindernis, das mit üblichen XML-Mitteln nicht überwunden werden kann. Auch fehlt ihm eine Entsprechung zur Einbettung von benutzerdefinierten Schemata. Die Office 2003-Schemata decken nur Teile der Office-Anwendungen ab und sind mit ihren proprietären Binäreinschlüssen im Gebrauch von XML nicht wirklich konsequent.

Mit Blick auf die Produkte wird deutlich, dass StarOffice/OpenOffice.org bereits eine langjährige Tradition beim Einsatz von XML-Dateiformaten hat und sich aufgrund seiner Marktposition als Herausforderer naturgemäß intensiv um Interoperabilität mit dem Marktführer bemüht. Darüber hinaus gehende Funktionalitäten im Dienste der Backend-Integration finden dagegen gerade erst ihren Weg in das Produkt, immerhin auf der Basis offener Standards. Dieses strategisch wichtige Thema besetzt Microsoft zwar mit einem eigenen Produkt, zeigt ansonsten aber eine noch lückenhafte und bis in die Oberflächen hinein uneinheitliche XML-Unterstützung.

Dass nun auch Microsoft Office wenigstens in Teilen XML-Dateiformate verwendet, hat die Perspektiven für Interoperabilität auf der Dateibasis ebenso verbessert wie die Standardisierungsbemühungen um OpenDocument. Dennoch lassen sowohl die Produkte als auch die Dateiformate offensichtlich noch einige Wünsche offen, so es in beiden Kategorien noch keine optimale Lösung gibt.

Ausgehend von der Prämisse eines möglichst konsequenten Einsatzes von XML ist allerdings OpenDocument heute für den Einsatz als normiertes Dateiformat besser geeignet als die Office 2003-Schemata.

Strategische Aspekte

Neben den angesprochenen technischen Aspekten spielen für die Eignung eines normierten Dateiformates auch rechtliche und strategische Fragen eine Rolle, deren Betrachtung empfiehlt sich in einem etwas erweiterten Blickwinkel. Interoperabilität muss nicht nur innerhalb einer Organisation hergestellt werden, sondern wird in aller Regel auch mit Dritten angestrebt. Wenn eine Organisation aber ein gemeinsames Interesse an Interoperabilität mit ihren Partnern und Kunden teilt, dann liegt es nahe, die Verantwortung für die Ausgestaltung der Interoperabilität bei übergreifenden Institutionen anzusiedeln, sich an deren Richtlinien zu orientieren, soweit sie bereits existieren, und dort deren Entwicklung voran zu treiben.

Für den Bereich der öffentlichen Verwaltung liefern in diesem Sinne die Publikationen der KBSt wichtige Hinweise, insbesondere das E-Government-Handbuch einschließlich SAGA. Durch seinen klaren Fokus auf Interoperabilität auf der Ebene des Dokumentenaustausches empfiehlt sich im Rahmen dieses Kapitels ergänzend das European Interoperability Framework for pan-European eGovernment Services (EIF) des IDABC-Programms (Interoperable Delivery of Euro-

pean eGovernment Services to public Administrations, Business and Citizens, vormals IDA, Interchange of Data between Administrations) der EU-Kommission[1]. Es adressiert die innereuropäische, grenzüberschreitende Interoperabilität unter Beteiligung der Öffentlichen Verwaltung und erhebt insofern ausdrücklich keinen Anspruch auf Geltung innerhalb der einzelnen EU-Länder. Allerdings hat IDA die Diskussion recht weit vorangetrieben. Darüber hinaus steht IDABC im Dialog mit den Herstellern, bei denen es durchaus eine gewisse Aufmerksamkeit genießt. Insofern bieten die Aktivitäten des IDABC-Programms und besonders EIF im Großen eine Orientierung über Interoperablitäts-Strategien, die sich aufgrund der dort wirksamen Kräfte fast zwangsläufig auch im Kleinen niederschlagen werden.

Mit dem Ziel der Interoperabilität verlangt das EIF den Einsatz offener Standards. Zugleich definiert es folgende Mindest-Anforderungen an offene Standards:

- Der Standard wird von einer Non-Profit-Organisation entwickelt und gepflegt, und seine Weiterentwicklung wird im Rahmen eines offenen Entscheidungsprozesses betrieben, der allen interessierten Parteien offen steht und Konsens- oder Mehrheitsentscheidungen trifft[2].
- Der Standard ist veröffentlicht und seine Spezifikation ist unentgeltlich oder gegen eine Schutzgebühr verfügbar. Vervielfältigung, Weiterverbreitung und Verwendung der Spezifikation muss unentgeltlich oder gegen eine Schutzgebühr gestattet sein[3].
- Geistiges Eigentum am Standard oder seinen Teilen, wie möglicherweise bestehende Patente, müssen unwiderruflich unentgeltlich verfügbar sein[4].
- Die weitere Verwendung des Standards ist unbeschränkt[5].

Das OpenDocument-Format genügt diesen Anforderungen.

Die Office 2003-Schemata sind öffentlich[6], ihre Spezifikation darf unentgeltlich weiterverbreitet werden. Für die Implementation von Software steht eine separate

---

1 http://europa.eu.int/idabc/servlets/Doc?id=19224

2 "The standard is adopted and will be maintained by a not-for-profit organisation, and its ongoing development occurs on the basis of an open decision-making procedure available to all interested parties (consensus or majority decision etc.)."

3 "The standard has been published and the standard specification document is available either freely or at a nominal charge. It must be permissible to all to copy, distribute and use it for no fee or at a nominal fee."

4 "The intellectual property i.e. patents possibly present of (parts of) the standard is made irrevocably available on a royalty-free basis."

5 "There are no constraints on the re-use of the standard." Ein Download-Link wird unter http://www.microsoft.com/office/xml angeboten. Bislang sind die Schemata allerdings in eine selbstextrahierende .exe-Datei verpackt, so dass sie nur in Windows-Umgebungen entpackt werden können.

6 Ein Download-Link wird unter http://www.microsoft.com/office/xml angeboten. Bislang sind die Schemata allerdings in eine selbstextrahierende .exe-Datei verpackt, so dass sie nur in Windows-Umgebungen entpackt werden können.

so genannte Patent License[1] zur Verfügung, die praktisch unwiderruflich genau und allein das Lesen und Schreiben von Dateien erlaubt, die den Office 2003-Schemata entsprechen. Das Recht, die Formate zu modifizieren oder andere Formate von ihnen abzuleiten, wird jedoch ausdrücklich verweigert. Microsoft lehnt die Weiterentwicklung der Formate in einem offenen Prozess ab, und trifft bisher nur unscharfe Aussagen über die Bedingungen, unter denen künftige Versionen der Schemata verfügbar sein werden. Insofern sind die Office 2003-Schemata kein Offener Standard im Sinne des EIF.

Die Motivation von Microsoft, sich in dieser Frage substanziell zu bewegen, hängt naturgemäß vom Druck des Marktes ab. Interessant sind in diesem Zusammenhang die recht detaillierten Empfehlungen sowohl an Microsoft wie auch an das OASIS-TC, die das IDA-TAC (Telematics between Administrations Committee) im Mai 2004 ausgesprochen hat. Mit Blick auf die rechtlichen, aber auch auf die technischen Aspekte offener Dateiformate empfahl das TAC unter anderem:

- Das OASIS-TC sollte sich Gedanken über die Notwendigkeit und Gelegenheit machen, das Offene Dateiformat um die Integration benutzerdefinierter Schemata zu erweitern.
- Unternehmen, die bisher nicht Mitglied des OASIS-TC sind, sollten ihm beitreten.
- Die Standardisierung des Offenen Dateiformates sollte einem offiziellen Gremium wie der ISO übertragen werden.
- Microsoft sollte eine öffentliche Zusage über die Verfügbarkeit künftiger Schemata machen und erwägen, die Formate bei einem internationalen Standardisierungsgremium einzureichen.
- Microsoft solle die Entfernung von nicht in XML ausgedrückten Elementen aus den Office-Dateien erwägen.

Inzwischen liegen sowohl von Microsoft als auch von Sun Microsystems[2] Stellungnahmen vor. Auf wahrscheinliche und weniger wahrscheinliche Entwicklungen liefert insbesondere die Stellungnahme von Microsoft[3] interessante Hinweise. Festgehalten werden kann, dass auf EU-Ebene ein merklicher Druck auf die Anbieter ausgeübt wird, neben den technischen auch die rechtlichen Optimierungspotentiale der Formate auszuschöpfen.

Zugleich erheben Software-Hersteller und deren Verbände naturgemäß Bedenken gegen den im EIF verwendeten Begriff des Offenen Standards, die zum Teil im Kontext der Diskussion um Softwarepatente zu sehen sind. Ein durchaus pragmatischer Hinweis ist, dass beispielsweise das PDF-Format kein Offener Standard im Sinne des EIF ist, auf nationaler Ebene – beispielsweise in diesem

1 http://www.microsoft.com/mscorp/ip/format/xmlpatentlicense.asp

2 http://europa.eu.int/ida/servlets/Doc?id=18016

3 http://www.microsoft.com/office/xml/response.mspx

Leitfaden – jedoch eine wichtige Rolle in interoperablen Szenarien spielt. Abzuwarten bleibt also durchaus, wie sich das EIF in den kommenden Monaten in nationalen Frameworks wie SAGA niederschlägt.

Unabhängig davon sind die Nutzungsbedingungen der Microsoft Office 2003-Schemata vergleichsweise restriktiv, die Zugänglichkeit künftiger Versionen ist unklar und Bedeutung und Implikationen der Patent-Lizenz sind weithin umstritten. Daher bieten sich diese Schemata nicht als normiertes Dateiformat an. Aus strategischer Sicht ist OpenDocument daher der Vorzug gegenüber den Office 2003-Schemata zu geben.

3.13.7.3 Fazit

Die strategische Orientierung hin auf dokumentierte und (mehr oder weniger) frei nutzbare XML-Dateiformate steht außer Zweifel. Vom Ideal einiger normierungsfähiger XML-Dateiformate, um die sich beliebige Anwendungen mit generischen Import-Export-Mechanismen scharen können, ist die Wirklichkeit jedoch noch ein Stück entfernt. Eine Organisation, die vor einer Migrationsentscheidung steht, muss daher zunächst abwägen, welches Gewicht sie dem strategischen Ziel normierter XML-Dateiformate beimisst.

XML-Normierung mit hoher Priorität

Steht dieses Ziel bereits kurzfristig im Vordergrund, bietet gegenwärtig nur OpenDocument zusammen mit OpenOffice.org bzw. StarOffice eine vollständige, aus heutiger Sicht zukunftssichere Perspektive. Im Lichte dieser Zielsetzung bietet sich also eine ablösende Migration an.

Die Interoperabilität mit Microsoft Office 2003 auf der Basis von XML-Dateien ist dabei auf Word und Excel beschränkt, ferner mit jeweils unterschiedlich gravierenden Einschränkungen verbunden und in der Handhabung noch recht umständlich. Allerdings unterstützt OOo/SO weiter die Microsoft-Binärformate, so dass auf dieser Basis ein Maß an Interoperabilität hergestellt werden kann, das für den Austausch mäßig komplexer Dokumente ausreicht.

Mittelfristig bleibt abzuwarten, ob und wie Microsoft einerseits die XML-Unterstützung in den Anwendungen komplettiert - hier besonders die Einsetzbarkeit von Standard-Konvertierungsmechanismen wie XSLT-Stylesheets- und ob anderseits Microsoft sich zur Unterstützung des offenen Dateiformat-Standards durchringen kann. Zumindest technisch ist es durchaus vorstellbar, dass die nächste Office-Generation zwei gleichermaßen vollständige und offene Dateiformat-Standards und zwei gleichermaßen interoperationsfreudige Werkzeug-Suiten zur Auswahl anbieten wird.

Mit dem Einstieg in die XML-Dateiformate bis auf diesen Tag zu warten, ist indes nicht sinnvoll. Die gleichen Möglichkeiten, die heute bereits der oben angesprochene "Universalfilter" bietet, stehen auch künftig zur Verfügung, um ganze Dokumentenbestände vergleichsweise mühelos von einem Format ins andere zu wandeln. Nicht zuletzt deshalb ist jede Investition in XML-Dateien sicher, vor allem sicherer als diejenige in Binärdateien.

XML-Normierung mit geringer Priorität

Kann eine Organisation auf die Etablierung normierter XML-Dateiformate zunächst verzichten, ist aber auf Interoperabilität angewiesen, dann bietet es sich gegenwärtig an, diese einstweilen auf der Basis der Microsoft-Binärformate zu realisieren. Die Migrationsentscheidung hängt nicht zuletzt von der Umgebung ab, mit der die Organisation interoperiert.

Eine Migration nach OOo/SO ist angesichts der in Kapitel 3.13.7.1 beschriebenen Einschränkungen dann möglich, wenn eine Organisation entweder

- nie oder nur selten Dokumente gemeinsam mit anderen Organisationen bearbeitet, die MS Office einsetzen, oder
- nur einfache Dokumente, also Dokumente ohne Makros und ohne besondere Formatierungen gemeinsam mit anderen Organisationen bearbeitet werden, die MS Office einsetzen.

Müssen häufig komplexe Dokumente gemeinsam mit anderen Behörden und Organisationen bearbeitet werden und wird in diesen Organisationen MS Office eingesetzt, dann ist zu erwarten, dass sich die Zusammenarbeit durch die Verwendung von OOo/SO über ein hinnehmbares Maß hinaus verkomplizieren wird.

Weitere Kriterien

Neben der XML-Strategie und Interoperabilitätserwägungen ist in vielen Fällen die Integration von Office-Anwendungen mit anderen Anwendungen zu berücksichtigen, insbesondere mit Fachanwendungen.

Diese Integrationen sind beispielsweise dann in die Betrachtung einzubeziehen, wenn Office-Anwendungen mit Hilfe spezieller Verfahren oder Lösungen auf Fachanwendungen zugreifen und wenn diese Funktionalität auch nach einer Migration weiter benötigt wird. Umgekehrt gibt es Fachanwendungen, die sich Dienste von Office-Anwendungen für bestimmte Teilfunktionalitäten zunutze machen, und ohne diese Unterstützung nicht auskommen.

Mit Blick auf eine Migration fallen solche Integrationen in der Regel in einen der folgenden drei Fälle, mit jeweils spezifischen Konsequenzen:

- Die integrierte Lösung kann auch mit der als Migrationsziel in Frage kommenden Anwendung unverändert weiter betrieben werden. In diesem Fall ergeben sich keine Migrationshindernisse.
- Mit der als Migrationsziel vorgesehenen Anwendung ist eine materiell andere, funktional aber identische Integrationslösung möglich. In diesem Fall ist die Umstellung der fraglichen Integration als Teil der Gesamtmigration zu sehen und zu beurteilen.
- Eine funktional identische Integration ist mit einer als Migrationsziel ins Auge gefassten Anwendung nicht zu realisieren. In diesem Fall bieten sich drei Möglichkeiten:

- Die fragliche Office-Anwendung scheidet als Migrationsziel aus.
- Die bisher verwendete Anwendung wird in möglichst eingegrenztem Umfang und nur im Zusammenhang mit der fraglichen integrierten Lösung parallel zu der als Migrationsziel identifizierten und neu eingeführten Office-Anwendung weiterbetrieben.
- Die Fachanwendung, mit der die Office-Anwendung integriert ist, wird angepasst oder abgelöst.

Im letztgenannten Fall bietet sich die Gelegenheit, Backend-orientierte Lösungsarchitekturen voran zu treiben, wie sie in Kapitel 3.9 vorgestellt wurden und auf diese Weise die Abhängigkeit von bestimmten Office-Produkten zu verringern.

3.13.8 Weitere Desktopanwendungen

Neben den zuvor betrachteten Officepaketen gibt es noch einer ganze Reihe weiterer Desktopanwendungen, die für die täglichen Arbeit unverzichtbar geworden sind. Nachfolgend werden zu den wichtigsten Desktopanwendungen, die dem Windows-Desktop zur Verfügung stehen, adäquate Alternativanwendungen auf dem Linux-Desktop kurz mit den wichtigsten Fakten aufgeführt.

3.13.8.1 MS Project und Visio

Für Microsoft Project gibt es derzeit keine vergleichbare Lösung unter Linux. Es gibt zwar einige Projekte (wie z.B. Mr. Project[1] und Gantt Project[2]), die daran arbeiten, heute aber bei weitem noch nicht die Funktionalitäten bieten wie MS Project. Daneben gibt es noch webbasierte Lösungen wie dotproject[3] oder tutos[4], die aber den Nachteil haben, dass sie nicht offline genutzt werden können.

Bei Visio sieht es ähnlich aus, ein wirklich vergleichbares Werkzeug gibt es derzeit nicht. Allerdings kann auf diverse Zeichenprogramme, so z.B. Draw aus O-Oo/SO zurückgegriffen werden.

3.13.8.2 Desktops

Unter den meisten Linux-Distributionen stehen den Anwendern fertige Desktops zur Verfügung, in die die wichtigsten Anwendungen ähnlich dem Windows-Desktop integriert sind. Die beiden Hauptvertreter sind KDE und GNOME.

Die graphischen Benutzeroberflächen der Desktops werden über das X-Window-System und verschiedene Window-Manager realisiert.

---

1 http://mrproject.codefactory.se/

2 http://ganttproject.sourceforge.net/

3 http://www.dotproject.net/index.php

4 http://www.tutos.org/homepage/about.html

Exkurs: X-Window-System und Window-Manager

Das X-Window-System[1], auch einfach als "X" bezeichnet, ist ein netzwerkfähiges Fenstersystem, das insbesondere in Verbindung mit UNIX eingesetzt wird. X basiert auf dem Client-Server-Prinzip, wobei der Server die Ressourcen Bildschirm, Tastatur und Maus zur Verfügung stellt und der Client, der z.B. ein Anwendungsprogramm ist, mit dem Server über das X-Protokoll kommuniziert. Server und Client können dabei sowohl auf getrennten Maschinen als auch auf ein und derselben Maschine laufen. Dies ist beim Einsatz von Linux auf PCs die Regel. Durch die Netzwerkfähigkeit eignet sich X besonders gut beim Einsatz von Thin Clients.

Das „Look and Feel“ der graphischen Benutzeroberfläche wird nicht durch X selbst, sondern durch das jeweils eingesetzte "Toolkit" (z.B. Xt, Athena Widgets, OSF/Motif, Tk, Qt, Gtk+ usw.) und den jeweiligen Window-Manager (z.B. IceWM) bestimmt.

Der Window Manager ist ein X-Client, dessen Aufgabe darin besteht, die Anordnung, Größe usw. der Fenster von Programmen, deren ”Dekoration“, die verfügbaren Farbtabellen und vieles mehr zu verwalten. Für die freie Gestaltung des Desktop stehen eine große Anzahl von Window Managern zur Verfügung[2]. Die nachfolgend beschriebenen Desktops bringen ihre eigenen Window-Manager mit.

KDE

KDE ist eine transparente und moderne Desktop-Umgebung für Linux- und UNIX-Arbeitsplatzsysteme. KDE steht für das Open Source Projekt „K Desktop Environment“. KDE bietet ein „Look and Feel“ ähnlich denen der Windows- und Mac-Desktops (siehe Bild 56). Dieses kann aber auch je nach Bedarf und Geschmack verändert werden (siehe Bild 57).

Grundsätzlich kann fast alles verändert werden. Es können verschiedene Farbthemen, Rahmen und Sätze von Icons gewählt werden und zwar zum Teil in Abhängigkeit von den dahinterliegenden Window-Managern, die auch frei gewählt werden können. Verwendet werden können alle X11R6 Window-Manager. Mit Hilfe dieser flexiblen Gestaltungsmöglichkeiten kann ein auf die individuellen Bedürfnisse einer Behörde oder auch einer Abteilung angepasster einheitlicher Desktop geschaffen werden. Dabei besteht die Möglichkeit beliebige Freiheitsgrade für die Benutzer bezüglich der persönlichen Anpassung einzurichten.

---

1 Weitergehende Informationen finden sie unter http://www.x.org/

2 http://www.plig.org/xwinman/intro.html

Bild 56: KDE-Desktop – Beispiel 1[1]

KDE liefert unter anderem mit Koffice ein eigenes Office-Paket. Weitere Desktopanwendungen für KDE sind:

- der Dateimanager und Browser „Konqueror“ (siehe Kapitel 3.13.8.3 bzw. 3.13.8.4)
- der Mail-Client „KMail“ (siehe Kapitel 3.13.8.5)
- die für das BSI entwickelte Groupware „Kroupware“ (siehe Kapitel 3.12)
- der MediaPlayer „Noatun“

Wichtig sind auch die verschiedenen Aministrations-Werkzeuge und die integrierte Entwicklungsumgebung. Eine komplette Dokumentation ist unter http://docs.kde.org/ zu finden.

[1] Quelle: http://www.kde.org/screenshots/

Bild 57: KDE-Desktop – Beispiel 2[1]

Daneben können natürlich auch alle „Nicht-KDE-Anwendungen“ über KDE nutzbar gemacht werden.

GNOME

GNOME[2] ist Teil des Open Source GNU-Projektes[3]. GNOME steht für „GNU Network Object Modell Environment“. Bezüglich des Layouts ist GNOME genauso flexible wie KDE (siehe Bild 58).

1 Quelle: http://www.kde.org/screenshots/

2 http://www.gnome.org/

3 http://www.gnu.org/

Bild 58: Beispiel - GNOME-Desktop[1]

GNOME bringt ebenfalls ein eigenes Office-Paket und eine Entwicklungsumgebung mit. Einige der bekannten Anwendungen sind:

- die Dateimanager „GNOME Commander“ und „Nautilus“ (siehe Kapitel 3.13.8.3)
- der Mail-Client „Balsa“
- der Browser „galeon“ (siehe Kapitel 3.13.8.4)
- der Packer „GnomeZip“.

Eine weitgehend vollständige Liste der verfügbaren GNOME-Anwendungen wird unter http://www.gnome.org/softwaremap/ bereitgestellt.

Standard Desktops

Im Zusammenhang mit den beiden zuvor aufgeführten Desktops ist es notwendig kurz auf die so genannten Standard Desktops (siehe auch Kapitel 2.3.5) wie den Sun Java Desktop (JDS), den Red Hat Desktop oder den Novell Linux Desktop einzugehen, um deutlich zu machen, wo hier die Unterschiede im Gesamtkonzept liegen. Die Standard Desktops sind eher zu vergleichen mit Editionen von bestimmten Distributionen, ähnlich wie es bei Windows XP die Editionen XP Ho-

[1] Quelle: http://vhost.dulug.duke.edu/~louie/screenshots/2.2/

me und XP Professional gibt. Bei den Standard Desktops ist eines der beiden vorgenannten Desktop-Systeme fester Bestandteil und auf die spezielle Zielrichtung des jeweiligen Standard Desktops angepasst. Basis dieser Desktops bildet eine der Distributionen von Novell/Suse oder Red Hat. Ziel der Standard Desktops ist es, einen auf Basis des gewählten Betriebssystems, von KDE oder Gnome und einem mehr oder weniger festen Bestand an Standardanwendungen sehr stark standardisierten (daher Standard Desktop) PC-Arbeitsplatz zur Verfügung zu stellen, auf dem die verfügbaren Anwendungen noch stärker miteinander verwebt sind als dies bei einer „normalen“ Distribution der Fall ist. Problem dabei ist, dass der Umfang an Software, die für diese Desktops zur Verfügung steht, zunächst beschränkt ist, da diese speziell für den jeweiligen Standard Desktop angepasst wurden bzw. angepasst werden muss, wenn weitere Softwarepakete installiert werden sollen. Eine weitere Besonderheit dieser Standard Desktops sind darauf optimierte und serverbasierte Systemmanagement- und Softwareverteilungssysteme für ein einfaches zentrales Systemmanagement. Eine detailliertere Beschreibung der Standard Desktops enthält Kapitel 2.3.5 im Rahmen der Beschreibung einzelner Linux-Distributionen.

3.13.8.3 Dateimanager

- Konqueror
- Nautilus
- GNOME Midnightcommander

3.13.8.4 Web-Browser

Unter Linux stehen den Anwendern eine ganze Reihe unterschiedlicher Browser zur Verfügung, die je nach Geschmack und / oder Bedarf ausgewählt werden können. Die wichtigsten sind:

- Galeon
  Galeon[1] ist ein GNOME Web-Browser, der auf der Mozilla Rendering Maschine „Gecko“ basiert. Galeon ist ein Leichtgewicht und nur mit den notwendigsten Funktionalitäten ausgestattet, dafür aber schnell und kompatibel zu allen Standards.
- Beonex Communicator
  Beonex Communicator ist ein Open Source Browser, der unter GPL Lizenz steht. Der Browser ist für alle bekannten Linux-Distributionen und auch für andere Plattformen verfügbar, er gehört wie viele andere Browser zur Familie der Mozilla-Browser. Beonex Communicator gilt als einer der sichersten Browser.

[1] http://galeon.sourceforge.net/

- Konqueror
  Konqueror[1] ist nicht nur als Dateimanager (s.o.), sondern auch als Web-Browser unter KDE einsetzbar. Ähnlich wie der Explorer in den Windows-Desktop ist der Konqueror in den KDE-Desktop nahtlos integriert. Konqueror steht ebenfalls unter GPL Lizenz.
- Mozilla
  Mozilla[2] ist ein Open Source Browser, dessen Source Code unter den vier Lizenzen MPL ("Mozilla Public License“), NPL ("Netscape Public License“), LGPL und GPL bzw. unter der so genannten „Dreierlizenz“[3] MPL/LGPL/GPL verfügbar ist.
- Mozilla/Firefox
  Firefox ist eine Lightvariante des Mozilla Browsers. Firefox besitzt im Wesentlichen nur Browserfunktionalitäten. Module des Mozilla Browsers, wie Mail-Client, Adressbuch usw., wurden im Firefox weggelassen. Bei Firefox handelt es sich damit um einen auf die notwendigen Funktionalitäten beschränkten aber dennoch überaus benutzerfreundlichen Internetbrowser.
- Netscape
  Netscape in der Version 7.x basiert auf dem Mozilla Browser und ist mit zusätzlichen Funktionen ausgestattet.
- Opera
  Opera[4] ist ein sehr schneller Browser, der für eine ganze Reihe von Plattformen zur Verfügung steht[5]. Opera ist ein kostenpflichtiges kommerzielles Produkt. Es sei denn, der Benutzer kann mit einer Reihe integrierter Werbe-Banner leben. In diesem Fall ist Opera als kostenfreies Download erhältlich.

Alle der aufgeführten Browser sind weitgehend HTML 4 konform und haben jeweils Vor- und Nachteile, z.B. in der Unterstützung von Java und XML. Wie bereits erwähnt, gilt Beonex als einer der sichersten Browser und Galeon sowie Opera gelten als sehr schnelle Browser. Die nachfolgende Tabelle gibt noch einmal einen zusammenfassenden Überblick.

Tab. 44: OSS Webbrowser Übersicht

Browser	Version[6]	Mail-Client POP3/IMAP	News-Client	HTML 4 konform
Galeon	1.3			x

1 http://www.konqueror.org/
2 http://www.mozilla.org/
3 http://www.mozilla.org/MPL/
4 http://www.opera.com/
5 http://www.opera.com/download/index.dml?custom=yes
6 Stand zum Zeitpunkt der Aktualisierung des Leitfadens.

Browser	Version[6]	Mail-Client POP3/IMAP	News-Client	HTML 4 konform
Beonex	0.8.2	x/x	x	x
Konqueror	3.3[1]			x
Mozilla	1.7.5	x/x	x	x
Firefox	1			x
Netscape	7.1	x/x	x	x
Opera	7.54	x/x		x

3.13.8.5 Mail-Client

Für einen Linux-Desktop gibt es ebenfalls zahlreiche Mail-Clients (u.a. auch die in die Browser integrierten). Zwei von ihnen sollen hervorgehoben und nachfolgend kurz dargestellt werden. Diese sind: K-Mail und Sylpheed:

KMail (mit Ägypten)

KMail[2] ist der KDE Mail-Client, der jedoch auch in jeder anderen Linux-Umgebung eingesetzt werden kann. KMail ist somit auch eine freie Software. KMail bietet für die Behörden einen wesentlichen Vorteil gegenüber anderen Mail-Clients unter Linux:

Für KMail gibt es für die Verschlüsselung und Signierung von E-Mails ein SPHINX-konformes Plug-In. Dieses Plug-In wurde im Auftrag des BSI im Rahmen des Open Source Projekt „Ägypten“[3] entwickelt und wird auch weiterentwickelt. Die SPHINX-Konformität gewährleistet u.a. die Interoperabilität zwischen den verschiedenen SPHINX-konformen Lösungen basierend auf dem „TeleTrust e.V. MailTrusT Version 2“ Protokoll. Somit kann ein Behörden-Anwender im Rahmen der Verwaltungs-PKI mit Hilfe von „Ägypten“ S/MIME verschlüsselte und signierte E-Mails mit Anwendern in anderen Organisationen austauschen, unabhängig davon, ob diese z.B. Outlook mit dem SPHINX-konformen Secude-Plug-In oder LotusNotes mit dem MailProtect-Plug-In einsetzen.

Daneben ist KMail auch Bestandteil der Groupware-Lösung „Kolab“ (siehe Kapitel 3.12).

KMail unterstützt folgende Protokolle:

- POP3
- IMAP
- SMTP
- SMTP AUTH.

---

1 KDE Version

2 http://kmail.kde.org/

3 http://www.gnupg.org/aegypten/

Für POP3, IMAP und SMTP gibt es auch SSL/TLS-Unterstützung.

Sylpheed

Der Mail-Client Sylpheed[1] ist ebenfalls ein Open Source Projekt (GPL) und deswegen erwähnenswert, weil Sylpheed das „Look and Feel“ von Outlook hat und ein schneller E-Mail-Client und News-Reader ist. Sylpheed unterstützt folgende Protokolle:

- POP3
- APOP
- IMAP4
- SMTP
- SMTP AUTH
- NNTP.

3.13.8.6 Weitere Werkzeuge

Im Folgenden werden zu einzelnen Kategorien von Werkzeugen alternative OSS-Lösungen aufgelistet:

- Bildbearbeitung
  - Gimp http://www.gimp.org/
- Videoplayer
  - MPlayer http://www.mplayerhq.hu/
  - XTheater http://xtheater.sourceforge.net/
- Audioplayer
  - SnackAmp http://snackamp.sourceforge.net/
  - MPEG123 http://www.mpg123.de/
  - XMMS http://xmms.org/
- Packer
  - gzip http://www.gzip.org/
  - karchiver http://perso.wanadoo.fr/coquelle/karchiver/
  - gnozip http://www.geocities.com/SiliconValley/9757/gnozip.html
  - gnochive/gnomera http://gnochive.sourceforge.net/index.html

[1] http://www.sylpheed.org/

3.13.9 Integration von Windows-Anwendungen beim Einsatz von Linux-Client

In fast allen Behörden gibt es eine oder mehrere Fachanwendungen oder Standardanwendungen, die dringend zur Erledigung der fachlichen Aufgaben benötigt werden und die leider nur als Windows-Anwendungen zur Verfügung stehen. Wenn es nicht gelingt, diese Anwendungen den Benutzern auch unter Linux zur Verfügung zu stellen, dann wird daran eine Migration hin zu einer Linux-Umgebung möglicherweise scheitern.

Langfristiges Ziel einer Migration nach Linux muss es auch sein, die vorgenannten Anwendungen letztendlich als Linuxanwendungen bereitzustellen. Bei den Standardanwendungen sind die Behörden hier auf die Entwicklungspolitik der Hersteller angewiesen, und da ist in der Regel nicht absehbar, wann diese die jeweilige Anwendung für die eine oder andere Linux-Plattform bereitstellen. Es bleibt zu hoffen, dass durch eine verstärkte Nutzung von Linux und Open Source Software (OSS) innerhalb der Behörden die Hersteller ihre Anwendungen mittelfristig auch für diese Plattform zur Verfügung zu stellen.

Bei den Fachanwendungen, die für eine oder mehrere Behörden als Individualanwendungen entwickelt wurden, müssten die Behörden die Neuentwicklung als plattformunabhängige Lösung oder die Portierung auf eine Linux-Plattform beauftragen. Dies kann allerdings nicht im Rahmen einer Migration durchgeführt werden, da dieses Vorhaben sowohl den zeitlichen als auch den finanziellen Rahmen sprengen würde und wirtschaftlich nicht vertretbar wäre.

Es muss also eine Zwischenlösung gefunden werden, die es den Behörden erlaubt, die o.g. Anwendungen auch unter Linux so lange weiter nutzen zu können, bis einerseits eine Neuentwicklung oder Portierung fachlich begründet und wirtschaftlich vertretbar und andererseits eine Standardanwendung auch als Linux-Anwendung verfügbar ist.

Seit langem gibt es Lösungen, die es auch auf linuxbasierten Arbeitsplätzen ermöglichen Windows-Anwendungen bereitzustellen. Diese Produkte lassen sich in drei Gruppen teilen:

- Lösungen, welche die Ausführung von Windows-Anwendungen direkt erlauben, ohne dass dazu Windows-Lizenzen notwendig sind. Hierzu zählen WINE und Crossover Office.
- Lösungen, die einen PC emulieren können, in dem Windows ausgeführt werden kann, so dass sich dadurch Windows- und Linux-Anwendungen parallel auf einem Rechner ausführen lassen. Hierzu zählen VMware, Win4LIN.
- Serverbasierte Produkte, bei denen Windows-Anwendungen auf einem windowsbasierten Applikationsserver ausgeführt werden und auf dem Linux-Client dargestellt und von dort aus bedient werden: (Citrix, Microsoft Terminal Services).

In jedem Einzelfall muss jedoch genau geprüft werden, welche Lösung für welche Anwendungen, Anforderungen und Umgebungen am besten geeignet ist. Die Eigenschaften der einzelnen Lösungen sowie die Kosten unterscheiden sich deutlich.

Die o.g. Lösungen werden nachfolgend zunächst hinsichtlich ihrer technischen und funktionalen Eigenschaften betrachtet. Insbesondere interessiert dabei der Grad der Integrationstiefe, mit dem die einzelnen Lösungen in das Gesamtsystem eingebunden werden können.

3.13.9.1 VMware

Workstation 4

VMware erlaubt es, u.a. unter Linux in einer virtuellen Maschine andere Betriebssysteme auszuführen. VMware emuliert dabei einen virtuellen Computer mit:

- Festplatten,
- Diskettenlaufwerk,
- diversen Schnittstellen und
- anderer Infrastruktur.

Die Software stellt dabei sicher, dass ein darin ausgeführtes Gast-Betriebssystem parallel zum eigentlichen Betriebssystem (Host-Betriebssystem) des Computers ausgeführt werden kann.

Unterstützte Betriebssysteme

Durch die vollständige Nachbildung eines Computers erreicht VMware eine sehr hohe Kompatibilität zu vielen Betriebssystemen. Unterstützt werden u.a. folgende Gast-Betriebssysteme[1]:

- Alle bekannten Microsoft Betriebssysteme
  (Windows Server 2003, Windows XP, Windows 2000, Windows NT 4.0, Windows ME, Windows 98, Windows 95, Windows 3.1, MS-DOS 6)
- Die bekannten Linux Distributionen inkl. Red Hat, Suse, und Mandrake
- FreeBSD
- Solaris
- Novell NetWare 6.0 und 5.1

VMware Workstation 4.0 steht für alle gängigen Linux-Distributionen zur Verfügung. Das Programm besteht aus einer Erweiterung des Linux-Kernels sowie einem Anwendungsprogramm. Die Erweiterung des Kernels wird im Quellcode

[1] Eine vollständige Auflistung aller unterstützter Gast-Betriebssysteme findet man unter: http://www.vmware.com/products/desktop/ws_specs.html#hostos

geliefert, so dass sie sich theoretisch auf beliebige Kernelversionen portieren lässt.

Ausführbare Programme

In Abhängigkeit des jeweiligen Betriebssystems kann der überwiegende Teil der unterstützten Anwendungen ohne Einschränkungen ausgeführt werden. Lediglich im Bereich von Multimedia-Programmen gibt es leichte Einschränkungen.

VMware Workstation eignet sich daher insbesondere auch für die Nutzung von Fachanwendungen sowie Office- und Internetanwendungen. Das Hauptanwendungsgebiet liegt heute allerdings im Bereich der Softwareentwicklung, da Entwickler die Entwicklung von Multiplattform-Anwendungen auf ein und derselben Maschine parallel unter verschiedenen Betriebssystemen testen können.

Einschränkung

Die vollständige Emulation eines Rechners stellt immer noch hohe Hardware-Anforderungen an die Maschine, auf der diese Emulation durchgeführt wird. Viele Programme laufen daher unter VMware spürbar langsamer als auf einem vergleichbaren echten Computer.

Integrationstiefe

VMware stellt den Desktop von Windows in einem eigenen Fenster auf dem Linux-Rechner dar, auf dem die Emulation erfolgt. Aus diesem Fenster heraus können dann die jeweiligen Windows-Anwendungen aufgerufen werden. Der Datenaustausch zwischen Linux und Windows findet über ein emuliertes Netzwerk statt. Dazu ist es notwendig, dass Samba bei der Installation von VMware eingerichtet wird und somit den Zugriff auf das Heimat-Verzeichnis des Linux-Rechners ermöglicht.

Bild 59: Windows-Desktop unter Linux mittels VMware[1]

Insgesamt liegt jedoch nur eine rudimentäre Integration in den Linux-Arbeitsplatz vor. Die Bereitstellung der Windows-Anwendungen über den Windows-Desktop ist ebenso als wenig ergonomisch zu bewerten.

Kosten

VMware ist ein kostenpflichtiges kommerzielles Produkt[2]. Um Windows-Anwendungen betreiben zu können, fallen zudem Windows-Lizenzen an. Hinzu kommen noch die erhöhten Hardwarekosten aufgrund der gesteigerten Anforderungen, die VMware stellt.

Damit ist es relativ teuer, Windows-Anwendungen mit VMware unter Linux bereitzustellen.

Bewertung

Die wahre Stärke von VMware besteht, wie bereits erwähnt, wohl eher in der Bereitstellung einer guten Entwicklungsplattform für Multiplattform-Anwendungen als darin, Windows-Applikationen unter Linux bereit zu stellen. VMware sollte daher für diese Zwecke nur in Ausnahmefällen eingesetzt werden.

---

1 Quelle: VMware http://www.vmware.com/products/desktop/ws_screens.html

2 Näheres findet sich unter der URL https://www.vmware.com/vmwarestore/newstore/index.jsp

GSX Server

VMware GSX Server basiert auf derselben Technologie wie VMware Workstation. Mit GSX Server können virtuelle Maschinen als Hintergrundprozesse ausgeführt, von Windows- oder Linux-Rechnern aus ferngesteuert und über ein Web-Interface und ein spezielles Scripting-API fernadministriert werden. Damit wird es auch möglich, auf Intel-Hardware mehrere Server-Betriebssysteme gleichzeitig auszuführen und Serverlandschaften auf diese Art zu konsolidieren.

Hinsichtlich „Unterstützter Betriebssysteme“, „Ausführbarer Programme“, „Einschränkungen“, „Integrationstiefe“, „Kosten“ und „Bewertung“ gelten die gleichen Aussagen wie zur Workstation-Variante[1].

3.13.9.2 Win4Lin

Win4Lin 4.0 – Workstation Edition

Win4Lin[2] ermöglicht es, die DOS-basierten Windows-Versionen 95, 98 und ME unter Linux auszuführen. Win4Lin emuliert dabei keinen PC wie VMware sondern stellt die von Windows benötigten Systemdienste durch eine Reihe von Kernel-Modulen bereit. Die Dateien des Windows-Betriebssvstems werden während der Installation so abgeändert, dass dieses die Dienste nicht mehr selbst ausführt, sondern auf die entsprechenden Services der Kernel-Module zurückgreift. Daher laufen Anwendungen unter Win4Lin in der Regel wesentlich schneller als unter VMware.

Mit Win4Lin wird, genau wie mit VMware, der Windows-Desktop in einem eigenen Fenster zur Verfügung gestellt. Nach dem Start des Programms öffnet dieses ein Fenster, in welchem dann Windows bootet. Anschließend kann der Benutzer darin die Windows-Anwendungen starten und damit arbeiten (siehe Bild 60).

Win4Lin verursacht auch keine besonderen Hardware-Anforderungen. Die Software kann auf jedem gängigen PC betrieben werden[3].

Unterstützte Betriebssysteme

Win4Lin kann auf allen gängigen Linux-Distributionen betrieben werden, sofern diese einen Kernel der Versionsfamilie 2.4.x verwenden.

---

1 Die Preise für die Server-Lizenz stehen unter https://www.vmware.com/vmwarestore/newstore/index.jsp

2 Hersteller Netraverse http://www.trelos.com/

3 Hardwareanforderungen gemäß Hersteller: http://www.netraverse.com/products/win4lin40/requirements.php

Wie bereits aufgeführt, können folgende Windowsversionen mit Win4Lin unter Linux ausgeführt werden[1]:

- 95
- 98
- ME

Ausführbare Programme

Mit Win4Lin 4.0 lassen sich i.d.R. Office-, Internet- oder etwa Datenbank-basierte Anwendungen an einem Linux-Arbeitsplatz zur Verfügung stellen.

Einschränkungen

Einschränkungen bestehen in folgenden Punkten:

- Unterstützte Windowsversionen
  Hier ist zu erwarten, dass viele neuere Anwendungen bald nicht mehr unter diesen lauffähig sind.
- Patchen von Windows-Modulen
  Die Einspielung Windows-Patches von Microsoft muss mit Vorsicht erfolgen, da nicht auszuschließen ist, dass durch Win4Lin geänderte Dateien ausgetauscht werden und das System so in einen inkonsistenten Zustand gerät.
- Verfügbarer Speicher
  Den unter Win4Lin betriebenen Windows-Anwendungen können seit Version 4.0 maximal 128Mbytes Arbeitsspeicher zur Verfügung gestellt werden.

  Der virtuelle Speicher wird lediglich durch die verfügbare Speicherkapazität der Plattenpartition begrenzt, auf welcher sich das Benutzer „$HOME/win“-Verzeichnis befindet.
- Schnittstellen-Unterstützung
  Die Schnittstellen DirectX und USB werden nicht unterstützt.

Integrationstiefe

Mit Win4Lin wird genau wie bei VMware der Windows-Desktop in einem eigenen Fenster zur Verfügung gestellt, aus dem heraus die Windows-Anwendungen aufgerufen werden können.

[1] Detailliertere Angaben unter
http://www.netraverse.com/support/docs/400_relnotes.html#install_winver

Bild 60: Windows-Desktop auf Linux mittels Win4Lin [1]

Der Datenaustausch zwischen Linux- und Windows-Anwendungen ist allerdings einfacher als bei VMware. Mit der Technik von Win4Lin können Linux-Verzeichnisse unter Windows einfach als Laufwerke dargestellt werden.

Von einer wirklichen Integration der einzelnen Applikationen kann allerdings auch hier nicht gesprochen werden. Nach seinem Start stellt das Programm ein Fenster dar, in dem der Benutzer Windows booten sieht, bevor er darin Anwendungen starten und damit arbeiten kann.

Kosten

Win4Lin ist ebenfalls ein kostenpflichtiges Produkt. Die Lizenzkosten[2] liegen jedoch deutlich unter denen von VMware. Hinzu kommen allerdings, genau wie bei VMware, die Microsoft Lizenzen, die aber bei den betroffenen Betriebssystemen überschaubar sind. Dadurch können mit Win4Lin Windows-Anwendungen unter Linux wesentlich günstiger als mit VMware betrieben werden.

Bewertung

---

1 Quelle: Netraverse http://www.netraverse.com/products/win4lin40/fullsizescreen shot.jpg

2 Lizenzkosten Win4Lin Workstation Edition; http://www.digitalriver.com/dr/v2/ec_MAIN.Entry10?xid=40113&PN=1&SP=10023&V1=538328&DSP=&CUR=840&PGRP=0&CACHE_ID=0

Trotz einiger technischer Einschränkungen stellt Win4Lin heute in vielen Fällen noch einen gangbaren Weg dar, einzelne einfache Windows-Anwendungen unter Linux zu nutzen, insbesondere dann, wenn eine solche Anwendung nur an einigen wenigen Arbeitsplätzen benötigt wird. Für den Fall, dass eine solche Anwendung doch an mehreren Arbeitsplätzen notwendig ist, bietet sich evtl. die Nutzung des Win4Lin Terminal Server an, der nachfolgend kurz beschrieben wird.

Win4Lin Terminal Server

Mit Win4Lin Terminal Server nutzt Netraverse die Netzwerkfähigkeit des X-Protokolls, um Win4Lin von einem anderen System aus zu benutzen. Dies wird möglich, da die Darstellung des Win4Lin-Fensters mittels dieses Protokolls auf dem Linux-Desktop erfolgt.

Mit Win4Lin Terminal Server wird dann auf einem Linux-Server für jeden Benutzer, der Win4Lin benutzt, eine eigene Sitzung des Programms ausgeführt. Diese werden dabei über das X-Protokoll an die Clients übertragen.

Dies hat den großen Vorteil, dass sowohl Lin4Win und das Windows-Betriebssystem als auch die benötigten Anwendungen zentral installiert und administriert werden können.

WINE

WINE ist ein freies Software Projekt[1], das die Windows-Linux-Integration auf Anwendungsebene konsequent seit 1993 verfolgt und stetig verbessert. WINE setzt bei der Bereitstellung von Windows-Anwendungen unter Linux auf ein grundlegend anderes Prinzip als die zuvor beschriebenen Lösungen.

WINE stellt eine freie Implementierung der Windows API zur Nutzung unter Linux und X-Windows zur Verfügung. Beim Start einer Windows-Anwendung lädt WINE diese, genau wie Windows selbst, in den Arbeitsspeicher des Rechners, verbindet sie mit den von WINE bereitgestellten Bibliotheken und kann die Anwendungen so unter Linux zum Laufen bringen. WINE ist also genau betrachtet doch kein Windows-Emulator.

Die größte Herausforderung liegt nun darin, die verfügbaren Windows-Bibliotheken weitgehend vollständig als freie Implementierungen bereitzustellen, so dass so viele Windows-Anwendungen als möglich unter Linux betrieben werden können. WINE implementiert mittlerweile die Windows-Bibliotheken mit den wichtigsten Funktionen, so dass dies kein Problem darstellt, wenn eine Windows-Anwendung nur auf die Standard-Funktionalität des (Windows-Betriebssystems) zugreift und alle weiteren Funktionen selbst mitbringt. Schwieriger wird es, wenn die Windows-Anwendung überwiegend auf neuere, noch nicht implementierte Funktionen von Windows-Bibliotheken oder auf Bibliotheken anderer Anwendungen zugreift. In diesem Zusammenhang muss auch darauf hingewiesen werden, dass Anwendungshersteller in der Regel bemüht sind, auch ältere Windows-Versionen zu unterstützen und deswegen neuere Features nur selten oder nur

[1] WINE Projekt Homepage: http://www.winehq.com/

optional nutzen, so dass dies in der Praxis nicht unbedingt zu Problemen führen muss.

Mittlerweile unterstützt WINE eine Vielzahl an Anwendungen[1] (siehe nachfolgenden Abschnitt „Ausführbare Programme“) und Features[2].

Unterstützte Betriebssysteme

WINE steht praktisch für jedes Linux-System zur Verfügung und ist Bestandteil der meisten Distributionen.

Ausführbare Programme

Prinzipiell können alle Windows-Anwendungen mit Hilfe von WINE unter Linux ausgeführt werden, sofern die benötigten Bibliotheken verfügbar sind.

Zu den Programmen, von denen dies bekannt ist, gehören u.a. Winword, Excel und Powerpoint aus den Office-Paketen 97 und 2000 sowie der Internet Explorer. In Einzelfällen muss die Funktionsfähigkeit vorab durch einen praktischen Test überprüft werden, wobei zunächst die WINE Anwendungs-Datenbank (http://appdb.winehq.com/) konsultiert werden sollte.

Einschränkungen

Problematisch an WINE ist die immer noch relativ aufwändige Konfiguration des Programms, die viel Know-how voraussetzt.

Integrationstiefe

Windows-Anwendungen werden mit WINE optimal in den Linux-Desktop integriert. Die Programme werden nicht über einen eigenen Desktop gestartet, sondern direkt mit dem Window-Manager des Linux-Desktops in einem eigenen X-Window-Fenster.

---

1 In diesem Zusammenhang soll kurz auf eine Software mit Namen „ganymede“ (http://www.itomig.de/produkte.html) verwiesen werden, mit der die Kompatibilität einer Windows-Software mit WINE analysiert werden kann. Dadurch kann ein ggf. kostenintensiver Testbetrieb verkürzt werden. Leider handelt es sich hierbei um keine OSS und die Software kann auch nicht käuflich erworben werden. Die Nutzung ist nur im Zusammenhang mit einer Beauftragung des Herstellers möglich.

2 Eine Auflistung ist unter der URL http://www.winehq.com/?page=wine_features;winehq=d35c3404fe39283bf96bb1dd54b14c8d zu finden.

Bild 61: Windows-Anwendungen auf dem Linux-Desktop mittels WINE[1]

Kosten

Lediglich die Lizenzkosten für die jeweilige Windows-Anwendung fallen an. Allerdings muss ein gegenüber den anderen Lösungen höherer Administrationsaufwand angesetzt werden.

Bewertung

Dieser Ansatz hat zwei wesentliche Vorteile:

- Es fallen keine Kosten für Windows-Betriebssystemlizenzen an.
- Es muss kein zusätzliches Betriebssystem ausgeführt werden, das die verfügbaren Ressourcen zusätzlich belasten würde. Die Windows-Anwendungen können theoretisch genauso schnell wie unter Windows ausgeführt werden und haben den gleichen Speicherbedarf.

Sofern also die benötigten Bibliotheken für eine Anwendung in WINE verfügbar sind, ist dem Einsatz von WINE durchaus der Vorzug zu geben.

WINE wäre eine Möglichkeit, MS-Projekt auf den Linux-Desktops auszuführen, da es derzeit keine Alternative Linux-Anwendung gibt. Allerdings ist in der Anwendungsdatenbank bisher kein positiver Eintrag zu finden.

[1] Quelle: http://www.winehq.com/?ss=1

Crossover 0ffice

Crossover Office (CO) ist ein Produkt der Firma Code Weavers[1]. CO basiert auf WINE und kompensiert den Nachteil der aufwändigen Konfiguration von WINE dadurch, dass WINE in CO durch ein komfortables Installationsprogramm und Scripte zur Einrichtung der Benutzer und zur Installation der Windows-Anwendungen ergänzt wird.

Ausführbare Programme

Crossover Office unterstützt zurzeit Microsoft Word, Excel und Powerpoint (aus Office 97, 2000 und XP). Weitere Anwendungen wie Outlook 2000/XP[2], IE 5.5 und Notes R5 werden relativ stabil ausgeführt.

Kosten

Neben Lizenzkosten für MS Office kommen noch die Lizenzkosten für Crossover Office hinzu[3].

Bewertung

Ansonsten gelten die gleichen Aussagen wie zu WINE. Wer also bezüglich der Installation und der Konfiguration mehr Komfort bevorzugt, der sollte CO WINE vorziehen.

Crossover Office Server Edition

Die Crossover Office Server Edition erlaubt es, Windows-Anwendungen zentral auf einem linuxbasierten Applikationsserver zu installieren und von dort aus über das X-Protokoll Client-Systemen zur Verfügung zu stellen. Dies hat wiederum den Vorteil, dass die Windows-Anwendungen zentral bereitgestellt und administriert werden können.

WineX

WineX heißt jetzt Cedega[4] und ist ein andere Variante von WINE, bei der sich die Firma Transgaming[5] auf die Verbesserung der DirectX-Unterstützung konzentriert hat. Mit WineX kann eine Reihe von aufwändigen Windows-Spielen unter Linux betrieben werden. WineX wird daher auch nicht näher betrachtet, sondern nur der Vollständigkeit halber aufgeführt.

WineX ist keine freie Software.

---

1 Code Weavers Homepage http://www.codeweavers.com/home/

2 Nur bedingt.

3 Preisinformationen für Crossover Office http://secure.codeweavers.com/store/

4 http://www.transgaming.com/news.php?newsid=119

5 Transgaming Homepage http://www.transgaming.com/

3.13.9.3 Citrix Metaframe

Die Funktionalitäten werden im Kapitel 3.14.5 beschrieben.

Unterstützte Betriebssysteme

(siehe Kapitel 3.14.5)

Ausführbare Programme

Es können alle Windows-Anwendungen ausgeführt werden, die auch unter Windows NT oder Windows 2000 nutzbar sind.

Einschränkungen

Einschränkungen hinsichtlich der Ausführbarkeit von Windows-Anwendungen gibt es nur insofern, als dass grafiklastige Anwendungen (s.o.) nach Möglichkeit nicht über Citrix Metaframe ausgeführt werden sollten.

Integrationstiefe

Genau wie VMware und Win4Lin lässt sich der Windows-Desktop in einem eigenen Fenster auf dem Linux-Desktop öffnen und die Windows-Anwendungen werden in diesem Fenster ausgeführt. Der Datenaustausch kann nur über das Netzwerk erfolgen. Somit liegt auch hier nur eine geringe Integrationstiefe vor.

Kosten

Die Kosten hängen von der jeweiligen Ausprägung des gewünschten Metaframes ab und sind im Einzelfall zu betrachten. Grundsätzlich fallen aber neben den Citrix-Lizenzen auch die gesamten Microsoft-Lizenzen an.

Bewertung

Citrix Metaframe ist als Zwischenlösung für die Bereitstellung von Windows-Anwendungen auf dem Desktop bis diese auch als Linux-Anwendung verfügbar sind, nicht zu empfehlen, da sie vor allem zu teuer und zu komplex ist.

Citrix Metaframe sollte allerdings Berücksichtigung finden, wenn absehbar ist, dass es Windows-Anwendungen gibt, die langfristig weiterbetrieben werden müssen.

Der große Vorteil von Citrix Metaframe ist die zentrale Installation und Verwaltung der Anwendungen sowie die zentrale Datenhaltung. Der Einsatz von Citrix Metaframe eignet sich auch gut in einer Umgebung mit Thin- der Diskless-Clients.

3.13.9.4 Windows Terminal Server

Die Funktionalitäten werden im Kapitel 3.14.5 beschrieben.

Unterstützte Betriebssysteme

(siehe Kapitel 3.14.5)

Ausführbare Programme

Das sind alle Windows-Anwendungen, die auch unter Windows 2000 ausgeführt werden können.

Einschränkungen

(siehe Kapitel 3.14.5)

Integrationstiefe

Hier gilt das Gleiche wie für Citrix Metaframe.

Kosten

Gegenüber Citrix fallen hier nur die Microsoftkosten an.

Bewertung

Diese Variante ist ähnlich zu bewerten wie die Citrix Metaframe Lösung, wobei sie die etwas günstigere Variante ist. Der Nachteil gegenüber Citrix Metaframe ist allerdings, dass es mit Windows Terminal Servern noch nicht so umfangreiche Erfahrungen wie mit Citrix Metaframe gibt, insbesondere für größere und komplexe Umgebungen. Das spielt allerdings bei der Suche nach einer Lösung für das vorliegende Problem nur eine unbedeutende Rolle.

Zusammenfassung

Die Lösungen VMware, Win4Lin, WINE und Crossover Office dürfen lediglich als Zwischenlösung gesehen werden oder als Lösung für einzelne kleinere Anwendungen an einzelnen Arbeitsplätzen. Mittelfristig muss es eine entsprechende plattformunabhängige Anwendung geben, die unter Linux ausgeführt werden kann.

Ansonsten kann geprüft werden, ob Citrix Metaframe eine wirtschaftliche Lösung sein kann, wobei dies wohl eine eher strategische Entscheidung ist.

Unter diesen Voraussetzung können dann folgende Aussagen getroffen werden:

- Bei einer überschaubaren Anzahl von Windows-Anwendungen lohnt sich der Einsatz von WINE (evtl. mit zusätzlichem Entwicklungsaufwand).
- Gibt es viele Windows-Anwendungen, die betroffen sind, dann ist die Wahrscheinlichkeit groß, dass nicht alle Anwendungen mit WINE ausführbar sind. Daher ist zu prüfen, ob Win4Lxn eingesetzt werden kann (Lauffähigkeit unter Windows 95, 98 oder ME).
- Ist die Anzahl der betroffenen Windows-Anwendungen sehr groß, dann stellt sich die grundsätzliche Frage der Sinnhaftigkeit einer Migration (die Grenze ist im Einzelfall zu prüfen).
- Für die Zukunft muss die Forderung nach der Plattformunabhängigkeit der Anwendungen stehen.

3.14 Terminal-Dienste und Client-Konzepte

3.14.1 Überblick

Die Entscheidung für den Einsatz von Terminal-Servern und Thin Clients kann auch innerhalb eines Migrationsprojektes erfolgen und ist daher auch inhaltlicher Bestandteil des Migrationsleitfadens. Es ist jedoch kein klassisches Migrationsthema, da in der Regel keine Terminal Server-Umgebungen migriert werden. Der Einsatz der im Folgenden betrachteten Technik ist primär eine Entscheidung innerhalb der gesamten IT-Strategie der jeweiligen Behörde. Die vorgestellten Lösungen sollen jedoch einen Einblick in die gesamte Thematik geben und das Potential der Technologie verdeutlichen.

Vorgestellt werden Technologien, die in den unterschiedlichsten Bereichen eingesetzt werden können:

- Linuxbasierte Server und Clientsysteme mit dem Linux-Terminal-Server-Projekt
- Terminalservices NX mit linuxbasierten Serversystemen und Clientsysteme für Windows und Linux
- Windows-Terminal-Server mit in erster Linie windowsbasierten Clientsystemen
- Metaframe-Lösung der Firma Citrix mit diversen Clientsystemen (DOS, Windows, Unix, Linux, usw.).

Die vorgestellten Systeme bieten eine große Bandbreite bzgl. der unterschiedlichen technischer Lösungen (Server- und Clientsysteme) und sind im Einzelfall genauer zu betrachten. Neben den technischen Unterschieden und Möglichkeiten variieren die Systeme auch stark im Hinblick auf die Lizenzierungsmodelle und Kosten.

3.14.2 Einleitung

Die Administration und Betreuung von Arbeitsplatz-Rechnern ist eine Aufgabe mit hohem Personalaufwand, insbesondere dann, wenn die Ausstattung der Rechner mit unterschiedlicher Hard- und Software erfolgte. Auch die wachsende Komplexität der eingesetzten Hard- und Software kann die Arbeitsplatzrechner störanfälliger machen und somit die administrativen Aufwände erhöhen. Die mit der Systembetreuung verbundenen Arbeiten werden im Folgenden aufgelistet:

- Installation – ev. Konfiguration vor Ort
- Anpassungen an individuelle Bedürfnisse
- Verwaltung von Softwareaktualisierungen – Erstellung und Pflege von Installationspaketen und Verteilung
- Fehlerdiagnose und –Behebung, Support
- Ersatzbeschaffung

Insgesamt können die Aufgaben mit Unterstützung geeigneter Verwaltungswerkzeuge bzw. Systemmanagementanwendungen automatisiert werden. Die Automatisierung kann die insgesamt benötigten Aufwände verringern, jedoch ist der Arbeitsaufwand in der Regel immer noch sehr hoch. Außerdem ist auch nicht jede Organisation in der finanziellen Lage, sich mit der zum Teil sehr kostspieligen Systemmanagement-Software auszustatten, insbesondere kleinere Organisationen.

Die Verwendung von Terminal-Servern kann die anskizzierten Probleme erheblich reduzieren. Auch im Rahmen von zukünftigen Migrationsprojekten bietet es sich an, über den zukünftigen Einsatz von Terminal-Servern und entsprechenden Thin Clients nachzudenken. In einer herkömmlichen dezentralen IT-Landschaft findet die Installation und Ausführung von Programmen meist auf den Arbeitsplatzrechnern statt. Die Serverstruktur dient primär zur zentralen Datenverwaltung, Datenbackups und der Steuerung der Zugriffsrechte. Bei der Verwendung einer Terminalserver-Lösung liefert einer oder mehrere leistungsfähige Zentralrechner, die eigentlichen Terminal-Server, einen standortunkabhängigen Zugriff auf die notwendigen Daten und Applikationen. Die Terminal-Server bieten den Benutzern einen direkten Zugang zur graphischen Benutzerschnittstelle des Betriebssystems über das Netzwerk. Auf dem Terminal-Server erhält jeder angemeldete Benutzer eine eigene Sitzung (Session) und den Zugriff auf alle verfügbaren Ressourcen des Betriebssystems. Im Gegensatz zu den herkömmlichen dezentralen Arbeitsplatz-Architekturen erfolgt die Bereitstellung nicht nur der Daten, sondern auch Applikationen auf zentralen Servern. Der Zugriff auf die Applikationen und Daten der Terminal-Server muss mittels spezieller Terminal-Programme bzw. so genannter Thin Clients erfolgen.

Die folgende Tabelle gibt einen kurzen Überblick über Vorteile durch den Einsatz von Terminal-Servern und Thin Clients.

Tab. 45: Vorteile von Terminal-Servern und Thin Clients

Vorteile	Erläuterungen
Zentrale Verwaltung	Betriebssystem und Anwendungen werden nur in einfacher Form zentral auf den Terminal-Servern vorgehalten. ❍ Die Pflege der Software kann jetzt zentral erfolgen (Patches, Updates). ❍ Es sind keine Arbeiten an den Client-Systemen mehr notwendig. ❍ Betreuung der Anwendungen findet zentralisiert statt, der Fehlerdiagnose und -behebung wird vereinfacht. ❍ Erhöhung der Produktivität für den Anwender und die Administration. ● Durch die Vereinfachung der Administration wird die Bereitstellung der Applikationen für die Benutzer beschleunigt. ● Durch den Wegfall der personalintensiven Fehlerbehebungen vor Ort werden die administrativen Aufwände drastisch reduziert.

Vorteile	Erläuterungen
Verringerte Hardwareanforderungen	❍ Die Client-System benötigen wenige Hardware-Ressourcen (Netzwerkkarte, Graphikkarte, Tastatur, Maus). ❍ Ein regelmäßiger Ausbau der Client-Hardware, durch erhöhte Anforderungen durch Betreibsysteme und Applikationen, ist nicht mehr notwendig. ❍ Die vorhandene Hardware kann länger genutzt werden.
Erhöhte Sicherheit	Durch den Einsatz von Thin Clients (ohne Festplatten) können Daten nur noch auf den zentralen Servern gespeichert werden [trifft auch auf Fat Clients zu]. Somit ist die Gefahr des Datenverlustes verringert bzw. können auch unbefugte Personen durch Manipulation oder Diebstahl an den Client-Systemen nicht an Daten gelangen.
Unabhängigkeit vom Client	Arbeitsplatzrechner können schnell ausgetauscht werden, weil keine persönlichen Daten oder Einstellungen mehr auf den Clients gespeichert werden. Vor allem aber können Benutzer einfach den Arbeitsplatz wechseln, ohne auf "ihre" vertraute Umgebung verzichten zu müssen.

Neben den oben genannten Vorteilen sind aber auch einige Nachteile zu nennen, die bei der Überlegung für oder gegen den Einsatz von Terminal-Servern abgewogen werden müssen.

Tab. 46: Ausgewählte Nachteile von Terminal-Servern und Thin Clients

Nachteile	Erläuterung
Abhängigkeit	Benutzersitzungen werden bei Ausfall der Terminal-Server abgebrochen und die Arbeitsaufnahme ist erst wieder möglich wenn die Fehler auf dem Terminal-Server behoben ist. Dies kann durch den Einsatz einer Serverfarm minimiert werden. Beim Abbruch der Benutzersitzung kann es zu Datenverlusten kommen.
Erhöhter Ressourcenbedarf	Die Terminal-Server müssen über eine deutlich erhöhte Ressourcen-Ausstattung verfügen, insbesondere beim Speicher. In Relation zum Gesamtbedarf (Server und Clients) werden jedoch weniger Ressourcen benötigt, da bestimmte Operationen auf einem Server nur einmal für alle Benutzer ausgeführt werden müssen und nicht auf jedem einzelnen Client.
Erhöhter Netzwerkverkehr	Die Kommunikation zwischen den Servern- und Clientsystemen erfolgt auf der Netzwerkebene, übertragen werden die Inhalts-Differenzen beim Bildaufbau oder Anweisungen für den Bildaufbau. Bestimmte Anwendungen (Graphikprogramme, usw.) können die Netzlast stark erhöhen. Bei anderen Applikationen (z.B. Textverarbeitung) kann sich Netzwerkverkehr allerdings auch reduzieren, da nicht regelmäßig ganze Dateien beim Speichern übertragen werden sondern nur die Änderungen (Tastatureingaben und Bildschirmveränderungen).

Nachteile	Erläuterung
Anpassungen bzgl. verwendeter Anwendungen	Nicht alle Anwendungen können störungsfrei auf einem Terminal-Server betreiben werden, insbesondere im Windows-Bereich kann es Applikationen geben, die Systemdateien zum Schreiben öffnen und sind somit für andere Benutzer gesperrt. Diese Probleme können oftmals durch administrative Eingriffe gelöst werden.

Für die Anbindung an die Terminal-Server können verschiedene Clienttypen eingesetzt werden.

Fat Clients

Es handelt sich dabei um einen vollwertigen Arbeitplatzrechner. Der Zugriff auf die Terminal-Server erfolgt über eine spezielle Terminalserver-Client-Software.

Bild 62: Ausführen von X-Anwendungen auf einem Fat Client

Thin Clients

Hierbei handelt es sich um Rechnersysteme mit minimalen Hardware-Ausstattungen. Das Betriebsystem beziehen die Clients entweder aus einem Flash-EPROM oder sie können mittels Netzwerk (pxe, tftp, nfs) gebootet werden (siehe Bild 64).

Bild 63: Ausführen von X- und Windows-Anwendungen auf einem Thin Client

Bild 64: Booten eines Linux-Systems übers Netzwerk

Im folgenden werden einige ausgewählte Ansätze zur Realisierung von Terminal-Umgebungen kurz vorgestellt.

3.14.3 Linux-Terminal-Server-Projekt

Das Linux Terminal Server Project (LTSP)[1] nutzt die hervorragenden Linux− und X−Window−Möglichkeiten, um Client-Systeme von Serversystemen booten zu lassen. Die benötigten Applikationen werden anschließend auf dem Serversystem ausgeführt. Die Grafikausgaben der auf dem Server laufenden Anwendungen werden via X−Protokoll zu Terminals übertragen. Die Konfiguration der Client-Systeme erfolgt über einfache Textdateien und bietet eine Reihe von Möglichkeiten über die Nutzung lokaler Drucker bis hin zur lokalen Ausführung von Programmen. Mit dem LTS-Projekt können preisgünstige Arbeitsplatzrechner als Terminals einen Linux- oder anderen Unix-Server nutzen, die Clients können sowohl textbasiert als auch mit graphischer Oberfläche arbeiten.

Der Bootvorgang der Client-Systeme erfolgt über das Netz vom Server aus. Dafür werden auf den Client-Systemen spezielle Boot−ROMS eingesetzt, die in die meisten aktuellen Netzwerkadaptern eingesetzt werden können. Die Verwaltung der Benutzerdaten bzw. Account-Daten erfolgt mit den üblichen GNU/Linux-Bordmitteln.

Nachfolgend werden zwei Beispiele dargestellt, die sich an den LTSP-Ansatz anlehnen.

3.14.3.1 GOto-Konzept

Im Rahmen des Migrationsprojektes des Institutes für Tierzucht wurde das GOto-Konzept[2] verwendet. Die Firma GONICUS hat das GOto-Konzept entwickelt und die Bestandteile als Freie Software verfügbar gemacht.

Die wesentlichen Unterschiede zum LTSP-Ansatz liegen in dem vereinfachten Management auf LDAP-Basis. Alle Konfigurationen und Benutzerprofile werden zentral auf den Servern unter Verwendung des LDAP (Lightweight Directory Access Protocol) Verzeichnisdienstes hinterlegt. Dadurch wird gewährleistet, dass jeder Benutzer an jedem beliebigen Arbeitsplatz Zugang zu seinem speziellen Profil, seinen Applikationen und Daten hat. Die Administration kann mittels des Web-Frontend Gosa erfolgen, dass Frontend ermöglicht den Zugriff auf die benötigten LDAP−Strukturen und deren Verwaltung. Beide Lösungen sind unter der GPL freigegeben.

Das GOto-Konzept erlaubt ebenfalls das vollständige Booten von Thin Client −Systemen über das Netz von den entsprechenden Servern. Der Bootvorgang wurde für das standardisierte PXE−Protokoll erweitert, da entsprechende Boot−Optionen bei vielen Netzwerkkarten mittlerweile zum Standard gehören, so dass in vielen Fällen nicht einmal mehr ein Boot−ROM eingesetzt werden muss. Neben den Thin Clients werden auch Fat Clients unterstützt. Die Verwaltung der Fat Clients kann äquivalent zu den der Thin Clients erfolgen. Nach einer Erstin-

---

1 http://www.ltsp.org/

2 http://www.gonicus.de/

stallation der Fat Clients können diese automatisiert auf einem aktuellen Stand gehalten werden.

3.14.3.2 UCS Thin Client Infrastruktur

Die UCS Thin Client Infrastruktur basiert auf der Distribution UCS und ist eine kommerzielle Lösung. Die UCS Thin Client Infrastruktur ist in ihrer Funktionsweise mit dem Linux Termin Server Projekt vergleichbar.

Die Unterschiede zum LTSP sind genau wie beim GOto-Konzept die Unterstützung des Systemstarts nicht nur über BOOTP, sondern auch über PXE. Daneben werden spezielle Werkzeuge zur Überwachung der Benutzersitzungen bereitgestellt, so dass es beim Ausschalten von Clients nicht zu "Prozessleichen" kommen kann. Zusätzlich wird der Zugriff auf lokale, am Thin Client angeschlossene Geräte wie CDROM, Floppy, Soundkarte oder Drucker ermöglicht (kann aber seitens der Administratoren eingeschränkt werden). Das gesamte Benutzer- und Konfigurationsmanagement befindet sich in einem LDAP-Verzeichnis. Außerdem passt sich die Administration in die von windows- oder linuxbasierter Fat Clients ein.

Im Gegensatz zum LTSP, das während der Authentifizierung das XDMCP-Protokoll verwendet und Passwörter dabei im Klartext im Netzwerk überträgt, wird in der UCS Thin Client Infrastruktur eine sichere Kerberos-Authentifizierung verwendet. Durch ein integriertes Load-Balancing wird eine gute Skalierbarkeit erreicht und bei Bedarf lassen sich einfach zusätzliche Boot- oder Applikationsserver in das System integrieren.

3.14.4 Terminalservices NX

Eine relative neue Terminalserver-Technologie auf der Basis von Linux ist das Produkt NX der Firma Nomachine[1] aus Italien. Es handelt sich hierbei um ein kommerzielles Produkt. Nach einer mehrjährigen Entwicklungsphase gelang es den Entwicklern einen extrem effizienten Kompressor für das X-Window Protokoll zu implementieren. Bekanntlich ist das X-Window System vom Design her netzwerktransparent. Das bedeutet, dass die Ausgabe jeder Anwendung auf einen entfernten Bildschirm erfolgen kann. Leider ist das benutzte Protokoll nicht gerade bandbreitenoptimiert. Daher war eine Nutzung des X-Window Protokoll bisher nur im LAN sinnvoll möglich. Es gab zwar schon einige Versuche, durch Caching von Events und Bitmaps bzw. durch eine Kompression des Protokolls (Low band X) die WAN-Tauglichkeit zu verbessern, die Ergebnisse waren jedoch nicht ausreichend.

Die NX-Technologie hat inzwischen einen Kompressionsfaktor erreicht, der in etwa der von Citrix entspricht. Der NX-Server läuft auf einem oder mehreren Linux Servern und kann neben dem X-Window Protokoll auch das Microsoft RDP und das Frame-Buffer-Prtokoll des VNC-Viewers effizient auf den NX-Client übertragen. Der NX-Client läuft unter Linux, Windows, auf iPAC und Zaurus PDAs.

---

[1] http://www.nomachine.com/

Die NX-Technologie erlaubt neben der effizienten Übertragung von Bildschirminhalten auch den Zugriff auf das lokale Dateisystem und die Übermittlung von Audio-Daten. Eine Umlenkung der seriellen Schnittstelle ist noch nicht möglich. Technologisch basiert das System im Wesentlichen auf Open Source Komponenten. Sämtliche Kompressionskomponenten wurde unter der GPL freigegeben. Die komplette Kommunikation erfolgt verschlüsselt über einen SSH-Tunnel. Ähnlich wie bei Citrix Metaframe ist es möglich, nur die Fenster einer einzelnen Applikation zu "publizieren". Damit lassen sich sehr flexible Integrationen zwischen der Windows- und Linux Applikationswelt realisieren. Es ist damit möglich, Windows-Applikationen auf den Linux-Desktop oder Linuxanwendungen auf den Windows-Desktop zu bringen. Durch die Trennung von Applikationsserver und Kompressions-Knoten, wird eine extreme Skalierbarkeit erreicht. Der Applikationsserver wird dabei nicht durch die Kompression der Daten zusätzlich belastet. Es kommt nicht zu möglichen Versionskonflikten zwischen Applikation und Kompressionsserver.

Interessant ist das Lizenzierungsmodell, da dieses nicht von der Zahl der Clients, sondern von der Zahl der Server-Knoten abhängig ist. Damit ist das Produkt erheblich preiswerter als andere Produkte am Markt.

3.14.5 Windows Terminal Services und Citrix

Die gesamte Anwendungslogik wird zentral von den Servern zur Verfügung gestellt, so dass sich die benötigte Bandbreite zwischen Client und Server auf ca. 10 bis 20 kBit/s beläuft. Durch die Trennung der Anwendungslogik von der Benutzeroberfläche auf den Terminal-Servern wird bei Zugriffen auf File-, Print- und Datenbankserver etc. der Backbone im Vergleich zu klassischen Client-Server-Umgebungen stärker beansprucht.

Ein zentraler Bestandteil der Terminal-Server-Technologie sind die Server, auf denen die Anwendungen installiert sind. Der Terminal-Server ermöglicht den parallelen Client-Zugriff von mehreren Benutzern in so genannten Sitzungen (Sessions), in denen die Benutzer die Anwendungen in einem geschützten Speicherbereich ausführen können. Da im unkonfigurierten Zustand die Benutzer alle Rechte haben, muss das System gegen unbeabsichtigte bzw. unberechtigte Aktionen von Seiten der Benutzer geschützt werden. Hierzu können die aus der NT-Administration bekannten Hilfsmitteln wie serverbasierende Profile, die Anwendung von Policies und Einstellungen von NTFS-Security auf Dateien und Verzeichnissen die nötige Sicherheit gewährleisten.

Außerdem kommt in einer Terminal-Server-Umgebung den Applikationstests eine besondere Gewichtung zu, um ein optimales Server-Sizing durchführen zu können. Es ist daher absolut unerlässlich, zu wissen

- wie viel Prozessorleistung und
- wie viel Arbeitsspeicher eine Applikation beansprucht,
- wie viele Benutzer gleichzeitig auf das Programm zugreifen,

- ob das Programm eine 16-Bit- oder DOS-Anwendung ist,
- ob die Applikation überhaupt multiuserfähig ist.

Die Windows Terminal Service werden für Windows NT 4 in einer separaten Produktvariante („Terminal Server Edition“, TSE) angeboten. Mit Windows 2000 ist dieser Dienst in jedem der Produktvarianten enthalten.

Sofern man nicht Metaframe von der Firma Citrix einsetzt, erfolgt die Kommunikation zwischen Terminal Server und Terminal Server Client über das IP-basierende Protokoll RDP (Remote Desktop Protocol). Windows NT 4 TSE unterstützt die RDP-Version 4, Windows 2000 das erweiterte RDP 5.

Microsoft liefert Terminal Server Clients (RDP Clients) für sämtliche Windows Betriebssysteme (auch 16bit). Drittthersteller liefern zusätzliche RDP-Clients für andere Laufzeitumgebungen (z.B. Java).

Nachteilig bei einer reinen Microsoft-basierenden Terminal Server Lösung, wirkt sich der Umstand aus, dass der Anwender sich mit einen bestimmten Server verbinden will. Dies führt zu Komplikationen, wenn

- der Server nicht verfügbar ist
- oder der Server überlastet ist.

Abhilfe schafft hier das Produkt Metaframe von der Firma Citrix. Mit Hilfe von Metaframe können mehrere Terminal Server logisch zu einer Serverfarm zusammengefasst werden. Der Anwender (Client) sieht dann nicht einen einzelnen Server sondern so genannte veröffentlichte Anwendungen, mit denen er sich verbindet. Auf welchem Server dann seine Anwendungen ausgeführt werden, entscheidet ein Mechanismus innerhalb der Serverfarm.

An dieser Stelle muss deutlich gemacht werden, dass damit die Komplexität des gesamten Citrix-Konzeptes und der Möglichkeiten nicht einmal in Ansätzen wiedergegeben wird, es wird lediglich das grundlegende Prinzip der Technologie angerissen. Dies ist allerdings an dieser Stelle völlig ausreichend, um die grundsätzliche Möglichkeit aufzuzeigen, mit der Windows-Anwendungen auf dem Linux-Desktop mittels Citrix Metaframe ausgeführt werden können.

Um diese Funktionalität zu gewährleisten, beinhaltet Metaframe das so genannte Protokoll ICA (Independent Computer Architecture). Der notwendige ICA Client existiert für

- sämtliche Windows Betriebssysteme
- DOS
- Java
- eine Vielzahl von Unix Derivaten (auch Linux)
- und Handheld Systeme.

Serverseitig werden in erster Linie die oben genannten Betriebssysteme von Microsoft (Windows NT 4 TSE und Windows 2000) unterstützt. Es existieren aber auch Varianten für Unix (z.B. Metaframe für Solaris).

Metaframe wird von Citrix zurzeit noch in zwei Produktvarianten geliefert:

- Metaframe 1.8
- und Metaframe XP.

Die Version XP ist als die strategische Variante zu betrachten, da 1.8 in naher Zukunft ausläuft.

Metaframe ist in großen Umgebungen mit eine Vielzahl von Servern anzutreffen, da diese Umgebungen ein intelligentes „Load Management“ (Lastverteilung)“ erfordern. Werden mehrere Terminal Server zur einer so genannten Serverfarm zusammengefasst, kann eine Lastverteilung für die Server eingerichtet werden.

Die folgende Abbildung zeigt schematisch eine Serverfarm unter Metaframe XP.

Bild 65: Serverfarm unter Metaframe XP

Die Lastverteilung trägt zur Leistungsfähigkeit und Applikationsverfügbarkeit im Gesamtsystem bei, da einem ausgefallenen Server keine Benutzer zugewiesen werden. Sobald den Servern ein Lastauswertungsprogramm zugeordnet worden ist, wird unter Metaframe XP die Auslastung dieses Servers an den Datensammelpunkt (Data Collector) weitergegeben und dort für Verbindungsanfragen gespeichert. Wird eine veröffentlichte Anwendung über den ICA-Client angefordert, so sucht und bestimmt der Datensammelpunkt den Server, der zu dem Zeitpunkt der Anfrage die größte Leistungskapazität hat und teilt dem Client dieses mit. Der Client verbindet sich dann mit diesem Server.

Bei Serverfarmen, die beispielsweise aus 1- und 2-Prozessor Maschinen bestehen, können für die entsprechenden Server die Verteilungsregeln unterschiedlich

gesetzt werden. So bedeutet die Regel Benutzer-Applikationslast für die 2-Prozessor Maschine eine Volllast bei 50 verbundenen Benutzern, während diese bei der 1-Prozessor Maschine schon bei 25 angemeldeten Benutzern erreicht wird. Durch dieses „Tuning“ können Unterschiede bei der Hardware ausgeglichen werden.

Hinsichtlich der Terminal Server Technologie sind folgende technischen Aspekte als sinnvoll bzw. zielführend zu beachten:

- Serverfarmen benötigen eine Windows Domäne (Anmeldung)
- Serverfarmen arbeiten mit servergestützten Profilen, um wandernde Benutzer zu unterstützen (stabile File Services)
- Windows Terminal Server drucken via RPC auf Windows Print-Server, um die Terminal Server zu entlasten
- Das Benutzerkonto in der Windows Domäne wird um zusätzliche Terminal Server spezifische Parameter ergänzt.
- Nicht jede Windows Anwendungen ist lauffähig auf Terminal Servern (Prüfung der Machbarkeit, Integrationsaufwand)

3.15 Hochverfügbarkeit

Um die Umsetzbarkeit von Hochverfügbarkeits-Anforderungen mit Open Source Software vorstellen zu können, wird eine Charakterisierung des Aufgabengebietes benötigt.

3.15.1 Ziele

Hochverfügbare Installation stellen Services so bereit, dass ihre Ausfallzeiten, Mindestkapazität, Datendurchsatz und weitere Parameter bestimmte Grenzen nicht unterschreiten. Für diese Anforderung kann es mehrere Gründe geben:

- Die Services werden intern dringend benötigt, z.B. sind sie die Grundlage für viele Aktivitäten vieler Nutzer und der wirtschaftliche Schaden ihres Ausfalls wäre enorm.
- Die Services sind sicherheitsrelevant, ihr Ausfall kann nationale Interessen behindern.
- Die Services sollen Bürgern oder Firmen ohne Ausfall oder ständig zur Verfügung stehen.

Die Bundesrepublik Deutschland stellt sich mit der E-Government-Initiative den Anforderungen an einen modernen leistungsfähigen Staat. Dies bedeutet zum einen, dass ständig Zugriffe auf BackEnd-Systeme (z.B. Datenbanken) geschehen oder ständig neue Anträge eingehen können, die nicht verloren gehen dürfen. Zum anderen bedeuten die damit verbundenen längeren Service-Zeiten auch neue Anforderungen an die Frontend-Systeme: Es sollen nicht nur die Kosten gesenkt und die Bearbeitungsdauer gekürzt, auch das Image der öffentlichen

Verwaltung kann durch solche Initiativen deutlich verbessert werden. Eine Nichtverfügbarkeit der Services würde die Ziele jedoch konterkarieren.

3.15.2 Die „fünf Neunen“ und die Realität

Hochverfügbare Systeme (HA-Systeme, nach dem englischen *high availability*) werden u.a. nach der prozentualen Zeit, in der sie die Services bereitstellen, kategorisiert. Was dies für ein HA-System, das rund um die Uhr bereitstehen soll, bedeutet, verdeutlicht die nachfolgende Tabelle:

Tab. 47: Anforderungen an ein HA-System

Verfügbarkeit	maximaler monatlicher Ausfall	maximaler jährlicher Ausfall
99,5%	3 Stunden, 39 Minuten	43 Stunden
99,7%	2 Stunden, 12 Minuten	26 Stunden
99,9%	44 Minuten	8 Stunden
99,99%	4 Minuten	1 Stunde
99,999%		5 Minuten

Diese oft zitierten Zahlen sind jedoch nicht realistisch. Die meisten Servicegütevereinbarungen (SLAs, *service level agreements*) enthalten definierte Wartungszeiten. In denen steht der Service nicht zur Verfügung, die Zeitdauer wird aber nicht als Ausfall gewertet. D.h., in den meisten Fällen wird Hochverfügbarkeit durch *ungeplante Ausfälle* kategorisiert.

Als Beispiel kann die Anforderung an eine SAP-Datenbank lauten, dass sie in der Bürozeit von 7–19 Uhr zu 99,99% bereitsteht. Durch die Möglichkeit von Systemarbeiten außerhalb dieser Uhrzeiten sind solche Anforderungen viel leichter und damit kostengünstiger zu realisieren als ein unrealistischer Anspruch von maximal 5 Minuten Ausfallzeit im Jahr bei 24x365 Betrieb.

3.15.3 Vorgehensweise

Hochverfügbarkeit wird erzeugt, indem Ressourcen redundant vorgehalten und ihre Funktionalität überwacht werden. Bei Fehlverhalten übernimmt eine Ersatzkomponente automatisch den Dienst. Ab dann ist allerdings die Redundanz beeinträchtigt oder sogar nicht mehr vorhanden, es müssen also unverzüglich Reparaturarbeiten vorgenommen werden. HA-Systeme benötigen so einen sehr hohen Betreuungsaufwand, sie laufen nicht von alleine. Ein wichtiger Qualitätsmaßstab ist dabei die benötigte Zeit bis zur Reparatur (MTTR, mean time to repair) anstelle der Zeit bis zu einem Fehler (MTBF, mean time between failure).

Redundanz kann auf allen Ebenen erzeugt werden:

Tab. 48: Zusammenstellung Abstraktionsebenen

Abstraktionsebene	
Benutzer- bzw. Administrationsumgebung	Disaster Recovery
Applikation	Verteilte Applikationen
Middleware	Clustering
Betriebssystem	Ressourcen überwachen, restart, failover
Hardware	Komponenten verdoppeln

Hardware-Redundanz bei Platten ist heute schon Standard (Spiegelung, RAID1; der Einsatz von RAID5 ist heutzutage kaum mehr vertretbar) und auf allen Plattformen verfügbar. Bei anderen Hardware-Komponenten wird es schon schwieriger: Redundant konfigurierbare Netzwerkkarten werden nur selten unterstützt. Im Zentrum der Ausführungen steht die Unterstützung der Hardware-Redundanz durch das Betriebssystem. Hier haben die proprietären Unix-Systeme und natürlich auch die Mainframes erhebliche Vorteile, die nach Einschätzung der Autoren auch in nächster Zeit von den Open Source Systemen nicht aufgeholt werden.

Redundanz auf der Betriebssystemebene wird durch die Überwachung von Ressourcen und deren Verlagerung auf einen anderen Rechner bei Defekt (failover) realisiert.

Einige Middleware-Komponenten (z.B. Datenbanken oder Transaktions-Monitore) stellen die Möglichkeit bereit, eine Vielzahl von Systemen als ein einzelnes zu behandeln. Einige Applikationen benötigen das nicht, weil sie per se verteilt auf vielen Rechnern ablaufen und das Abstürzen von einem der Rechner keine Probleme bereitet.

Wenn Hochverfügbarkeit auf einer Abstraktionsebene bereitgestellt werden kann, ist es in der Theorie für alle darunter liegenden Abstraktionsebenen ausreichend. In der Praxis wird die Robustheit und damit die Zuverlässigkeit eines HA-Systems erhöht, indem Redundanz-Maßnahmen auf möglichst vielen Ebenen vorgenommen werden – schließlich kann auch ein HA-Subsystem einmal fehlerhaft sein, welches dann durch eine andere redundante Komponente abgefangen werden kann.

Letztendlich darf die größte Fehlerquelle überhaupt nicht vergessen werden: Der Mensch, hier in der Rolle der Systemadministratoren oder der Programmierer. Administrations- oder Programmierfehlern werden häufig vom System übernommen: anschließend sind alle redundant vorgehaltenen Services oder Komponente in dem fehlerhaften Zustand. Wenn z.B. durch ein Administrationsfehler ein paar Hundert GB gelöscht werden, hilft keine Spiegelung und keine Service-Redundanz – die Daten sind dann auf allen Komponenten gelöscht. Deshalb sind gute Backup und Restore, u.U. auch Disaster Recovery im Rahmen der Business Continuity Planung, elementare Bestandteile einer HA-Lösung.

3.15.4 Kategorien von HA-Systemen

Während das Basisprinzip der Hochverfügbarkeit immer Redundanz ist, kann diese Redundanz unterschiedlich erzeugt werden:

- Failover:
  Dies ist die „klassische“ Architektur eines HA-Systems; zwei bis drei Maschinen, die bei Ausfall eines Services zuerst versuchen, den wieder zu starten. Wenn das nicht geht, wird der Service auf die anderen Maschine transferiert und dort gestartet.
- Application Clustering
  Einige wenige Applikationen sind bereits clusterfähig und in der Lage, auf mehreren Maschinen zu arbeiten, die sie nach außen als ein System aussehen lassen und in dem der Ausfall von einzelnen Maschinen transparent verkraftet wird. Das bekannteste Beispiel dieser Architektur ist Oracle 9*i* mit der Real Application Cluster (RAC) Option.
- Server-Farmen
  Diese Vorgehensweise ist insbesondere bei Web-Servern populär geworden. Ein „*load balancer*“ verteilt einkommende Requests auf eine Menge von Maschinen. Diese Methode ist vor allem bei Services anwendbar, die keinen Zustand haben. Häufig wird sie für die Front-End-Realisierung genutzt, während die BackEnds auf einer Failover-Anlage betrieben werden.

Im Datenbankbereich wird häufig auch Redo-Log-Shipping zum Disaster Recovery eingesetzt. Dabei werden von allen Transaktionen Redo-Logs erzeugt und diese dann zum Backup-Rechner übertragen, wo ihre Abarbeitung den aktuellen Datenbankzustand auch auf dem Backup-System herstellt.

Durch diese Kategorisierung kann eingeordnet werden, welche Hochverfügbarkeits-Lösungen existieren und wo Open Source Produkte sinnvoll einzusetzen sind:

Bild 66: HA-Lösungen

Die ungenügende Realisierung der Cluster-Typen, die mit wenigen großen vollständig redundant ausgelegten Maschinen arbeiten, liegt vor allem an der eingesetzten Spezialhardware, für die es häufig keine ausreichende Unterstützung im Betriebssystem gibt.

Open Source Software kann vor allem im Bereich der Server-Farmen eingesetzt werden, idealerweise bei Systemen ohne große Session-Zustände. Typische Vertreter sind Web-Server, E-Mail-Gateways, File- und Print-Server.

Es gibt wenige Open Source Anwendungen bei Applikationsservern. Hier können sie eingesetzt werden, wenn die SLA-Anforderungen nicht sehr hoch sind (z.B. 99,9% während der Bürozeiten o.ä.) Meistens wird dann die Hochverfügbarkeit über eine Failover-Architektur sichergestellt, es gibt aber auch Clustering-Möglichkeiten auf der Middleware-Ebene (z.B. bei JBoss).

Hochverfügbare Open Source Datenbanken gibt es keine. Hier können jedoch der Einsatz der proprietären Software (z.B. Oracle RAC) auf Linux geplant und zum Teil erhebliche Einsparungen an Hardware-Kosten erzielt werden.

3.15.5 Proprietäre HA-Software

HA-Software ist eine Domäne der Unix- und Mainframe-Welt, Windows DataCenter wird in der Regel als nicht ausreichend für mission-critical Anwendungen gesehen.

Auf Betriebssystem-Ebene stellt jeder der großen Unix-Hersteller eine HA-Lösung nach der Failover-Architektur bereit; HP nach der Fusion mit Compaq sogar zwei, von der hier nur die Überlebende benannt wird:

Tab. 49: Übersicht

	IBM	HP	Sun
Betriebssystem/ HA-Paket	AIX HACMP	HP-UX MC/Serviceguard	Solaris Sun Cluster
Dateisystem	JFS2	HFS	UFS mit Sun VM
clusterweites Dateisystem	ja	nein	ja
Maximale Anzahl Maschinen	32	16	8
Multiple Anwendungs-Instanzen unterstützt	ja	ja	ja
Partitionierung	ja	ja	ja
Failover bestehender TCP-Verbindungen	nein	ja	ja
Speicher-Technologie	Ultra3 SCSI Fiberchannel	Ultra3 SCSI Fiberchannel	Ultra3 SCSI Fiberchannel
Optionen zum Disaster Recovery	HAGEO GeoRM	CampusCluster Metrocluster Continental cluster Continuous Access XP	Storage Data Network replicator
Management	GUI integriert in SMIT	separates GUI	GUI integriert in SUNMC

Wie bereits erwähnt, ist Oracle RAC im Datenbankbereich eine wichtige Möglichkeit, Hochverfügbarkeit auch auf der Middleware-Ebene bereitzustellen. Diese Lösung ist für die proprietären Unix-Systeme, Linux und Windows-Server verfügbar.

3.15.6 Open Source HA-Software

Die Welt der Open Source Tools unterliegt einer extrem schnellen Entwicklung. Der folgende Abschnitt gibt einen Überblick über existierende Open Source HA-Software, die in breiten praktischen Einsatz ist und sich an vielen Installationen erprobt hat. Für konkrete HA-Projekte kann sie aber nur ein Hinweis auf potentielle Nutzbarkeit sein. Jedes Projekt muss aufs Neue die Architektur festlegen und die Anwendbarkeit der jeweiligen Tools überprüfen. Die Autoren der Studie empfehlen dazu dringend, erfahrene Spezialisten in die jeweiligen Projekte einzubinden.

Viele der unten genannten Tools werden selbstverständlich auch von Firmen bereitgestellt. In Deutschland sind fast alle linuxbasierten Tools von Suse erhältlich. Support und Projektunterstützung liefern viele Firmen, u.a. auch EDS.

3.15.6.1 Plattensubsysteme

Seit dem Linux-Kernel 2.4, der in allen aktuellen Distributionen verwendet wird, unterstützt Linux die Plattenspiegelung mit Hilfe des Multi-Disk (md) Kernel-

Moduls. Dieses Subsystem unterstützt auch multi-path-Zugriff, d.h., den gleichzeitigen Anschluss von Platten-Subsystemen an verschiedene Rechner. Dies wird für Daten- und Anwendungsplatten in einer Failover-Architektur benötigt; Systemplatten müssen immer an genau einem Rechner angeschlossen sein.

Mit LVM existiert ein funktionierender Volume Manager. ext3 entwickelt sich zum Standard-Filesystem mit Journaling-Eigenschaften (siehe auch Kapitel 3.2.3).

3.15.6.2 Failover mittels heartbeat

Für Linux-Systeme kann eine Failover-Architektur durch heartbeat realisiert werden. heartbeat unterstützt die Definition von Ressource-Gruppen (Services, Dateisysteme und IP-Adressen), die bei Ausfall auf einem anderen Server gestartet werden können. Der Anwendungszustand existierender Sessions wird dabei nicht übernommen.

Da Linux keine Multi-Path-Konfiguration von Netzwerkkarten unterstützt, kann die Überprüfung der Service-Verfügbarkeit über unterschiedliche Kommunikationskanäle (seriell und Netzwerk) durchgeführt werden.

Häufig soll bei Service-Ausfall das Gerät vollautomatisch gebootet werden. Die am meisten dokumentierte Lösung „watchdog“ ist fehleranfällig und führt zu überflüssigen Reboots. Ein neues Modul namens „hangcheck-timer“ soll in vielen Situation besser sein. Die Auswahl des jeweiligen Moduls sollte den Beratern überlassen werden, die die konkrete HA-Architektur für den Anwendungsfall planen.

Jedes HA-Projekt sollte sich auch über die Einschränkungen der Open Source Failover Lösung im Klaren sein: Es gibt kein clusterweites Dateisystem, die maximale Anzahl der Maschinen in einem Failover-Cluster sollte drei nicht übersteigen, die logische Partitionierung existierender Maschinen (Zuordnung von Hardware-Ressourcen wie CPU und Plattenplatz zu Ressource-Gruppen) wird nicht unterstützt, und Optionen zum Disaster Recovery sind auch nicht vorhanden.

heartbeat ist als Modul in weitem Einsatz; das Linux-HA Projekt gibt an, es gäbe weltweit mehrere Tausend Installation im produktiven Einsatz. Es ist das Kernstück der HA-Lösungen, die führende Linux-Hersteller (Suse, Conectiva, Mandrake) anbieten. Ein bekannter Nutzer in Deutschland ist der Bayerische Rundfunk, der die Olympia-Web-Site 2002 der ARD als Linux-Lösung mit heartbeat realisierte.

Im Hause des Bundesbeauftragten für den Datenschutz konnte im Rahmen des Migrationsprojektes auf Basis von Heartbeat[1] eine zuverlässige Hochverfügbarkeitslösung realisiert werden. Die folgende Abbildung gibt einen Überblick über die eingesetzte Lösung und deren Architektur.

[1] http://linux-ha.org/heartbeat/

Bild 67: Lösung mit Heartbeat und DRBD

Die eingesetzte Programmkombination, bestehend aus Heartbeat und DRBD[1] (Distributed Replicated Block Device) realisiert eine Hochverfügbarlösung für den Datei- und Druckservice, die Maildienste, den Webserver, die Domaindienste (DNS, DHCP) und den Verzeichnisdienst. Die Überwachung der Serverknoten erfolgt mittels Heartbeat, zu diesem Zweck wurden die Maschinen mit einen Crossover-Ethernet und seriellen Nullmodemkabel verbunden. Kann der aktive Server nicht mehr über diese Kommunikationswege erreicht werden, übernimmt automatisch der Failover-Server die virtuelle IP-Adresse und die entsprechenden Dienste. Neben der Hochverfügbarkeit wird durch das Programm DRBD eine Raid-1 Spiegelung der Partitionen bzw. logical Volumens erzielt. Somit stehen bei einem Ausfall des aktiven Servers die geschrieben Daten bereits dem zweiten System zur Verfügung. Der Einsatz von DRBD kann für bestimmte Szenarien eine kostengünstige Alternative zu externen SAN-Systemen darstellen.

3.15.6.3 Server-Farmen

Der Linux Virtual Server (LVS) stellt die Infrastruktur für eine Server-Farm bereit. Ein Last-Balancierer unter Linux verteilt einkommende Requests auf eine Menge realer Systeme. Für den Endanwender sind diese realen Systeme nicht sichtbar, die gesamte Installation sieht für ihn wie ein einziger großer Server aus. Typische Anwendungsbeispiele sind Web-, Email- oder Media-Server.

Der Einsatz eines Linux Virtual Servers wird häufig mit einer Failover-Architektur für den Last-Balancierer verbunden. Für die einfache Kombination dieser beiden Technologien gibt es das UltraMonkey-Projekt oder das Open Source Produkt Piranha von Red Hat.

LVS ist bei vielen Firmen im produktiven Einsatz. Sehr große Web-Sites wie `linux.com` und `sourceforge.net` sichern ihre hochverfügbare Internet-Präsenz mit LVS. Real Networks nutzt LVS für ein Cluster von Media-Servern.

3.15.6.4 Application Clustering

Die führenden Open Source Applikationsserver stellen Application Clustering bereit:

[1] http://www.complang.tuwien.ac.at/reisner/drbd/

- Tomcat ist der low-level Applikationsserver, mit dessen Hilfe Java-Servlets und Java Server Pages (JSP) realisiert werden. Er unterstützt Clustering durch sein Last-Balancierungs-Feature. Tomcat ist ähnlich weit verbreitet wie Apache.
- JBoss ist einer der Stars der Open Source Welt: ein vollwertiger Applikationsserver, der die J2EE-Standards realisiert. Alleine in 2002 gab es mehr als 2 Millionen Downloads nur von der Referenz-Site, die Anzahl der Implementierungen im produktiven Einsatz ist sehr groß. Zu seinem Funktionsumfang gehört auch Application Clustering.

Open Source Datenbanken stellen keine hochverfügbaren Lösungen bereit. Meistens ist eines der Hauptprobleme die fehlende Möglichkeit des Online-Backups. Für Linux-Systeme stellt Oracle aber seine RAC-Option bereit, so können im Hardware- und Service-Bereich erhebliche Einsparungen erspart werden.

3.15.6.5 Compute Cluster

Der Vollständigkeit halber soll an dieser Stelle auch noch auf die HA-Lösungen im High Performance Computing verwiesen werden, auch wenn dieses Einsatzgebiet für die öffentliche Verwaltung nur eingeschränkt von Interesse sein wird: Beowolf war die erste Compute-Cluster-Realisierung unter Linux und wird auch heute noch am häufigsten eingesetzt. Job Scheduling innerhalb eines Clusters wird durch das Portable Batch System (PBS) oder den MAUI Scheduler bereitgestellt.

4 Rechtliche Aspekte

4.1 Einleitung

Die Wahl einer Behörde zwischen einer fortführenden und einer ablösenden Migration beruht in erster Linie auf technischen und wirtschaftlichen Kriterien. Die Entwicklungen der letzten Jahre haben allerdings gezeigt, dass auch rechtliche Aspekte eine erhebliche Rolle spielen können.

Die Entscheider in Behörden sehen sich zum einem der Aufgabe gegenüber, die rechtlichen Risiken zu bewerten, die mit einer ablösenden Migration einhergehen. Die ablösende Migration bringt es mit sich, dass die Behörde mit neuen Vertragspartnern zusammenarbeiten muss. Das Profil der in Anspruch genommen Dienstleistungen ändert sich, das Gleiche gilt für die rechtliche Bewertung dieser Vertragsverhältnisse. Hierbei sind auch urheber- und patentrechtliche Fragen zu beurteilen. Zudem gilt es Haftungsrisiken zu evaluieren. Zugleich ist zu fragen, welche Ansprüche die Behörde gegenüber ihren Vertragspartnern und Dritten geltend machen kann, wenn die eingesetzten Programme fehlerhaft sind oder einer Nutzung Rechte Dritter entgegenstehen. Schließlich sind die Beschaffungsvorgänge so zu gestalten, dass Ausschreibungen und Vergabeentscheidungen den Anforderungen des Vergaberechts entsprechen.

Die Entscheider sind zum anderen aber auch aufgerufen, die rechtlichen Risiken einer ablösenden Migration mit denjenigen zu vergleichen, die sich bei einer fortführenden Migration ergeben. Erst in der vergleichenden Perspektive lassen sich Chancen und Risiken realistisch bewerten.

Im Folgenden soll die Behörde als Nutzer von Informationstechnologie im Vordergrund stehen. Fragen, die sich bei der Entwicklung und beim Vertrieb von OSS durch Behörden ergeben, werden dagegen nur am Rande gestreift. Sie liegen außerhalb des Fokus des Migrationsleitfadens.

Das folgende Kapitel wird vier Fragenkomplexe schwerpunktmäßig beleuchten:

- Vertragsrecht
- Urheber- und Patentrecht
- Haftung und Gewährleistung
- Vergaberecht

4.2 Methode

Im Folgenden wird als Ausgangspunkt die Situation einer ablösenden Migration betrachtet. Am Ende der einzelnen Unterabschnitte werden vergleichende Hinweise zur Situation bei einer fortführenden Migration gegeben. Grundsätzlich werden also auch bei den rechtlichen Fragestellungen beide Migrationswege betrachtet. Die rechtlichen Besonderheiten, die sich bei der Nutzung von OSS und

COLS ergeben, stehen aber im Vordergrund. Diese Schwerpunktbildung ist gerechtfertigt, weil sich bei einer fortführenden Migration für die Behörde zumeist keine Unterschiede zur Ausgangslage ergeben. Dagegen bringt die ablösende Migration erhebliche Veränderungen für die Rechtslage mit sich. Vor diesem Hintergrund ist es verständlich, dass Entscheider primär Fragen zu den Rechtsfragen der OSS haben. Der Migrationsleitfaden richtet sich an diesem Interessenschwerpunkt aus.

Die Rechtsfragen der OSS haben zu einer regelrechten Flut juristischer Fachveröffentlichungen geführt[1]. Hinzukommt eine erste Entscheidung des Landgerichts München vom 19.05.2004, welche die Wirksamkeit einiger zentraler Aspekte der GPL bestätigt hat[2]. Es ist dennoch darauf hinzuweisen, dass bislang keine höchstrichterlichen Entscheidungen zu den Rechtsfragen der OSS ergangen sind. Zudem werden in der stark akademisch geprägten Fachliteratur einige Fragen uneinheitlich beurteilt. Es kann nicht die Aufgabe dieses Leitfadens sein, jedes Detail dieser juristischen Fachdiskussion nachzuzeichnen. Vielmehr muss es mit einer Darstellung der jeweils vorherrschenden Auffassung sein Bewenden haben. Abweichungen in der juristischen Fachliteratur zu einzelnen Fragen sind ausdrücklich vorbehalten.

4.3 Notwendigkeit der Rechtsberatung im Einzelfall

Der Abschnitt zu den rechtlichen Aspekten verfolgt zwei Ziele. Er will zum einen dabei helfen, unberechtigten Ängsten durch gezielte Informationen entgegenzutreten. Zum anderen erscheint es als notwendig, dort auf rechtliche Probleme hinzuweisen, wo sie tatsächlich bestehen. Wo eines der aufgezeigten Rechtsprobleme auftritt, kann der Migrationsleitfaden eine individuelle Rechtsberatung nicht ersetzen. Hier müssen die Behörden auf Rechtsämter, Rechtsabteilungen oder externen Sachverstand, insbesondere Rechtsanwälte zurückgreifen. Dies gilt auch für die Vertragsgestaltung im Einzelfall.

4.4 Vertragsrecht

4.4.1 Ablösende Migration: Vertragsverhältnisse

Bei Softwareüberlassungsverträgen sind grundsätzlich zwei Vertragsgegenstände zu unterscheiden: Die Software als solche, also die Bits und Bytes und die Nutzungsrechte an der Software, welche oftmals entsprechend internationaler Sprachgewohnheiten als Einräumung einer "Lizenz" bezeichnet wird. Die Lizenz kann dem Nutzer Unterschiedliches gestatten. Sie kann das einfache Laufenlassen der Software gestatten, sie kann dem Nutzer aber auch Entwicklungs- und Vertriebsbefugnisse einräumen. Proprietäre Softwarelizenzen erlauben typi-

1 Eine Auflistung von ca. 40 deutschsprachigen und einer Reihe fremdsprachiger Beiträge findet sich nter http://www.ifross.de.

2 Vgl. Landgericht München, Urteil vom 19.05.2004, AZ 21 O 6123/04, Computer und Recht 2004,S. 774.

scherweise nur das Ablaufenlassen des Programms; OSS-Lizenzen sind demgegenüber durch besonders weitgehende Rechtseinräumungen gekennzeichnet.

Typischerweise erhält der Nutzer von OSS die Software als solche nicht direkt von den Rechtsinhabern, also den Inhabern der geistigen Eigentumsrechte an OSS - das sind die Entwickler oder Unternehmen, die die Programme entwickelt haben. Der Nutzer wird in aller Regel eine Distribution erwerben, und zwar entweder vom Distributor direkt oder von einem Dienstleister. Gerade für kleinere Behörden ebenfalls denkbar, aber praktisch weniger relevant, dürfte der Erwerb einer Distribution im Einzelhandel sein. In allen genannten Konstellationen fallen der Erwerb der Rechte vom Rechtsinhaber einerseits und der Erwerb der Bits und Bytes andererseits auseinander. Es handelt sich deshalb typischerweise um ein Dreipersonenverhältnis zwischen Nutzer, Rechtsinhaber und Zwischenhändler (Distributor, Softwarehaus, Beratungsunternehmen, Einzelhandel, Dienstleister) mit jeweils rechtlich unabhängigen Vertragsverhältnissen:

Bild 68: Vertragsverhältnisse

Der Nutzer braucht für die Benutzung der Software zunächst lediglich einen Vertrag mit dem Zwischenhändler, auf dessen Grundlage er die Software als solche erwirbt. Bereits durch den Erwerb einer rechtmäßig in Verkehr gebrachten Programmkopie erwirbt der Nutzer die Befugnis, das Programm bestimmungsgemäß zu benutzen.

Möchte der Nutzer die zusätzlichen Rechte aus der GPL oder einer anderen OSS-Lizenz wahrnehmen, so muss er einen weiteren Vertrag abschließen, diesmal mit den Rechtsinhabern. Nur wenn eine solche Nutzung der OSS gewünscht wird, ist die OSS-Lizenz überhaupt relevant. Möchte der Nutzer die Software dagegen nur ablaufen lassen, so bedarf es nicht des Abschlusses eines Lizenzvertrags mit den Rechtsinhabern.

Die wichtigsten OSS-Lizenzen (GPL und Lesser GPL (siehe auch Kapitel 2.4.1 und 2.4.2)) klammern die einfache Benutzung des Programms aus ihrem Anwendungsbereich aus, vgl. Paragraph 0 Absatz 2 GPL: "Activities other than co-

pying, distribution and modification are not covered by this license; they are outside its scope. The act of running the program is not restricted [...]." Dies korrespondiert mit den Regelungen des deutschen Urheberrechts. Gemäß § 69d Abs. 1 UrhG bedarf es für die "bestimmungsgemäße Benutzung" eines Computerprogramms keiner Lizenz oder sonstigen Erlaubnis des Rechtsinhabers, sofern das Programm rechtmäßig in Verkehr gebracht worden ist. Solange sich also der Distributor und der Zwischenhändler an die Bedingungen der Lizenz gehalten haben und der Vertrieb rechtmäßig gewesen ist, bedarf der Nutzer für die einfache Benutzung des Programms keines Vertrags mit den Inhabern der Rechte an dem Programm. Die GPL oder sonstige OSS-Lizenz ist dann irrelevant.

Einige OSS-Lizenzen klammern die einfache Benutzung nicht ausdrücklich aus, dies gilt insbesondere für die BSD Lizenz (siehe 2.4.3). Dies ändert aber nichts an der Tatsache, dass der Nutzer eines rechtmäßig in Verkehr gebrachten Programms im Normalfall keiner weiteren Lizenz bedarf, wenn er das Programm nur bestimmungsgemäß benutzen möchte. Kommt es nicht zum Abschluss des Lizenzvertrags, so handelt es sich um ein einfaches Zweipersonenverhältnis zwischen dem Nutzer und dem Dienstleister. D.h., dass von vornherein nur der Dienstleister für vertragliche Ansprüche auf Haftung und Gewährleistung in Frage kommt.

Zur bestimmungsgemäßen Benutzung gehört nach dem Urheberrechtsgesetz auch das Erstellen einer Sicherungskopie (§ 69d Abs. 2 UrhG), die Fehlerberichtigung (§ 69d Abs. 1 UrhG) sowie die Dekompilierung zur Herstellung der Interoperabilität mit anderen Programmen (§ 69e UrhG). Erst wenn mehr Programmkopien als nur eine Sicherungskopie erstellt und weitergegeben werden oder wenn das Programm jenseits der Fehlerberichtigung verändert wird, ist der Abschluss eines Lizenzvertrags erforderlich. Ob die OSS-Lizenzen für die Behörde im Einzelfall von Bedeutung sind, hängt also von der Art der Nutzung des Programms ab. Wenn eine Behörde zum Beispiel mit einer einzelnen Linux-Distribution eine Vielzahl von Arbeitsplätzen ausrüstet, so wird man bei Anwendung des deutschen Urheberrechts von einer Vervielfältigung auszugehen haben, so dass eine OSS-Lizenz abgeschlossen werden muss. Gleiches gilt für die Weitergabe von Programmkopien an andere Behörden, die öffentliche Zugänglichmachung in Datennetzen und die Weiterentwicklung.

Tab. 76: Relevanz der OSS-Lizenzen für Nutzer

Art der Nutzung	Relevanz der OSS-Lizenzen
Ablaufenlassen	nein
Erstellen Sicherungskopie	nein
Fehlerberichtigung	nein
Dekompilieren für Interoperabilität	nein

Art der Nutzung	Relevanz der OSS-Lizenzen
Vervielfältigung	ja
Veränderung	ja
Verbreitung	ja
Öffentlich Zugänglichmachen	ja

4.4.2 Ablösende Migration: Vertrag mit Zwischenhändler

Für das Verhältnis zwischen der Behörde als Nutzer und demjenigen, von dem sie das Programm erhalten hat, sind unterschiedliche Fallgestaltungen denkbar, in denen unterschiedliche Gesetzesregelungen anzuwenden sind. Dies ist vor allem für die Haftung und Gewährleistung von Bedeutung.

In der einfachsten Konstellation erwirbt die Behörde eine Standard-OSS, ohne weitere Leistung ihres Vertragspartners in Anspruch zu nehmen. Ist ein Entgelt zu zahlen, so finden die Vorschriften über den Kaufvertrag Anwendung. Wird die Software dagegen kostenlos abgegeben, so sind die Vorschriften des Schenkungsrechts maßgeblich. Hierher gehört zum Beispiel der kostenlose Download eines Programms von der Website eines Distributors. Entsprechende Angebote können regelmäßig auch von Behörden wahrgenommen werden.

Wird das Programm dagegen im Rahmen einer Gesamtleistung überlassen, so ist die rechtliche Beurteilung schwieriger. Als Grundregel kann hier festgehalten werden, dass eine künstliche Aufspaltung der einzelnen Teilleistungen in Einzelverträge zum Nachteil der Behörde vertragsrechtlich nicht möglich ist. Wird etwa Hardware mit vorinstallierter OSS vertrieben und wird hierbei auch für die Software ein Entgelt verlangt, so handelt es sich um einen einheitlichen Kaufvertrag. Wird dagegen die Software verschenkt, während die Hardware verkauft wird, so sind die Vorschriften von Kauf- und Schenkungsvertrag zu kombinieren. Entsprechendes gilt für die Einbindung der Softwareüberlassung in ein umfassendes Dienstleistungsangebot. Hier wird man die gesetzlichen Vorschriften zum Dienstleistungsvertrag mit denjenigen des Kauf- oder Schenkungsvertrags kombinieren müssen, je nach dem, ob für das Programm ein Entgelt zu leisten ist oder nicht.

Die Entwicklung neuer Software kann hier nur im Überblick erläutert werden. Die Behandlung des Vertrags über die Entwicklung von Individualsoftware ist im juristischen Schrifttum gegenwärtig stark umstritten. Bis zu einer Klärung durch die Gerichte wird man damit leben müssen, dass manche von der Anwendung des Werkvertragsrechts ausgehen, während andere das Kaufvertragsrecht für maßgeblich halten. Soll bestehende OSS im Auftrag einer Behörde weiterentwickelt werden, so hängt die rechtliche Beurteilung davon ab, ob die vorbestehenden Programmbestandteile bereits bei der Behörde vorhanden waren oder erst vom Auftragnehmer geliefert wurden. Im ersten Fall ist von einem isolierten Werk- bzw. Kaufvertrag über die hinzugefügten Programmbestandteile auszugehen, dagegen ist im zweiten Fall ein einheitlicher Vertrag anzunehmen.

Bei Verwendung der EVB-IT bzw. BVB[1] ist im Einzelnen zu prüfen, ob die Vertragsbestimmungen im Einklang mit den jeweils maßgeblichen OSS-Lizenzen stehen. Eine unveränderte Heranziehung der Standardverträge kann mitunter problematisch sein. Dies soll an zwei Beispielen näher dargestellt werden:

Die EVB-IT Überlassung Typ A und Typ B können bei der Beschaffung von Standard-Open Source Software von einem Zwischenhändler nicht ohne weiteres benutzt werden. Die genannten Vertragswerke sehen eine Rechtseinräumung durch den Auftragnehmer (d.h. den Zwischenhändler) vor; dies kommt beim Erwerb von OSS in aller Regel aber nicht in Frage, da der Zwischenhändler keine entsprechenden Rechte innehat und deswegen auch keine Nutzungsrechte einräumen kann. Die Klauseln über die Nutzungsrechtseinräumung müssten hier also gestrichen werden, um das Formular benutzen zu können.

Die BVB-Erstellung kann ohne Veränderung nur verwendet werden, wenn die Behörde eine völlige Neuentwicklung in Auftrag gibt. Für Aufträge über die Weiterentwicklung von bereits bestehender GPL-Software bedarf das Vertragsmuster dagegen gewisser Veränderungen: Es enthält Klauseln, die nicht mit den Vorgaben der GPL vereinbar sind und die dementsprechend gestrichen oder verändert werden müssten[2].

Der Vertrag zwischen Behörde und Dienstleister richtet sich immer dann nach deutschem Recht, wenn sowohl die Behörde als auch der Dienstleister ihren Sitz in Deutschland haben. In diesem Fall richtet sich sowohl die Wirksamkeit der Verträge als auch die vertragliche Haftung und Gewährleistung nach deutschem Recht. Hat der Dienstleister dagegen seinen Sitz im Ausland, so kann ausländisches Recht maßgeblich sein, es sei denn die Behörde vereinbart in dem Vertrag eine Rechtswahl zugunsten des deutschen Rechts. Hierzu ist dringend zu raten. Da für dieses Vertragsverhältnis die OSS-Lizenzen ohne Bedeutung sind, sind die Parteien in der Vertragsgestaltung im Rahmen der gesetzlichen Möglichkeiten frei.

Tab. 50: Vertragsverhältnisse Nutzer-Zwischenhändler

Art der Leistung des Zwischenhändlers	Vertragstyp
Standard-OSS gegen Entgelt	Kaufvertrag
Standard-OSS kostenlos	Schenkungsvertrag
Kombination Hardware und Standardsoftware: beide gegen Entgelt oder Software kostenlos	Einheitlicher Kaufvertrag
Neuentwicklung von OSS	Werkvertrag (andere Auffassung: Kauf)
Fortentwicklung von OSS	Werkvertrag (andere Auffassung: Kauf)

1 Abrufbar unter http:///www.kbst.bund.de/.

2 Dies gilt insbesondere für die Nutzungsrechtsklausel in Ziffer 6 und die unklare Regelung im Hinblick auf die Offenlegung der Quelltexte gegenüber dem Auftraggeber.

4.4.3 Ablösende Migration: Vertrag mit Rechtsinhabern

Möchte die Behörde die Software in einer Weise nutzen, die über eine "bestimmungsgemäße Benutzung" im Sinne des § 69d UrhG hinausgeht, so bedarf sie hierfür der Zustimmung der Rechtsinhaber. Nur in diesem Fall sind die OSS-Lizenzen überhaupt von praktischer Bedeutung. Damit die OSS-Lizenzen rechtliche Geltung erlangen, bedarf es eines entsprechenden Vertragsschlusses, also eines Angebots und der Annahme dieses Angebots. Rechtstechnisch handelt es sich bei einem Programm, welches einer OSS-Lizenz unterstellt worden ist, um ein Angebot an jedermann auf Abschluss eines Lizenzvertrags mit dem Inhalt der jeweiligen Lizenzbedingungen (GPL o.ä.). Wer einen solchen Lizenzvertrag abschließen möchte, kann seine Annahme dadurch erklären, dass er eine Handlung vornimmt, die nach der Lizenz jedem Lizenznehmer gestattet ist, also eine Vervielfältigung, eine Verbreitung oder eine Veränderung des Programms. Der Lizenzvertrag kommt durch die bloße Vornahme dieser Handlung automatisch zustande, es bedarf keines direkten Kontakts mit den Rechtsinhabern per E-mail oder ähnliches. Das deutsche Vertragsrecht erkennt einen Vertragsschluss an, bei dem der Anbietende auf den Zugang der Annahme verzichtet[1]. Einem solchen Vertragsschluss steht auch nicht entgegen, dass die üblicherweise verwandten OSS-Lizenzen ausschließlich in englischer Sprache rechtlich bindend sind. Dies gilt nach der Entscheidung des Landgerichts München vom 19.05.2004[2] und der weit überwiegenden Zahl der juristischen Fachautoren jedenfalls dann, wenn ein Unternehmen oder eine Behörde Lizenznehmer werden möchte.

Ein praktisches Problem besteht bei OSS darin, dass die Rechtsinhaberschaft oftmals sehr unübersichtlich ist. Dies gilt für alle diejenigen OSS-Programme, die in einer weit verstreuten Entwicklergemeinschaft geschrieben worden sind. Linux ist hier das exemplarische Beispiel. Es haben hunderte Programmierer, die weltweit verstreut sind, an dem Programm mitgearbeitet. Manche haben als freie Entwickler mitgewirkt und sind Inhaber der Urheberrechte an den Teilen, die sie beigesteuert haben. Andere haben als angestellte Programmierer gearbeitet. Hier sind in der Regel die Arbeitgeber Inhaber der wichtigsten Rechte[3]. Wieder andere haben ihre Rechte auf Organisationen, wie die Free Software Foundation Europe übertragen, welche die Rechte treuhänderisch wahrnehmen.[4] Wer heute eine Lizenz an Linux erwirbt, schließt mit allen diesen Rechtsinhabern gleichzeitig identische Verträge mit dem Inhalt der GPL/LGPL ab. Dadurch sind die rechtlichen Verhältnisse äußerst kompliziert.

---

1 Vgl. § 151 BGB.

2 Vgl. Landgericht München, Urteil vom 19.05.2004, siehe oben Fn.

3 Vgl. § 69b UrhG.

4 Vgl. das entsprechende Projekt der Free Software Foundation Europe unter http://www.fsfeurope.org/projects/fla/fla.de.html

Dieses Problem tritt nicht bei allen OSS-Programmen auf. Einige der am weitesten verbreiteten Programme wurden in Unternehmen entwickelt und erst später nach den Bedingungen einer OSS-Lizenz freigegeben. Dies trifft z.B. für Open Office zu. Hier liegen die Rechte an den wichtigsten Bestandteilen bei einem Unternehmen, dementsprechend sind die Vertragsverhältnisse einfacher.

Im Hinblick auf das anwendbare Recht muss für die Lizenzverträge differenziert werden. Alle (Vor-)Fragen des Urheber- und Patentrechts, also insbesondere ob entsprechende Rechte bestehen, wer Inhaber des Rechts ist, unter welchen Voraussetzungen Lizenzen eingeräumt werden können, richten sich nach deutschem Recht, sofern die jeweils in Frage stehende Nutzungshandlung (Vervielfältigung, Verbreitung, Veränderung etc.) in Deutschland stattfindet. Für die vertragsrechtlichen Fragen, insbesondere die Voraussetzungen des Vertragsschlusses, die Auslegung der Lizenzen, die vertragliche Haftung und Gewährleistung, findet dagegen deutsches Recht nur dann Anwendung, wenn die Rechtsinhaber ihren Sitz oder gewöhnlichen Aufenthalt in Deutschland haben. Oft werden die Rechtsinhaber aber nicht in Deutschland sitzen, sondern in den USA oder einem anderen Land. Dann findet das jeweilige ausländische Recht auf die genannten Fragen Anwendung. Hier kann zumeist auch eine Rechtswahlklausel nichtweiter helfen. Wenn die Rechte an einem Programm bei einer weltweiten Entwicklergemeinschaft liegen, dürfte es kaum möglich sein, Sondervereinbarungen jenseits der standardisierten OSS-Lizenzen zu erreichen. Liegen die Rechte hingegen bei einem Unternehmen oder einer kleineren Community, ist es ggf. möglich, eine Sondervereinbarung zum anwendbaren Recht zu erreichen.[1]

Tab. 51: Anwendbares Recht

	Rechtsfrage	Anwendbares Recht
Vertrag mit Zwischenhändler	Zustandekommen des Vertrags	Recht des Landes, in dem Zwischenhändler seinen Sitz hat
	Auslegung	
	Rechtsfolgen bei Nichtleistung	
	Vertragliche Haftung und Gewährleistung	
Vertrag mit Rechtsinhabern	Zustandekommen des Vertrags	Recht des Landes, in dem der Rechtsinhaber seinen Sitz hat
	Auslegung	
	Rechtsfolgen bei entgegenstehenden Rechten Dritter	
	Schutzfähigkeit des Werks bzw. der Erfindung	Recht des Landes, für das Schutz beansprucht wird (= in dem urheber- bzw. patentrechtlich relevante Handlun-
	Bestehen von Urheber- und	

[1] Beispielsweise MySQL bietet zwei Lizenzmöglichkeiten an. Nutzer können die Software entweder nach den Bestimmungen der GPL nutzen oder eine "Commercial license" erwerben, vgl. http://www.mysql.com/company/legal/licensing. Hier sind dann ggf. auch Rechtswahlklauseln möglich.

	Rechtsfrage	Anwendbares Recht
	Patentrechten	gen stattgefunden haben)
	Rechtsinhaberschaft	
	Übertragbarkeit	
	Lizenzierbarkeit	

4.4.4 Vergleich fortführender und ablösender Migration

Auf den ersten Blick erscheinen die Vertragsverhältnisse bei einer fortführenden Migration als einfacher und dadurch vorteilhafter. Dies trifft aber nur in bestimmten Fallkonstellationen zu, in anderen Sachverhaltsgestaltungen sind die Vertragsverhältnisse proprietärer Software mit Nachteilen gegenüber OSS verbunden. Es ist deswegen notwendig zu differenzieren.

Bei beiden Migrationswegen sind Konstellationen möglich, in denen die Behörde nur einen Vertrag mit einem Vertragspartner für die Softwareüberlassung abschließen muss. In bestimmten Fällen wird der Inhaber der Rechte an einer proprietären Software diese der Behörde auch direkt überlassen. In diesem Fall handelt es sich um einen Vertrag zwischen zwei (juristischen) Personen, in dem sowohl die Überlassung der Bits und Bytes als auch die Einräumung von Nutzungsrechten geregelt sind.[1] Dies hat den Vorteil der Übersichtlichkeit und Einfachheit. Es ist allerdings darauf hinzuweisen, dass es auch bei OSS in vielen Fällen mit einem solchen Zweipersonenverhältnis sein Bewenden hat. Solange die Behörde die Software nur bestimmungsgemäß benutzt, werden keine Lizenzverträge mit den Rechtsinhabern abgeschlossen.

Handelt es sich dagegen um ein Dreipersonenverhältnis zwischen Nutzer, Rechtsinhaber und Zwischenhändler, so sind die rechtlichen Probleme bei proprietärer Software größer. Proprietäre Software wird nicht immer im Zweipersonenverhältnis überlassen. Gerade kleinere Behörden werden Software oft nicht direkt beim Rechtsinhaber erwerben, sondern im Einzelhandel oder bei sonstigen lokalen Dienstleistern. In diesem Fall kann es ebenfalls zu Dreipersonenverhältnissen kommen, und zwar dann, wenn der Rechtsinhaber den Abschluss eines Lizenzvertrags wünscht. Microsoft und andere Anbieter proprietärer Programme verlangen regelmäßig vom Erwerber einer Standardsoftware, dass dieser neben dem Kaufvertrag mit dem Einzelhändler ein zusätzliches "End User License Agreement" (EULA) mit dem Rechtsinhaber direkt abschließt. Dieser Lizenzvertrag soll typischerweise durch das Anwählen eines "o.k."-Buttons oder die Benutzung der Software zustande kommen.[2] Die Wirksamkeit entsprechender Verträ-

[1] Vgl. z.B. die hierauf zugeschnittenen EVB-IT Überlassung Typ A, abrufbar unter http//www.kbst.bund.de/.

[2] Vgl. zu den heute üblichen Vertragsgestaltungen in diesem Bereich exemplarisch Jochen Marly, Softwareüberlassungverträge (4. Aufl. 2003), S. 213 ff. mit zahlreichen Beispielen aus der Vertragspraxis.

ge wird von namhaften Fachautoren mit guten Argumenten verneint.[1] Gerichtsentscheidungen liegen hierzu allerdings nicht vor, es fehlt an entsprechenden Klagen der Rechtsinhaber gegen die Kunden auf Einhaltung der oftmals restriktiven Lizenzverträge.

Demgegenüber ist der Vertrieb von OSS über Einzel- oder Zwischenhändler bzw. Dienstleister weniger problematisch. Solange die Behörde die Software lediglich bestimmungsgemäß benutzt, kommt es überhaupt nicht zum Abschluss eines Lizenzvertrags mit den Rechtsinhabern. Ist aber ein Lizenzvertrag erforderlich, weil die Behörde die Rechte aus der GPL oder einer anderen OSS-Lizenz wahrnehmen möchte, so wirft das dadurch entstehende Dreipersonenverhältnis weniger rechtliche Probleme auf als im Fall der EULAs. Während die OSS-Lizenz dem Nutzer Rechte einräumt, die über die bereits nach dem Gesetz erlaubte bestimmungsgemäße Benutzung hinausgehen, beschränken EULAs diese Rechte, indem Weitergabeverbote, CPU-Klauseln und Ähnliches zu Lasten des Nutzers vereinbart werden. Warum aber sollte ein Nutzer, der durch den Erwerb einer rechtmäßig in Verkehr gebrachten Programmkopie bereits das Recht zur bestimmungsgemäßen Benutzung gemäß §§ 69d und § 69e UrhG erworben hat, nachträglich einer Beschränkung dieser Rechte zustimmen wollen? Es ist mehr als fragwürdig, ein Anwählen des "o.k."-Buttons als Zustimmung zu werten, wenn dem Nutzer keine andere Möglichkeit offen steht, die bereits erworbene Software überhaupt verwenden zu können. Diese spezifischen Probleme der EULAs treffen auf OSS-Lizenzen nicht zu.

4.5 Urheberrecht

4.5.1 Ablösende Migration: Zulässigkeit von OSS-Lizenzen nach deutschem Urheberrecht

Sofern es für eine Behörde notwendig ist, eine OSS-Lizenz abzuschließen, stellt sich die Frage nach der urheberrechtlichen Zulässigkeit der in den Lizenzen geregelten Rechte und Pflichten. Dies ist von Bedeutung für die Planungssicherheit im Hinblick auf die erworbenen Rechte und die damit einhergehenden Pflichten.

Will man die Fülle der hierzu erschienenen Fachveröffentlichungen in einem Satz zusammenfassen, so könnte man festhalten, dass die GPL und die anderen weit verbreiteten OSS-Lizenzen im Grundsatz mit dem deutschen Urheberrecht vereinbar sind. Auch das Landgericht München kommt zu dem Ergebnis, dass die zentralen Bestimmungen der GPL (Paragraph 2, 3 und 4) urheberrechtlich unbedenklich sind.[2]

Die bestehenden rechtlichen Bedenken gegen einzelne Klauseln der OSS-Lizenzen haben bislang nicht zu gerichtlichen Auseinandersetzungen geführt .

---

1 So im Ergebnis auch Marly, a.a.O., S. 225.

2 Vgl. Landgericht München, Urteil vom 19.05.2004, oben Fn.

Zu nennen sind hier erstens die Urheberpersönlichkeitsrechte der Softwareentwickler.[1] Gemäß §§ 69a Abs. 4, 14 UrhG kann sich der Urheber eines Computerprogramms gegen Entstellungen oder Beeinträchtigungen seines Werkes zur Wehr setzen, sofern diese geeignet sind, seine persönlichen oder geistigen Interessen zu verletzten. Dieses Verbotsrecht steht in Konflikt zur Veränderungsfreiheit, welche die OSS-Lizenzen jedem Nutzer einräumt. Bei Veränderungen eines Computerprogramms dürften Verletzungen des Urheberpersönlichkeitsrechts allerdings nur in Ausnahmefällen gegeben sein.

Als ein zweites Problem wird oftmals darauf hingewiesen, dass es nach deutschem Urheberrecht wegen § 31 Abs. 4 UrhG nicht möglich ist, für Nutzungsarten Rechte einzuräumen, die zum Zeitpunkt des Vertragsschlusses noch nicht bekannt gewesen sind. Stellt man auf den Zeitpunkt der ersten Lizenzierung durch den Rechtsinhaber ab, so wäre es etwa für den Linux-Kernel durchaus fraglich, ob auch solche Nutzungsarten umfasst sind, die erst Ende der 90er Jahre in ihrer wirtschaftlichen Bedeutung bekannt geworden sind. Ein gutes Beispiel bietet hier das so genannte Application Service Providing.

Als weiterer Problembereich wird schließlich auf den Erschöpfungsgrundsatz aus § 69c Nr. 3 Satz 2 UrhG verwiesen.[2] Die Frage der Erschöpfung des Verbreitungsrechts ist aus der Sicht der Behörde als Nutzer jedoch irrelevant. Die OSS-Lizenzen verbieten die Weitergabe einer einmal rechtmäßig in den Verkehr gebrachten Programmkopie nicht, auch werden keine Bedingungen an die Weitergabe dieser Programmkopie geknüpft.

4.5.2 Ablösende Migration: Umfang der Rechtseinräumung bei OSS-Lizenzen

Von erheblicher Bedeutung für die Migrationsentscheidung von Behörden ist der Umfang der Rechtseinräumung, den OSS-Lizenzen vorsehen. Ist für eine Behörde eine Nutzung von Software notwendig oder wünschenswert, die über eine bloß bestimmungsgemäße Benutzung hinausgeht, so ist dies bei OSS ohne weiteres möglich. Eine Lizenz entspricht nur dann den Kriterien der Open Source Defintion[3] und der Free Software Definition[4], wenn sie dem Nutzer umfangreiche "Freiheiten" im Umgang mit dem Programm einräumt, insbesondere das Programm in veränderter oder unveränderter Form vervielfältigen und verbreiten zu können.

Rechtstechnisch handelt es sich hierbei um die Einräumung einfacher, urheberrechtlicher Nutzungsrechte gem. § 31 Abs. 2 UrhG. Dieser umfassende Rechtserwerb geht denkbar einfach vonstatten. Wer die Rechte aus den Lizenzen

---

1 Vgl. hierzu exemplarisch Jaeger/Metzger, Open Source Software: Rechtliche Rahmenbedingungen der Freien Software (2002), S. 35 f.;

2 Vgl. insbesondere Spindler (Hrsg.), Rechtsfragen bei Open Source (2004), S. 91 ff.

3 Abrufbar unter http://www.opensource.org/docs/defintion.php.

4 Abrufbar unter http://www.gnu.org/philosophy/free-sw.html.

wahrnehmen möchte, kann dies ohne weiteres tun, solange er auch die Verpflichtungen einhält, die die jeweilige Lizenz mit sich bringt. Die Einräumung der Nutzungsrechte erfolgt kostenfrei.

Einige Autoren weisen darauf hin, dass die Einräumung des Rechts für den unkörperlichen Vertrieb durch die üblichen OSS-Lizenzen, insbesondere das Bereithalten zum Download im Internet, zweifelhaft sei.[1] Die GPL und die BSD Lizenz räumen zwar ausdrücklich das Recht ein, das Programm in körperlicher Form zu verbreiten ("distribute"), erwähnen aber den unkörperlichen Vertrieb nicht ausdrücklich. Verwiesen wird in diesem Zusammenhang auch auf § 31 Abs. 4 UrhG, es sei zu fragen, ab welchem Zeitpunkt der Vertrieb in Datennetzen in seiner wirtschaftlichen Bedeutung bekannt gewesen sei.[2]

Dem ist entgegenzuhalten, dass in der US-amerikanischen Terminologie das Wort "distribute" auch den unkörperlichen Vertrieb umfasst. Oft wird ohnehin für die Auslegung eines der 50 US-amerikanischen Vertragsrechte maßgeblich sein, weil der Lizenzgeber in den USA sitzt. In den Fällen, in denen eine Auslegung nach deutschem Recht vorzunehmen ist, muss aber ebenfalls berücksichtigt werden, dass die heute verwandten OSS-Lizenzen in ihrer Terminologie auf das US-amerikanische Recht Bezug nehmen. Dessen Begriffe sind deswegen auch bei Anwendung des deutschen Rechts zu berücksichtigen.[3] Schließlich ist auf den letzten Absatz von Paragraph 3 GPL hinzuweisen. Dort heißt es: "If distribution of executable or object code is made by offering access to copy from a designated place [...]; mit "designated place" kann in diesem Zusammenhang nur eine Internetadresse gemeint sein, von der das Programm abgerufen werden kann. Dies spricht ebenfalls für eine Einbeziehung des unkörperlichen Vertriebs. Im Hinblick auf § 31 Abs. 4 UrhG kann auf das oben Ausgeführte verwiesen werden (siehe auch 4.5.1). Im Ergebnis ist deswegen davon auszugehen, dass auch der Vertrieb in Datennetzen wie dem Internet gestattet ist.

4.5.3 Ablösende Migration: Entgegenstehende Urheberrechte Dritter

Für einiges Aufsehen hat in den letzten Monaten der Rechtsstreit zwischen SCO und IBM gesorgt.[4] SCO beschuldigt IBM, Bestandteile von Programmen, an denen SCO behauptet die Rechte innezuhaben, ohne die erforderliche Erlaubnis in Linux integriert und damit Geschäftsgeheimnisse verletzt zu haben, ferner sich des unlauteren Wettbewerbs schuldig gemacht und Verträge verletzt zu haben. Mittlerweile sind auch die Urheberrechte an den fraglichen Modulen Gegenstand

---

1 Vgl. insbesondere Spindler, a.a.O., 82.

2 Vgl. insbesondere Spindler, a.a.O., 82.

3 Vgl. Metzger, in: Hilty/Peukert, Interessenausgleich im Urheberrecht (2004), 253, 260 mit weiteren Nachweisen.

4 Vgl. den Text der 06.03.2003 in Salt Lake City erhobenen Klage unter http://www.sco.com/ibmlawsuit/

des Verfahrens.[1] Es soll hier nicht um die Details dieses Rechtsstreits gehen. Dieser dient nur als Illustration der folgenden Frage: Welche Risiken hat eine Behörde zu befürchten, wenn sich im Nachhinein herausstellt, dass an genutzter OSS Rechte Dritter bestehen?

Für die Beantwortung sind zwei Situationen zu unterscheiden. Es macht einen Unterschied, ob die Behörde die Software (1.) vervielfältigt, verbreitet oder verändert oder (2.) ob sie sie nur bestimmungsgemäß benutzt hat.

Im ersten Fall liegt es auf der Hand, dass eine entsprechende Nutzung nur urheberrechtlich zulässig ist, wenn der Rechtsinhaber hierfür die entsprechenden Rechte eingeräumt hat, insbesondere das Programm oder die Programmteile, an denen er die Rechte hält, einer OSS-Lizenz unterstellt hat. Stellt sich im Nachhinein heraus, dass der vermeintliche Lizenzgeber nicht Inhaber der Rechte an dem gesamten Programm ist, so kann der Behörde die weitere Verbreitung des Gesamtprogramms etc. für die Zukunft untersagt werden. Für die Vergangenheit können Schadensersatzforderungen geltend gemacht werden, sofern die Behörde ein Verschulden trifft.[2] Wer urheberrechtlich geschützte Güter nutzt, muss sich über die hierfür erforderlichen Rechte Gewissheit verschaffen, um nicht seine Sorgfaltspflichten zu verletzen. Dabei beziehen sich sowohl Unterlassungs- als auch Schadensersatzansprüche nur auf den Teil des Programms, für den entgegenstehende Rechte Dritter bestehen. Das heißt, die anderen Programmteile, die nicht mit Rechten Dritter belastet sind, dürfen weiter verbreitet werden.

Im zweiten Fall ist die Rechtslage etwas komplizierter. Hier kann es so sein, dass der Zwischenhändler, von dem die Behörde das Programm erhalten hat, dieses nicht vertreiben durfte, da die OSS-Lizenz ihm hierfür nicht die erforderlichen Rechte vermittelt hat. Dies führt dazu, dass sich die Behörde nicht auf § 69d Abs.1 UrhG berufen kann, da ihre Programmkopie nicht rechtmäßig in den Verkehr gelangt ist.

Auf den ersten Blick scheint als Ergebnis festzustehen, dass sie das gesamte Programm nicht mehr benutzen darf; schließlich ist das Programm nicht rechtmäßig in Verkehr gebracht worden. Dieser erste Anschein trügt aber. Es wurde bereits darauf hingewiesen, dass manche OSS-Lizenzen, etwa die BSD-Lizenz, dem Nutzer auch das Recht einräumen, die Software einfach nur zu benutzen, das heißt, bestimmungsgemäß ablaufen zu lassen. Diese Klauseln erlangen Bedeutung, wenn sich der Nutzer nicht auf die gesetzliche Lizenz des § 69d Abs. 1 UrhG berufen kann, weil es hierfür an den Voraussetzungen fehlt. Auch die GPL, welche an sich ja die einfache Benutzung aus ihrem Anwendungsbereich ausklammert, hält für diese Situation ein Hilfsmittel zugunsten der Nutzer bereit. Paragraph 7 verbietet den Vertrieb eines Programms unter der GPL, wenn dieses

---

1 Vgl. den Text der am 25.09.2003 erhobenen Gegenklage, insb. Rz. 119 ff. unter und die Erwiderung seitens SCO vom 24.10.2003, ebenfalls Rz. 119 ff., beide unter http://www.sco.com/ibmlawsuit/

2 Zur Berechnung des Schadensersatzes vergleiche Schricker-Wild, Urheberrecht (2. Aufl. 1999), § 97, Rz. 56 ff.

durch ein Gerichtsurteil untersagt worden ist. In diesem Fall sollen gemäß Paragraph 4 GPL aber nur die Rechte des Lizenznehmers entfallen, Rechtspositionen Dritter, die vom Lizenznehmer Programmkopien erhalten haben, sollen hingegen fortbestehen, solange der Dritte die Bestimmungen der Lizenz einhält.

Freilich kann das nur für die Programmteile gelten, an denen die Lizenzgeber auch tatsächlich die Rechte innehaben. Diese Programmteile dürfen weiter benutzt werden. Für die Teile des Programms, auf denen Rechte Dritter lasten, können gegen die Behörde unter den oben genannten Voraussetzungen Unterlassungs- und Schadensersatzansprüche geltend gemacht werden.

Man stelle sich etwa folgenden Beispielfall vor. Ein Entwicklungsprojekt stellt eine umfangreiche Datenbanksoftware unter die GPL und verbreitet das Programm. Die Behörde A lädt sich die Software herunter, modifiziert sie für die besonderen Anforderungen von Behörden und vertreibt sie an die Behörden B, C und D. Stellt sich im Nachhinein heraus, dass einer der Programmierer des Projekts unsauber gearbeitet und einzelne Teile des Programms in urheberrechtlich unzulässiger Weise übernommen hat, so kann der Inhaber der Rechte an diesen Programmteilen grundsätzlich nur die Verbreitung und Benutzung dieser Programmteile untersagen. Daraus folgt, dass A die Verbreitung dieser Programmteile untersagt werden kann, nicht aber die Verbreitung der sonstigen Programmteile. Lässt sich der problematische Bestandteil ersetzen, so kann das auf diese Weise bereinigte Gesamtprogramm weiter verbreitet werden. B, C, und D kann ebenfalls nur die Benutzung der Programmteile untersagt werden, an denen Rechte Dritter bestehen. Können diese ersetzt oder gelöscht werden, etwa weil der jeweilige Benutzer diese Programmbestandteile gar nicht benötigt, so darf das Restprogramm weiterhin benutzt werden.

Wo sich eine Behörde aufgrund entgegenstehender Rechte Dritter entsprechenden Ansprüchen ausgesetzt sieht, ist jeweils zu fragen, ob sie ihrerseits Ansprüche gegen ihre Vertragspartner geltend machen kann. Dies ist eine Frage der Gewährleistung (siehe auch 4.7).

4.5.4 Vergleich fortführender und ablösender Migration

Im Hinblick auf die urheberrechtlichen Fragestellungen ergeben sich aus der Sicht einer Behörde als Nutzer eine Reihe relevanter Unterschiede zwischen einer fortführenden und einer ablösenden Migration.

Hierbei ist zunächst festzustellen, dass die unter 4.5.1 thematisierten rechtlichen Probleme der OSS-Lizenzen, soweit diese praktisch überhaupt relevant werden, auch bei proprietären Lizenzmodellen auftreten können. Es handelt sich hier nicht um spezifische Rechtsfragen der OSS.

Erhebliche Vorteile von OSS gegenüber proprietären Konkurrenzprodukten sind im Hinblick auf den Umfang der Rechtseinräumung festzuhalten. OSS-Lizenzen erlauben den Behörden eine denkbar umfassende Nutzung der Programme, der Erwerb dieser Rechte ist kostenfrei und in der Abwicklung denkbar einfach. Demgegenüber gestatten proprietäre Softwarelizenzen in der Regel nur eine be-

stimmungsgemäße Benutzung der Software. Hinzu kommen die mannigfaltigen Verwendungs- und Weitergabebeschränkungen in üblichen Softwarelizenzen, die den ohnehin geringen Spielraum der Nutzer zusätzlich einengen. Benötigt der Nutzer zusätzliche Rechte, etwa weil er die Software verändern oder in weiterem Umfang einsetzen möchte, so muss er in aller Regel eine erhöhte Lizenzgebühr hinnehmen. Entsprechende Vertragsgestaltungen sind üblich und oft auch rechtlich wirksam, etwa die Erhöhung der Lizenzgebühren bei der Verwendung von Software auf einer leistungsstärkeren Hardware.[1]

Für die unter 4.5.3 genannten Unterlassungs- und Schadensersatzansprüche, können sich dagegen gewisse Vorteile für eine fortführende Migration ergeben. Es ist zwar festzuhalten, dass eine Behörde als Softwarenutzer nie absolut sicher sein kann, dass der weiteren Nutzung eines Programms keine Rechte Dritter entgegenstehen. Entsprechende Probleme sind allerdings umso weniger wahrscheinlich, je seriöser und transparenter die Herkunft eines Programms ist. OSS wird hier mitunter mit Nachteilen behaftet sein, wenn die Herkunft eines Programms nicht oder nur mit erheblichem Aufwand geklärt werden kann, während das konkurrierende proprietäre Produkt eindeutig zuzuordnen ist. Hier zeigen sich die Nachteile der dezentralen Entwicklung im Rahmen von mitunter weltweit verstreuten Communities. Freilich ist auch die umgekehrte Situation denkbar, in der die Herkunft eines proprietären Programms weniger transparent ist als diejenige der konkurrierenden OSS. Man muss hier also die jeweils in Konkurrenz stehenden Produkte im Einzelfall vergleichen. Zu berücksichtigen ist bei der Evaluierung der fortführenden Migration durchaus auch, welche diesbezüglichen Erfahrungen die Behörde mit den jeweiligen Anbietern in der Vergangenheit gemacht hat.

Tab. 52: Urheberrechtliche Fragen

	Ablösende Migration	Fortführende Migration
Urheberrechtliche Zulässigkeit einzelner Lizenzklauseln	Aus der Sicht der Nutzer keine praktisch relevanten Rechtsprobleme	Bei entsprechender Vertragsgestaltung keine praktisch relevanten Rechtsprobleme
Umfang der Rechtseinräumung	Sehr weitgehend	Oft restriktiv
Risiko entgegenstehender Rechte Dritter	Erhöht bei unklarer Herkunft	Geringer bei seriösen Anbietern

[1] Vgl. hierzu Bundesgerichtshof, Urteil vom 24.10.2002, Neue Juristische Wochenschrift 2003, 2014.

4.6 Patentrecht

4.6.1 Allgemeines

Die Fragen des Patentrechts haben in der Diskussion der letzten Monate um die Rechtssicherheit von OSS breiten Raum eingenommen. Die dabei in erster Linie diskutierten rechtspolitischen Fragen sollen hier ausdrücklich ausgeklammert werden. Der Migrationsleitfaden konzentriert sich auf den juristischen Status quo aus der Perspektive einer Behörde als Nutzer.

Es ist darauf hinzuweisen, dass allein das europäische Patentamt seit 1993 über 30.000 Patente für programmbezogene Erfindungen in allen Technikbereichen erteilt hat, zu denen auch Erfindungen z.B. im Automobilbau, im Maschinenbau und in der Mess- und Regeltechnik gehören, weil bei ihnen Computerprogramme eingesetzt werden. Hinzu kommen die vom Deutschen Patent- und Markenamt in diesem Bereich erteilten Patente. Dadurch ist es bereits heute möglich, ein realistisches Bild von den rechtlichen Problemen zu gewinnen, welche sich für die Nutzer von OSS durch entsprechende Patente ergeben können, unabhängig von der im Juli 2005 vorerst gescheiterten europäische "Richtlinie über die Patentierbarkeit computerimplementierter Erfindungen".[1] Es liegt allerdings in der Natur der Sache, dass die im Folgenden dargestellten rechtlichen Probleme mit einer wachsenden Zahl von Patenten in zunehmendem Maße auftreten dürften. Ein erstes Beispiel für ein Migrationsprojekt eines öffentlichen Trägers, welches wegen patentrechtlicher Fragestellungen kurzfristig gestoppt worden ist, bietet das "Limux"-Projekt der Stadt München. Das von der Stadt München in Auftrag gegebene Kurzgutachten ist zu dem Ergebnis gekommen, dass "das Risiko einer Verstrickung der Stadt München in einen Patentverletzungsprozess nach der bestehenden Rechtslage als gering einzustufen" sei.[2] Die Stadt hat das Projekt daraufhin fortgesetzt. Patentrechtliche Verletzungsverfahren gegen Nutzer von OSS wegen dieser Nutzung sind bisher nicht bekannt geworden.

4.6.2 Ablösende Migration: Entgegenstehende Patentrechte Dritter

In der Praxis können allerdings Rechtsprobleme auftreten, wenn Dritte Inhaber von Patenten sind, die durch die Nutzung von Software verletzt werden.

Ob eine Patentverletzung vorliegt, ist gemäß § 9 PatG zu bestimmen. Man wird sowohl bei einem so genannten Erzeugnispatent gemäß § 9 Nr. 1 PatG (Verbindung von Hard- und Software; programmgesteuerte Maschinen etc.) als auch bei einem Verfahrenspatent gemäß § 9 Nr. 2 PatG (in Software umgesetzte Lehren zum technischen Handeln, z.B. ein programmgesteuertes Messverfahren) davon

---

1 Vgl. zu den Entwürfen der Europäischen Kommission, des Rats und des Europäischen Parlaments im Einzelnen Metzger, Softwarepatente im künftigen europäischen Patentrecht, Computer und Recht 2003, 313 und Metzger, EP: Eindämmung der Softwarepatente verabschiedet, Computer und Recht 2003, 871.

2 Vgl. das Kurzgutachten von Sedlmaier/Gigerich vom 10.09.2004, abrufbar unter http://www.jurpc.de/aufsatz/20050010.htm

auszugehen haben, dass bereits die bloße bestimmungsgemäße Benutzung einer geschützten Software eine Verletzung dieses Patents darstellen kann.

Für das Erzeugnispatent kann es sich bei der Benutzung eines Programms um ein "Gebrauchen" im Sinne von § 9 Nr. 1 PatG handeln. Wenn etwa in einer Behörde eine patentrechtlich geschützte Maschine benutzt wird, so liegt eine Patentverletzung vor. Einschränkungen sind hier nur denkbar, wenn lediglich ein Teil der von der Behörde genutzten Vorrichtung patentrechtlich geschützt ist. Hier kommt es darauf an, ob der geschützte Teil für das Ganze wesentlich ist. Bei einem Verfahrenspatent kann die bloße Benutzung von Software eine "Anwendung" des geschützten Verfahrens im Sinne von § 9 Nr. 2 PatG und damit eine Patentverletzung darstellen.

Als Patentverletzung sind in beiden Fällen auch der Vertrieb des Programms anzusehen ("Inverkehrbringen" oder "Anbieten").

Liegt eine Patentverletzung vor, so können gegen die Behörde Unterlassungs- und Schadensersatzansprüche geltend gemacht werden. Schadensersatz ist auch im Patentrecht nur unter der Voraussetzung zu leisten, dass die Behörde ein Verschulden trifft, wobei leichte Fahrlässigkeit ausreichen kann. Die Gerichte legen gerade bei Unternehmen hierbei einen strengen Maßstab an. Es wird im Grundsatz erwartet, dass man sich über bestehende Schutzrechte informiert. Gewisse Milderungen sind allerdings in den Fällen möglich, in denen ein Unternehmen das Programm wie ein Endabnehmer nutzt, ohne genauere Fachkenntnis zu haben.[1] Diese Grundsätze wird man auch bei Behörden anzuwenden haben.

Auch bei entgegenstehenden Patentrechten Dritter bleibt stets zu fragen, welche Ansprüche die Behörde ihrerseits gegen die eigenen Lieferanten geltend machen kann. Dies ist eine Frage der vertraglichen Gewährleistung.

4.6.3 Vergleich fortführender und ablösender Migration

Die oben ausgeführten Rechtsprobleme, die sich bei der Nutzung von OSS aufgrund entgegenstehender Rechte Dritter ergeben können, sind keineswegs spezifisch für diese Entwicklungs- und Vertriebsform. Entsprechende Probleme können genauso bei proprietären Konkurrenzprodukten auftreten.

Im Hinblick auf patentrechtliche Ansprüche kann auch nicht für eine fortführende Migration auf das Argument der größeren Transparenz der Herkunft der einzelnen Softwarebestandteile verwiesen werden. Auch wenn im Einzelnen dokumentiert ist, wer welche Partie eines Programms geschrieben hat und dass die entsprechenden Rechte erworben worden sind, so kann daraus nicht gefolgert werden, inwieweit Patente Dritter berührt werden. Da das Patent die zugrunde liegenden technischen Lösungen schützt und nicht die konkrete Form der Programmierung, genügt es mit Blick auf etwaige Patentrechte nicht, alle Rechte der

[1] Vgl. Kraßer, Patenrecht (5. Aufl. 2004), S. 876.

jeweiligen Programmierer erworben zu haben. In patentrechtlicher Hinsicht ergeben sich deshalb für beide Migrationswege im Grundsatz die gleichen rechtlichen Risiken.

4.7 Haftung und Gewährleistung

4.7.1 Allgemeines

Einer der wesentlichen Punkte in der Bewertung der unterschiedlichen Risiken ablösender und fortführender Migration ist die Frage nach dem Maßstab der jeweiligen Haftung und Gewährleistung. Unter Gewährleistung versteht man das Einstehenmüssen für die Vertragsgemäßheit des Programms. Der Begriff der Haftung beschreibt zunächst das vertragliche Einstehenmüssen für Schäden, die sich beim Vertragspartner an sonstigen Rechtsgütern ergeben, etwa Schäden an Hardware oder anderer Software (vertragliche Haftung). Mit Haftung bezeichnet man darüber hinaus auch jedes sonstige außervertragliche Einstehenmüssen für Schäden (außervertragliche Haftung).

Die Haftung und Gewährleistung kann, abhängig von der Ausgestaltung der jeweiligen vertraglichen Beziehungen, unterschiedlichen gesetzlichen Maßstäben unterliegen. So gelten insbesondere bei unentgeltlichen Verträgen vielfach weit reichende Gewährleistungs- und Haftungserleichterungen. Von den gesetzlichen Regelungen können die Vertragsparteien innerhalb bestimmter gesetzlicher Grenzen abweichen und einen schärferen oder milderen Haftungs- und Gewährleistungsmaßstab vertraglich vereinbaren. Behörden sollten darauf bedacht sein, dass die Haftung und Gewährleistung nicht zu ihrem Nachteil ausgeschlossen wird. Werden diese Vereinbarungen nicht wirksam getroffen, etwa weil man sich außerhalb des gesetzlich zulässigen Rahmens befindet, gilt wiederum der gesetzliche Haftungsmaßstab.

Für die Behörde kommen bei der ablösenden Migration unterschiedliche vertragliche Haftungs- und Gewährleistungsschulder in Betracht. Einerseits können Ansprüche gegenüber dem Distributor oder sonstigen Lieferanten der Software bestehen. Andererseits können dort, wo die Behörde eine Open Source Lizenz erworben hat, um die Software zu verändern, zu vervielfältigen und weiterzugeben, Ansprüche auch gegenüber den jeweiligen Lizenzgebern bestehen. Auch bei der außervertraglichen Haftung kann es unterschiedliche Anspruchsgegner geben.

4.7.2 Ablösende Migration: Vertragliche Haftung und Gewährleistung bei Überlassungsverträgen

Verträge über die Überlassung von Open Source Software von einem Zwischenhändler an die Behörde sind regelmäßig als Kauf oder als Schenkung einzuordnen, abhängig davon, ob die Parteien die Überlassung gegen (Einmal-) Entgelt oder aber die unentgeltliche Überlassung verabreden. Ein entgeltlicher Erwerb kann dabei insbesondere auch deshalb interessant sein, da der Lieferant bei einer entgeltlichen Überlassung in größerem Umfang Gewährleistungs- und Haf-

tungsrisiken übernehmen muss. Das Risiko einer ablösenden Migration wird hierdurch unter Umständen besser kalkulierbar.

Ist Kaufrecht anwendbar, hat die Behörde einen Anspruch darauf, dass der Zwischenhändler die OSS frei von Sach- und Rechtsmängeln verschafft. Der Zwischenhändler muss dafür einstehen, dass der Vertragsgegenstand die vertraglich vereinbarte oder vorauszusetzende Beschaffenheit aufweist und dass keine Rechte Dritter, insbesondere Urheber- und Patentrechte, an dem Vertragsgegenstand bestehen, die die bestimmungsgemäße Benutzung behindern.

Liegen Mängel vor, so kann die Behörde in erster Linie Nacherfüllung verlangen. Schlägt diese Nacherfüllung fehl, dann hat der Käufer die Auswahl unter mehreren Ansprüchen. Er kann vom Vertrag zurücktreten (§§ 440, 323 BGB). Als Alternative steht dem Erwerber das Recht zu, am Vertrag zwar festzuhalten, den Kaufpreis aber zu mindern (§ 441 BGB). Schließlich hat der Käufer auch einen Anspruch auf Schadensersatz auf Grundlage der §§ 280, 440 BGB, wenn der Zwischenhändler – was gesetzlich vermutet wird – den Schaden zu vertreten hat. Zu vertreten hat der Schuldner dabei regelmäßig auch leichte Fahrlässigkeit.

Auch für Schäden an sonstigen Rechtsgütern der Behörde, insbesondere Hardware oder andere Software, hat der Zwischenhändler grundsätzlich zu haften. Die Behörde kann in diesem Fall Ersatz ihres Schadens verlangen; Anspruchsgrundlage ist § 280 BGB. Voraussetzung ist wiederum, dass der Zwischenhändler den Schaden zu vertreten hat. Ein Verschulden wird aber auch hier grundsätzlich vermutet; es ist Aufgabe des Verkäufers, sich zu entlasten.

Von dieser gesetzlichen Verteilung des Haftungs- und Gewährleistungsrisikos können die Parteien innerhalb bestimmter Grenzen abweichen. Zwischenhändler versuchen oftmals unter Verweis auf die Usancen der Open Source Entwickler, eine für sie günstigere vertragliche Regelung durchzusetzen und die Haftung und Gewährleistung weitestgehend auszuschließen. Entsprechende Ausschlussklauseln sind aber in aller Regel nicht gerechtfertigt, da die Zwischenhändler die Software entgeltlich weitergeben. Behörden sollten sich hier keinesfalls auf einen Ausschluss ihrer Ansprüche einlassen, sondern auf der Beibehaltung der gesetzlichen Standards bestehen. Im Übrigen ist zugunsten der Behörde zu beachten, dass gerade in Standardverträgen ("Allgemeine Geschäftsbedingungen") Haftungs- und Gewährleistungsbeschränkungen nur begrenzt vereinbart werden können. Ein vollständiger Ausschluss der Haftung und Gewährleistung, wie er sich im Kleingedruckten mancher GNU/Linux-Standarddistribution findet, ist deswegen zumeist unwirksam. Hierauf sollten sich Behörden aber nicht verlassen, sondern von vornherein darauf dringen, dass eine sinnvolle vertragliche Lösung gefunden wird. Die Regelungen der EVB-IT Überlassung TYP A und B zur Ge-

währleistung und Haftung[1] sind grundsätzlich auch beim Erwerb von Standard-Open Source Software geeignet[2].

Hat sich die Behörde die Software kostenlos verschafft, ist auf den Vertrag in der Regel Schenkungsrecht anzuwenden. In diesen Fällen haftet der Lieferant nur in engen Grenzen. Dafür, dass die Software die vorauszusetzende Beschaffenheit aufweist und Rechte Dritter einer Verwendung nicht entgegenstehen, hat der Schenker nur dann einzustehen, wenn er den Mangel arglistig verschwiegen hat (§§ 523, 524 BGB). Der Lieferant muss den Mangel kennen oder zumindest für möglich halten. Zudem muss eine Aufklärungspflicht bestehen, d.h., der Beschenkte muss eine vorherige Aufklärung über den jeweiligen Mangel erwarten können. Für die Haftung im Hinblick auf die sonstigen Rechtsgüter des Erwerbers hat der Lieferant bei kostenloser Überlassung nur Vorsatz und grobe Fahrlässigkeit zu vertreten (§ 521 BGB). Falls es durch das Programm also zu einer Verletzung der sonstigen Rechtsgüter des Erwerbers kommt, so haftet er nur, wenn er die Rechtsverletzung wissentlich herbeiführt oder seine Sorgfaltspflichten in besonders schwerem Maße verletzt.

Oftmals wird zugleich mit dem Softwareüberlassungsvertrag auch ein Supportvertrag abgeschlossen, in dem sich der Softwarelieferant zur Pflege und Instandhaltung der überlassenen Programme verpflichtet. Hier stellt sich die Frage nach dem Verhältnis der Mängelgewährleistung aus dem Überlassungsvertrag und den Pflichten des Dienstleisters aus dem Supportvertrag. Wird die Software gegen Entgelt überlassen, so hat die Behörde grundsätzlich einen Anspruch darauf, dass Mängel beseitigt werden, ohne dass hierfür ein besonderes Entgelt bezahlt werden muss. Während der Gewährleistungsfrist darf also nur für solche Leistungen ein Entgelt verlangt werden, die über das hinausgehen, was eine Behörde bereits im Rahmen der gesetzlichen Mängelgewährleistung verlangen kann, etwa 24-Stunden-Service und die Garantie, Ausfälle in bestimmten Reaktionszeiten zu beheben. Schwierig zu beurteilen sind solche Vertragsgestaltungen, in denen der Behörde die Software kostenlos überlassen wird, während für den Support ein Entgelt verlangt wird. Hier ist zugunsten der Behörde davon auszugehen, dass eine künstliche Aufspaltung in einen unentgeltlichen Teil mit nur geringer Gewährleistung und einen entgeltlichen Teil, für den eine erhöhte Einstandspflicht besteht, nicht wirksam vereitelt werden kann. Stellt sich eine Dienstleistung aus der Sicht der Behörde als eine einheitliche entgeltliche Leistung dar, so muss der Anbieter auch dafür einstehen, dass das Programm grundsätzlich funktionsfähig ist. Entsprechende Einstandspflichten für diese Basisgewährleistung dürfen nicht als kostenpflichtiger Support abgerechnet werden.

---

1 Ziffern 7-9 EVB-IT Überlassung Typ A und Ziffer 7-9 EVB-IT Überlassung Typ B (Haftung bei Mängeln).

2 Zum Einsatz der EVB-IT bei der Beschaffung von Open Source Software siehe oben 0 .

Tab. 53: Vertragliche Ansprüche auf Haftung und Gewährleistung gegen den Zwischenhändler

Entgeltlicher Erwerb	Sachmangel Rechtsmangel	Nacherfüllung
		Bei Fehlschlag der Nacherfüllung: ● Minderung ● Rücktritt ● Bei Verschulden Schadensersatz
	Schäden an sonstigen Rechtsgütern	Bei Verschulden Schadensersatz
Unentgeltlicher Erwerb	Sachmangel Rechtsmangel	Bei Arglist Schadensersatz
	Schäden an sonstigen Rechtsgütern	Bei grober Fahrlässigkeit / Vorsatz Schadensersatz

4.7.3 Ablösende Migration: Vertragliche Haftung und Gewährleistung bei Open Source Lizenzverträgen

Von den Verträgen mit den Lieferanten über die Überlassung der Software sind die Open Source Lizenzverträge zu unterscheiden. Letztere werden direkt mit den Rechtsinhabern abgeschlossen. Gegenstand dieser OSS-Lizenzen ist die Einräumung bestimmter Nutzungsrechte an der Software, insbesondere der Rechte zur Vervielfältigung, Verbreitung und Bearbeitung.

Die Erkenntnis, dass es sich um unterschiedliche Geschäfte handelt, ist für die Frage der vertraglichen Haftung und Gewährleistung von weit reichender Bedeutung. Denn jeder Vertragspartner hat nur für die von ihm zu verschaffenden Vertragsgegenstände eine Gewährleistung zu übernehmen und haftet auch nur für die Einhaltung seiner eigenen vertraglichen Verpflichtungen. Daraus folgt, dass die Urheber dem Lizenznehmer der OSS-Lizenz im Wesentlichen für den Bestand und Erhalt der Nutzungsrechte einzustehen haben. Nur insoweit kann die Behörde vertragliche Ansprüche gegenüber diesen geltend machen. Die tatsächliche Eignung der Software für die Programmbenutzung ist hingegen eine Frage des Einstehenmüssens der Distributoren oder der sonstigen Zwischenhändler aufgrund des Überlassungsvertrages. Das Gleiche gilt für die Befugnis der Behörde, die Software bestimmungsgemäß benutzen zu können; dieses Recht ergibt sich in der Regel bereits aus dem Erwerb einer rechtmäßig in Verkehr gebrachten Programmkopie. Fehlt es hieran, so ist der Distributor in Anspruch zu nehmen und nicht die Rechtsinhaber.

Bei der Frage, in welchem Umfang die jeweiligen Urheber für den Bestand der Nutzungsrechte einzustehen haben, gilt es zunächst festzuhalten, dass sich der Gewährleistungs- und Haftungsmaßstab in der Regel nicht nach den entsprechenden Klauseln in den jeweiligen OSS-Lizenzen richtet. Denn die allermeisten OSS-Lizenzen verwenden einen umfassenden, vollständigen Haftungs- und Ge-

währleistungsausschluss.[1] Entsprechende Klauseln sind nach deutschem Recht nichtig.[2] Rechtsfolge dieser Unwirksamkeit ist, dass die gesetzlichen Regelungen Anwendung finden.

Open Source Lizenzen stellen so genannte Lizenzverträge dar, deren Haftung und Gewährleistung im Gesetz nicht ausdrücklich geregelt ist. Da die Nutzungsrechte jedoch von den Urhebern gewährt werden, ohne dass die Zahlung einer Lizenzgebühr verlangt wird, wird ganz überwiegend davon ausgegangen, dass auf diese Verträge das Haftungs- und Gewährleistungsrecht der verschiedenen unentgeltlichen Verträge entsprechend anzuwenden ist. Weil zentraler Vertragsgegenstand der OSS-Lizenzen die Einräumung von Rechten ist, steht im Mittelpunkt gewährleistungsrechtlicher Fragen dabei das Einstehenmüssen für Rechtsmängel; Sachmängelgewährleistung spielt daneben in der Regel keine Rolle. Für Rechtsmängel, also insbesondere dafür, dass der Lizenzgeber Inhaber der lizenzierten Nutzungsrechte ist und Rechte Dritter einer Lizenzierung nicht entgegenstehen, hat dieser in Anlehnung an die schenkungs- und leihrechtlichen Vorschriften nur dann einzustehen, wenn er den Mangel arglistig verschwiegen hat. Liegt kein Fall der Arglist vor, so hat die Behörde das Risiko des Bestehens von Rechtsmängeln zu tragen.

Hinsichtlich der Schäden an sonstigen Rechtsgütern der Behörde ist die Haftung der Rechtsinhaber ebenfalls in Anlehnung an die Vorschriften für unentgeltliche Verträge auf Vorsatz und grobe Fahrlässigkeit beschränkt. Diese haften daher nur, wenn sie wissentlich gehandelt oder aber ihre Sorgfaltspflichten in besonders schwerem Maße verletzt haben.

4.7.4 Ablösende Migration: Vertragliche Haftung und Gewährleistung bei Erstellung und Änderung von Freier Software

Wird Software gegen Entgelt im Kundenauftrag erstellt, ist Werkvertragsrecht oder nach anderer Auffassung im Wesentlichen Kaufvertragsrecht anwendbar. Auch bei der entgeltlichen Anpassung von Software an die spezifischen Bedürfnisse der Behörde besteht eine Gewährleistung und Haftung nach werk- oder kaufvertraglichen Grundsätzen, abhängig von der jeweiligen Einordnung des Geschäftes.

Unabhängig davon, ob es sich bei den genannten Verträgen um Kauf- oder Werkverträge handelt, kann die Behörde von ihrem jeweiligen Vertragspartner bei Mängeln zunächst Nacherfüllung verlangen, wobei Unterschiede in der Ausübung je nach vertragstypologischer Einordnung der Verträge bestehen. Scheitert die Nacherfüllung, stehen dem Besteller Minderung, Rücktritt und – bei Verschulden der anderen Vertragspartei – Schadensersatzansprüche zu. Ob darüber hinaus die Behörde berechtigt ist, den Mangel selbst zu beseitigen oder beseitigen zu lassen und Ersatz der hierzu erforderlichen Aufwendungen verlangen

1 Vgl. z.B. Ziffern 11 und 12 GPL.

2 Dazu ausführlicher Jaeger/Metzger, Open Source Software: Rechtliche Rahmenbedingungen der Freien Software (2002), S. 145 ff.

kann, ist davon abhängig, ob man den Vertrag als Werkvertrag ansieht und nicht als einen Vertrag, auf den Kaufrecht Anwendung findet.

Für die vertragliche Haftung des Auftragnehmers gilt, dass dieser für schuldhaft verursachte Schäden an sonstigen Rechtsgütern des Erwerbers einzustehen hat. Eine fahrlässige Herbeiführung des Schadens begründet bereits eine entsprechende Haftung.

Wie bei allen Verträgen gilt auch hier, dass die Parteien innerhalb bestimmter Grenzen abweichende Abreden treffen können. Im Hinblick auf die keineswegs eindeutige Rechtslage sollte davon gerade auch im Bereich der OSS-Erstellungs- und Anpassungsverträge Gebrauch gemacht werden. Hier bietet es sich an, die Pflichten und Obliegenheiten der Vertragsparteien, insbesondere eine (aus dem Werkvertragsrecht bekannte) Abnahme ausdrücklich zu regeln sowie Vereinbarungen über Mängelrügefristen etc. zu treffen.

4.7.5 Ablösende Migration: Produkthaftung

Schäden im Zusammenhang mit der ablösenden Migration können nicht nur zu vertraglichen Ansprüchen gegenüber den jeweiligen Partnern führen. Vielmehr sind auch außervertragliche Haftungstatbestände zu beachten, insbesondere nach dem Produkthaftungsgesetz und dem allgemeinen Deliktsrecht der §§ 823 ff. BGB. Das Produkthaftungsgesetz begründet eine Haftung nur für Personenschäden und solche Sachschäden, die an einer anderen Sache als dem fehlerhaften Produkt eintreten. Eine Haftung besteht nach diesem Gesetz, das in erster Linie den Verbraucher schützen soll, dabei jedoch nicht für solche Sachen, die nicht primär privat verwendet werden.[1] Sachschadensersatzforderungen aus dem nichtprivaten Bereich sieht sich der Hersteller insoweit auf der Grundlage dieses Gesetzes nicht ausgesetzt. Insoweit ist gerade für die Behörde die Geltendmachung von Sachschäden aufgrund des Produkthaftungsgesetzes weitestgehend ausgeschlossen.

4.7.6 Ablösende Migration: Verschuldensabhängige außervertragliche Haftung

Neben der verschuldensunabhängigen Haftung nach dem Produkthaftungsgesetz kommt auch eine außervertragliche Haftung aufgrund allgemeiner außervertraglicher Haftungstatbestände (Deliktstatbestände) vor. Gerade weil das Produkthaftungsgesetz bei Sachschäden nur private Güter schützt, haben diese Regelungen für Behörden besondere Relevanz. Eine Geltendmachung auf Grundlage deliktsrechtlicher Vorschriften setzt kein Vertragsverhältnis voraus. Wenn beispielsweise eine Behörde ein Programm von einem Zwischenhändler erwirbt, so kommen gegenüber dem Distributor nur außervertragliche Ansprüche in Betracht, da insoweit kein Vertragsverhältnis besteht.

[1] Vgl. § 1 Abs. 1 ProdHaftG.

Interessant ist insbesondere die Regelung des § 823 BGB. Nach dieser Vorschrift ist derjenige zum Schadensersatz verpflichtet, der vorsätzlich oder fahrlässig Leben, Körper, Eigentum oder sonstige ähnlich „absolut“ geschützte Rechtspositionen widerrechtlich verletzt. Schwierig und nur im Einzelfall zu beurteilen ist dabei die Frage, wann die Verletzung „fahrlässig“ erfolgte. Fahrlässigkeit setzt die Verletzung von Sorgfaltspflichten voraus. Bei den jeweiligen einzelnen Entwicklern der Software wird man den zu beachtenden Sorgfaltsmaßstab nicht zu hoch ansetzen dürfen. Bei der Entwicklung von OSS werden regelmäßig auch unfertige Lösungen verbreitet, an denen die Community arbeitet. Deutlich weit reichender stellt sich hingegen die außervertragliche Haftung der Distributoren von OSS dar. Diese stellen in der Regel ein fertiges Endprodukt zur Verfügung, so dass von vornherein höhere Sorgfaltsanforderungen angezeigt erscheinen.

In der Praxis bestehen zum Teil Schwierigkeiten, das Vorliegen aller Tatsachen für das Bestehen eines Schadensersatzanspruchs zu beweisen. Dort, wo das Produkt in industrieller Weise gefertigt und vertrieben wird, kommt jedoch unter Umständen eine Anwendung der von der Rechtsprechung entwickelten Grundsätze der sog. Produzentenhaftung in Betracht. Dies betrifft vor allem die Herstellung fertiger Betriebssystemdistributionen durch Distributoren. Im Rahmen einer solchen Produzentenhaftung wird in verschiedener Hinsicht die Beweisführung des Verletzten erleichtert.[1]

4.7.7 Ablösende Migration: Mitverschulden

Sowohl bei der vertraglichen als auch bei der außervertraglichen Haftung ist zu berücksichtigen, dass die Ansprüche jeweils durch ein Mitverschulden der Behörde ganz oder teilweise im Umfang begrenzt sein können. Im Grenzfall können sie sogar wegen eines „überwiegenden“ Mitverschuldens der Behörde vollständig entfallen.

Ein wichtiger Bereich, in dem in der Praxis gehäuft Probleme eines möglichen Mitverschuldens auftreten, ist die Haftung für den Verlust von Datenbeständen. Hier ist zu beachten, dass es im gewerblichen Anwenderbereich vielfach als selbstverständlich angesehen wird, dass der Anwender eine zuverlässige, zeitnahe und umfassende Sicherung der Daten sicherstellt. Entsprechende Anforderungen wird man auch an Behörden stellen dürfen.

4.7.8 Vergleich fortführender und ablösender Migration

Ein Vergleich zwischen fortführender und ablösender Migration zeigt, dass dort, wo entgeltliche Verträge geschlossen werden, weitgehende Parallelen in der Haftung und Gewährleistung bestehen. Dort, wo bei der ablösenden Migration Software oder Nutzungsrechte kostenlos erworben werden, bestehen Gewährleistungs- und Haftungsprivilegierungen der Vertragspartner. Hier kann zu überlegen sein, ob die ersparten Erwerbskosten jedenfalls teilweise für eine Risikoab-

[1] Vgl. dazu Schiffner, Open Source Software (2002), S. 253 f.

sicherung (Supportverträge, Garantieverträge, Versicherungen) eingesetzt werden können und sollten.

Beim Erwerb der Software zur Benutzung innerhalb der Behörde ist Anspruchsgegner der vertraglichen Haftung und Gewährleistung der jeweilige Vertragspartner des Überlassungsvertrages. Die Frage, ob eine ablösende oder eine fortführende Migration gewählt wird, führt hier zu keinen Unterschieden. Arbeitet die Software nicht vertragsgemäß oder stehen Rechte Dritter einer Benutzung entgegen, ist stets der Händler zur Beseitigung der Beeinträchtigung verpflichtet. Der Händler haftet auch für Schäden an sonstigen Rechtsgütern der Behörde. Der gesetzliche Haftungsumfang ist dabei derselbe, solange die Software entgeltlich erworben wird. Macht die Behörde hingegen von der bei ablösender Migration bestehenden Möglichkeit Gebrauch, die Software kostenlos zu erwerben, so muss sie Abstriche im Haftungs- und Gewährleistungsumfang hinnehmen.

Will die Behörde Lizenzrechte erwerben, etwa um die Software zu vervielfältigen, anzupassen oder an andere Behörden weiterzugeben, so werden bei OSS diese Rechte stets kostenlos eingeräumt. Bei fortführender Migration bedarf es hingegen regelmäßig – soweit überhaupt eine entsprechende Rechtseinräumung erfolgt – der Zahlung einer Lizenzgebühr. Aufgrund dieser Unterschiedlichkeit der zugrunde liegenden Verträge variiert auch der Haftungs- und Gewährleistungsmaßstab beträchtlich. Bei kostenloser Einräumung besteht eine weitgehende Privilegierung. Hier steht es der Behörde bei der ablösenden Migration allerdings offen, ersparte Erwerbskosten für eine Risikoabsicherung einzusetzen.

Gewisse Unterschiede im Haftungsumfang bestehen im Bereich der außervertraglichen Haftung. Da der proprietäre Hersteller auf sämtliche Schritte im Entwicklungsprozess Einfluss nehmen kann, wird man auch einen höheren Sorgfaltsmaßstab anlegen können. Allerdings spielt die außervertragliche Haftung des Herstellers von Computerprogrammen in der Praxis bisher allenfalls eine untergeordnete Rolle.

4.8 Vergaberecht

4.8.1 Allgemeines

Die Wahl der Behörde zwischen einer fortführenden und einer ablösenden Migration hat unter Beachtung der Prinzipien des Vergaberechts zu erfolgen.[1] Die Beschaffung von Informationstechnologie muss grundsätzlich nach Maßgabe des Wettbewerbsprinzips erfolgen, vgl. § 97 Abs. 1 GWB. Hierbei sind alle Bewerber gleich zu behandeln ("Gleichbehandlungsgrundsatz", vgl. § 97 Abs. 2 GWB). Vergabefremde Kriterien, die nicht an die Wirtschaftlichkeit des Angebots oder die Fachkunde, Leistungsfähigkeit und Zuverlässigkeit des Bewerbers anknüpfen, dürfen nicht berücksichtigt werden (vgl. § 97 Abs. 4 GWB).

[1] Vgl. zum Folgenden eingehend Heckmann in: Spindler (Hrsg.), Rechtsfragen bei Open Source (2004), S. 281 ff.

Überschreitet der Beschaffungsauftrag die Schwellenwerte der Vergabeverordnung[1], so besteht für die übergangenen Bieter die Möglichkeit, eine Nachprüfung der Vergabeentscheidung nach den Vorschriften des GWB zu beantragen. Dies kann zu einer Verzögerung der Beschaffung führen und birgt das Risiko zusätzlicher Kosten für das Verfahren vor der Vergabekammer und die ggf. erforderliche erneute Ausschreibung, falls die Behörde die Vergaberechtsprinzipien missachtet hat.

4.8.2 Ablösende Migration: Neutrale Ausschreibung

Aus dem Wettbewerbsprinzip und dem Gleichbehandlungsgrundsatz ergibt sich als erste Anforderung an eine vergaberechtskonforme Beschaffung, dass in der Ausschreibung die geforderten Leistungen neutral beschrieben werden. Die Anforderungen an eine neutrale Leistungsbeschreibung sind in § 8 VOL/A näher bestimmt.

In der juristischen Fachliteratur wird zum Teil unter Berufung auf § 8 VOL/A gefordert, dass eine Ausschreibung für IT-Aufträge nicht von vornherein auf Open Source Software beschränkt erfolgen darf. Folgt man dieser strengen Auslegung des Vergaberechts, so muss eine Ausschreibung die geforderten Leistungen in einer Weise beschreiben, die es auch den proprietären Konkurrenzprodukten ermöglicht, ihre Leistungen anzubieten, soweit die Ziele der Behörde auch mit diesen erreicht werden können. Die Entscheidung für eine ablösende Migration darf dementsprechend nicht bereits vor der Ausschreibung gefallen sein. Es fehlt hier bislang eine Klärung durch die Vergabekammern des Bundes und der Länder. Einstweilen ist Behörden zu raten, ihre Beschaffungsvorgänge am Maßstab dieser strengen Auslegung des Vergaberechts auszurichten.

Danach muss im Grundsatz sowohl auf eine Leistungsbeschreibung "Linux-Server" als auch auf die Bezeichnungen "Open Source oder quelloffene Software" verzichtet werden. Stattdessen sind die konkreten Merkmale der geforderten Leistungen abstrakt zu beschreiben, damit auch proprietäre Konkurrenten ihre Leistungen anbieten können.

Es ist also statt der Bezeichnung "Linux-Server" neutral zu beschreiben, welche Merkmale der Server erfüllen soll. Sind die Vorgaben entsprechend neutral formuliert, sollten zumindest auch Server, die mit anderen UNIX-Derivaten betrieben werden, die Spezifikationen erfüllen können.

Statt "Open Source Software" sollte beschrieben werden, welche konkreten Ziele die Behörde hiermit erreichen möchte. Es erscheint als vergaberechtlich bedenklich, pauschal die Offenlegung der Quellcodes zu verlangen, wenn für die Bieter nicht erkennbar ist, welche Ziele die Behörde hiermit verfolgt. Dagegen erscheint der Hinweis auf das Erfordernis offener Quellcodes als zulässig, sofern die Behörde angibt, dass ein erhöhtes Maß an Sicherheit gegen "backdoors", Virenat-

[1] IT-Aufträge der obersten und oberen Bundesbehörden und vergleichbarer Bundeseinrichtugen: 130.000 €, alle anderen IT-Aufträge: 200.000 €.

tacken und Ähnliches für die Erfüllung der öffentlichen Aufgabe erforderlich ist. Dies bietet proprietären Bietern die Möglichkeit, sich durch eine Offenlegung im Einzelfall an der Ausschreibung zu beteiligen.[1]

Die gleichen Grundsätze gelten für Leistungsbeschreibungen, die die OSS-Lizenzen als Leistungsanforderungen beinhalten ("GPL-Software" o.ä.). Entsprechende Anforderungen sollten durch neutrale Beschreibungen ersetzt werden, die auf den Umfang der gewünschten Nutzungsrechte hinweisen und erkennen lassen, wofür die Behörde diese Rechte einsetzen möchte. Auch im Hinblick auf die Nutzungsrechte muss proprietären Geboten eine realistische Chance gegeben werden.

Schließlich ist darauf hinzuweisen, dass die ausgeschriebene Leistung nicht so zugeschnitten sein darf, dass ein tatsächlicher Wettbewerb im Hinblick auf die vollständigen Kosten einer IT-Beschaffung verhindert wird. Es ist vergaberechtlich zweifelhaft, wenn die Behörde zwar eine einheitliche IT-Infrastruktur benötigt, durch eine künstliche Aufspaltung der einzelnen Bestandteile aber die eigentliche Wirtschaftlichkeitsentscheidung umgeht. Dies wäre etwa der Fall, wenn die Lieferung von OSS als kostenlos eingeordnet wird, was zur Folge hätte, dass die Leistung überhaupt nicht ausgeschrieben werden müsste[2], während der kostenpflichtige Support ausgeschrieben wird. Ein vollständiges Bild kann hier nur gewonnen werden, wenn jeweils Software und Support gemeinsam als einheitliches Erfüllungsgeschäft verglichen werden. Die Ausschreibung muss also den Vergleich der jeweiligen Gesamtwirtschaftlichkeit gestatten, um nicht von vornherein die proprietären Anbieter zu benachteiligen.

4.8.3 Ablösende Migration: transparente Ausschreibung

Um einen echten Wettbewerb zwischen den Angeboten zu erreichen, sind in der Ausschreibung alle die Entscheidung beeinflussenden Umstände aufzunehmen (vgl. § 97 Abs. 1 GWB, § 8 Abs. 2 VOL). Faktoren, die in der Ausschreibung nicht genannt wurden, dürfen später bei der Entscheidung nicht berücksichtigt werden.

Behörden, die eine ablösende Migration in Betracht ziehen, müssen deswegen bereits in der Ausschreibung auf die Eigenschaften hinweisen, die für eine solche Entscheidung sprechen könnten. Dies sollte allerdings auf einer Abstraktionsebene geschehen, die es auch Anbietern proprietärer Produkte ermöglicht, sich an der Ausschreibung zu beteiligen. Es erscheint als vergaberechtlich unbedenklich, wenn auf die besondere Bedeutung der Kompatibilität der Programme und der mit diesen Programmen erzeugten Dateien mit anderen Programmen und deren erzeugten Dateien hingewiesen wird. Auch sollte auf die Bedeutung der Verwendung von Standardschnittstellen verwiesen werden. Es kann auch dazu

---

1 Dass dies proprietären Anbietern eine realistische Chance eröffnet, zeigt das "Shared Source"-Programm von Microsoft, welches bestimmten Lizenznehmern Einblick in die Quelltexte der Microsoft-Programme gewährt. Siehe hierzu http://www.microsoft.com/resources/sharedsource/default.mspx.

2 Vgl. § 99 GWB: "Öffentliche Aufträge sind entgeltliche Verträge [...].

angeführt werden, dass eine größtmögliche Unabhängigkeit von einzelnen Anbietern im Hinblick auf andere Informationstechnologien, aber auch im Hinblick auf Supportdienstleistungen gewünscht wird. Auch sollte bereits in der Ausschreibung klargestellt werden, dass Leistungen gefordert sind, die eine nachhaltige Entwicklung der Behördenhard- und -software versprechen.

Entsprechende Leistungsbeschreibungen sollten es allen Bietern gestatten, sich auf die Entscheidungskriterien der Behörde einzustellen und die Gebote entsprechend auszurichten.

4.8.4 Ablösende Migration: Vergabeentscheidung

Der vergaberechtlich richtige Zeitpunkt für eine Migrationsentscheidung ist die Wertung der Angebote bei der Vergabeentscheidung. Der Zuschlag ist gemäß § 97 Abs. 5 GWB auf das wirtschaftlichste Angebot zu erteilen. § 25 Nr. 3 VOL/A bestimmt näher, dass der niedrigste Angebotspreis nicht allein entscheidend ist. Es ist deswegen vergaberechtlich nicht zu beanstanden, wenn sich Behörden entgegen kurzfristiger monetärer Anreize für ein höherwertiges Angebot entscheiden. Entscheidend für die Wirtschaftlichkeit eines Angebots ist das günstigste Verhältnis zwischen der gewünschten Leistung und dem angebotenen Preis.

Vergabefremde Kriterien sind dabei auszuscheiden, es sei denn, sie sind ausdrücklich durch Bundes- oder Landesgesetz vorgesehen (vgl. § 97 Abs. 4 GWB). Entsprechende Gesetze, welche eine bevorzugte Beschaffung von OSS vorschreiben, sind bislang nicht erlassen worden, und zwar weder auf Bundes- noch auf Landesebene. "Grundsatzbeschlüsse", wie etwa der des Deutschen Bundestags vom 09.11.2003, in welchem der Bundestag "die Einführung von unter Open-Source-Lizenzen erstellten Produkten in der Bundesverwaltung" gefordert hat[1], können weder als Ersatz für ein Gesetz im Sinne von § 97 Abs. 4 GWB bewertet werden, noch entbinden sie Behörden von den Vorgaben des Vergaberechts. Die Vergabeentscheidung ist also auch bei Vorliegen entsprechender Empfehlungen nach dem Wirtschaftlichkeitsprinzip auszurichten.

Bei Anlegung dieser Grundsätze ergibt sich das folgende Bild: Pauschale Hinweise auf die Förderung von OSS oder des Wettbewerbs auf den IT-Märkten sind als vergabefremde Kriterien unzulässig. Die IT-Beschaffung durch Behörden ist nicht der richtige Platz, um Wettbewerbspolitik zu betreiben. Das Gleiche gilt für sozialpolitische oder sonstige allgemeine Erwägungen. Behörden dürfen entsprechende Argumente bei der Begründung einer Vergabeentscheidung nicht zugrunde legen.

Es ist aber darauf hinzuweisen, dass sich Behörden nicht mit einem einfachen Preisvergleich der Gesamtangebote begnügen müssen. Die Erfahrung zeigt, dass kurzfristige monetäre Vorteile oftmals später teuer bezahlt werden müssen.

[1] Vgl. den dem Beschluss zugrunde liegenden Antrag der Regierungsfraktionen, Bundestags-Drucksache 14/5246, S. 4 ff.

Dies kann insbesondere dann der Fall sein, wenn Behörden Produkte anschaffen, die nur mit Produkten desselben Anbieters kombiniert werden können oder für die ausschließlich dieser Anbieter Supportleistungen anbietet. Kurzfristige Preisnachteile können oft mittelfristig durch die Unabhängigkeit von einzelnen Anbietern auf den Folgemärkten ausgeglichen werden. OSS bietet hier einen strategischen Vorteil. Offene Quelltexte und die Freiheit, Änderungen an diesen vorzunehmen, sorgen dafür, dass wichtige Folgemärkte für eine Mehrzahl von Anbietern offen stehen. Dies sorgt für Wettbewerb und Kostenvorteile. Eine entsprechende Einbeziehung konkret absehbarer Begleit- und Folgekosten ist im Sinne einer nachhaltigen Verwendung öffentlicher Mittel wünschenswert. Es sollte hierbei aber nicht direkt auf die zu erwartenden mittel- und langfristigen Kosten verwiesen werden, denn die Vergabekriterien müssen stets auf die ausgeschriebene Leistung bezogen sein. Vielmehr müssen die genannten Eigenschaften von OSS als Vorteil einer ablösenden Migration im Rahmen des Preis-Leistungs-Vergleichs berücksichtigt werden.

Vergaberechtlich zulässig sind auch alle sonstigen Kriterien, denen Aussagekraft für die Leistungsfähigkeit der einzelnen Angebote zukommt. Hier können unter anderem einbezogen werden: die technische Sicherheit der IT-Angebote, die Kompatibilität mit anderen Programmen, die Kompatibilität der mit dem Programm erzeugten Dokumente, die technischen und rechtlichen Nutzungsmöglichkeiten, Fragen der Haftung und Gewährleistung. Entsprechende Kriterien dürfen allerdings nur unter der Voraussetzung berücksichtigt werden, dass sie in der Ausschreibung ausdrücklich benannt worden sind.

4.8.5 Vergleich fortführender und ablösender Migration

Die Anforderungen des Vergaberechts gelten in gleichem Maße für eine ablösende wie eine fortführende Migration. Ausschreibungen dürfen nicht so gestaltet sein, dass bestimmte Bieter, seien es Anbieter proprietärer oder OSS-Produkte, von vornherein faktisch ausgeschlossen sind. Das oben Ausgeführte kann also entsprechend angewandt werden.

Allerdings bestehen im Hinblick auf proprietäre IT-Produkte vergaberechtliche Probleme, die auf OSS nicht in gleichem Maße zutreffen. Dies gilt insbesondere für das oft anzutreffende Problem der mangelnden Kompatibilität von Software einzelner Anbieter mit den Produkten anderer Anbieter. Hier hat sich in der Vergangenheit für Behörden häufig das Problem gestellt, dass bei der Migration von Teilen der eigenen IT-Infrastruktur letztlich nur Leistungen desselben Bieters in Betracht gezogen worden sind, da eine Migration auf Produkte anderer Anbieter mit technischen Hürden verbunden gewesen wäre.

Andere Bieter hatten es auch in solchen Fällen schwer, sich durchzusetzen, in denen die Behörde elektronische Dokumente mit anderen Behörden oder Privaten austauschen muss, wobei die Programme eines Anbieters bei den anderen Behörden oder Privaten eine Art faktischer Standard darstellen, ohne dass auf die Dokumente mit anderen Programmen zugegriffen werden kann. Dieses Prob-

lem hat in den letzten Jahren beispielsweise eine ablösende Migration von MS Office zu anderen Produkten aus der Sicht vieler Behörden verhindert. Das Wettbewerbsprinzip ist bei entsprechenden Beschaffungsvorgängen oft auf vergaberechtlich unzulässige Weise ausgehebelt worden, indem eine Überprüfung der Kompatibilität anderer Programme gar nicht erst vorgenommen worden ist.[1]

Entsprechende Probleme ergeben sich bei OSS in geringerem Maße, da OSS-Programme oftmals auf eine größtmögliche Kompatibilität mit anderen, auch proprietären Produkten ausgelegt sind. So gestattet etwa Open Office den Export von Textdateien als PDF-Dokumente sowie das Abspeichern als MS Word-Dokument. Von besonderer Bedeutung ist auch, dass das standardmäßige Dateiformat in Open Office ein offenes XML-Dateiformat ist. Es kann damit auch auf entsprechende Dokumente zugegriffen werden, ohne Open Office zu benutzen. Die Systemabhängigkeit ist dadurch abgeschwächt, die technischen Hürden für eine Migration sind geringer. Der Einsatz von technischen Lösungen, welche den Übergang zu anderen Produkten erleichtert, verringert vergaberechtliche Probleme bei der Beschaffung von IT-Produkten.

4.9 Fazit

Eine Gesamtschau der untersuchten rechtlichen Fragen lässt weder den Schluss auf eine rechtliche Überlegenheit einer fortführenden, noch einer ablösenden Migration zu. Je nach Fallgestaltung können bei beiden Migrationswegen die gleichen oder doch vergleichbare rechtliche Probleme entstehen.

In einigen Fragen sind aus der Sicht der Behörde als Nutzer besondere Stärken von OSS festzustellen, in anderen Einzelaspekten erweist sich proprietäre Software als rechtlich überlegen. Für eine fortführende Migration kann sprechen, dass hier die Inhaberschaft an den Urheberrechten mitunter transparenter ist als bei OSS. Dies verringert das Risiko entgegenstehender Rechte Dritter. Dies gilt allerdings nicht für etwaige Patente Dritter. Hier bestehen für beide Migrationswege die gleichen rechtlichen Risiken. Für eine ablösende Migration spricht vor allem die umfassende Einräumung von Rechten an den Nutzer. Dieser genießt weitgehende Freiheiten beim Umgang mit OSS.

Welcher Migrationsweg im Einzelfall rechtlich vorteilhafter ist, hängt von verschiedenen Faktoren ab, insbesondere der angestrebten Art der Nutzung der Software, den möglichen Vertragspartnern und den hierbei ausgehandelten Konditionen. Eine abschließende Gesamtempfehlung ist deswegen nicht möglich. Festzuhalten ist aber auch, dass es zumeist nicht gerechtfertigt ist, eine ablösende oder fortführende Migration unter pauschalem Verweis auf die rechtlichen Risiken auszuscheiden.

[1] Vgl. beispielsweise Bundeskartellamt, 2. Vergabekammer des Bundes, Beschluss vom 08.08.2003, AZ: VK 2-52/03, S. 30-32 (abrufbar unter http://www.bundeskartellamt.de).

5 Wirtschaftlichkeitsbetrachtung

5.1 Vorwort

Die Wirtschaftlichkeitsbetrachtungen für Migrationsvorhaben im Rahmen des Migrationsleitfadens sind in wesentlichen Punkten überarbeitet worden.

Das Hauptaugenmerk liegt jetzt auf der Methodenvermittlung. Berechnungsbeispiele werden nur und ausschließlich zu Verständniszwecken im Anhang eingefügt.

Die beiden Methoden WiBe 4.0 und Migrationskostenmatrix (MiKoMa) werden weiterhin als Alternativen betrachtet. In diesem Zusammenhang ist zu betonen, dass ausschließlich die WiBe 4.0 über einen rechtlich verbindenden Charakter verfügt. Sie stellt eine auch vom Bundesrechnungshof anerkannte Methodik zur Ermittlung der Wirtschaftlichkeit von IT-Maßnahmen dar. Die MiKoMa wird von den Autoren als Alternative zur WiBe vorgestellt. In rechtlich nicht relevanten Situationen bietet sie eine schlankere Möglichkeit zur WiBe. Um dem Leser eine stringente und abgrenzbare Betrachtung der beiden Methodiken zu gewährleisten, wird zunächst die WiBe 4.0 vorgestellt und anschließend auf die MiKoMa eingegangen.

Zusätzlich wird eine spezifische Sprachregelung eingeführt: In den Wirtschaftlichkeitsbetrachtungen des Migrationsleitfadens wird der Begriff "WiBe" nur im Zusammenhang mit der WiBe 4.0 verwendet. In der Beschreibung der MiKoMa 2.0 wird der Begriff Wirtschaftlichkeitsbetrachtung entweder ausgeschrieben oder durch "MigrationsWibe" ersetzt.

Eine Produktivitätsbetrachtung in der IT-Wertschöpfungskette findet im Umfang dieses Leitfadens nicht statt, da entsprechende neutrale Langzeituntersuchungen insbesondere in der Verwaltung nicht vorhanden sind. Sie würde auf Basis heutiger Erfahrungen und insbesondere im Hinblick darauf, dass es sich sowohl bei Linux/Unix- als auch Microsoft-Plattformen um reife Produkte mit langjähriger Entwicklungszeit handelt, voraussichtlich zu einem ausgewogenen Ergebnis führen.

Weiterhin werden im Rahmen der nachfolgenden Wirtschaftlichkeitsbetrachtungen die Auswirkungen von besonderen Integrationsaspekten nicht tiefergehend betrachtet. Eine tiefergehende Berücksichtigung der Integrationsaspekte kann aufgrund der Zielsetzungen des Migrationsleitfadens nur im Rahmen der behörden- und damit anforderungsspezifischen Wirtschaftlichkeitsbetrachtungen hinreichend qualifiziert erfolgen. Da es aber nicht das Ziel des Migrationsleitfadens (siehe Vorwort zum Leitfaden) ist, für die öffentliche Verwaltung global Anforderungen an die IT-Infrastruktur zu definieren und damit auch nicht Ziel sein kann festzulegen, welche integrierten Systeme diesen Anforderungen genügen, kann in den Wirtschaftlichkeitsbetrachtungen auch der Aspekt Integration nicht besonders berücksichtigt werden. Da der Leitfaden am Ende aber offen lässt bzw. auch

offen lassen muss, welcher Migrationspfad im Einzelfall der wirtschaftlichere ist, dürfte dies für die Leser des Leitfadens keine Beeinträchtigung darstellen.

5.2 Einleitung

Wie die Diskussion über die auf dem Markt verfügbaren Studien zum Thema TCO[1] beim Einsatz von OSS- und COLS-Produkten[2] zeigt, ist die Durchführung einer Wirtschaftlichkeitsbetrachtung für IT-Vorhaben generell sehr schwierig und wird bei den häufig multidimensionalen Wirtschaftlichkeitsmodellen zu einer nahezu unlösbaren Aufgabe.

Bei einer breitgefächerten und facettenreichen Analyse – was beim Vergleich von Kosten für Microsoft- und OSS/ COLS-Plattformen zweifelsohne der Fall ist – gehört die Herstellung der Vergleichbarkeit der Untersuchungsobjekte sowie des richtigen Umfangs der Analyse zu den wesentlichen Aufgaben. Eine schmale Betrachtung isolierter Aspekte lässt das Ergebnis nicht notwendigerweise auf das Gesamtbild übertragen, wie das Beispiel der von Microsoft in Auftrag gegebenen IDC-Studie „Windows 2000 vs. Linux für Unternehmensanwendungen“ verdeutlicht. Da die Studie lediglich die Kosten der Server für Infrastruktur-Aufgaben untersucht, bei denen der Anteil der Softwarelizenzen zu den Gesamtkosten in einem anderen Verhältnis als beispielsweise bei Client-Anwendungen steht, sind Angaben zur Wirtschaftlichkeit im Anwendungs- oder Desktop-Bereich nicht direkt ableitbar.

Eine weitere Notwendigkeit bei der Untersuchung besteht in der Berücksichtigung der Nutzerstrukturen. Insbesondere die Größe von Organisationen und die unterschiedlichen Ausgangsszenarien der IT-Umgebung sind relevant für die Wirtschaftlichkeitsbetrachtung einer Migration. Häufig kann beobachtet werden, dass in kleineren Behörden (beispielsweise im kommunalen Sektor) die IT-Infrastruktur mit einfachen Mitteln und ohne intensive Ausbildung der Beteiligten aufgebaut und betrieben werden kann. Auf der anderen Seite erfordert der zuverlässige Betrieb von Infrastrukturen oder Rechenzentren für große und/ oder spezialisierte Behörden und Datenzentralen mit Service Level Agreements einen erhöhten Ausbildungsstand der Mitarbeiter, organisatorische Regelungen für Ausfall- und Notfallzeiten sowie häufig eine andere Hardware-Ausstattung.

Unter Berücksichtigung dieser Randbedingungen ist für die IuK-Wirtschaftlichkeit eine mehrdimensionale Betrachtung notwendig. Im Vorfeld der Untersuchung der IT-Kosten gilt, dass ein wesentlicher Beitrag zur Erhöhung der Wirtschaftlichkeit zunächst einmal durch personelle, organisatorische und rationalisierende Maßnahmen in den Verwaltungen erreicht werden kann. Darüber hinaus kann jedoch durch entsprechend ausgelegte IT-Strategie ebenfalls ein wesentlicher Beitrag zur Erhöhung der Wirtschaftlichkeit geliefert werden.

---

1 TCO = Total Cost of Ownership

2 OSS = Open Source Software, COLS = Commercial Linux Software

Die Gesamtwirtschaftlichkeit der IT wird stark beeinflusst durch:

- Den Grad der funktionalen Abdeckung durch preiswerte Standardprodukte
- Qualität, Änderungsflexibilität und Entwicklungsfähigkeit der eingesetzten Standards, Technologien und Produkte
- Effizientes Einführungs- und Systemmanagement
- Bruchfreie Integration von Komponenten und Systemen in einer prozessorientierten Wertschöpfungskette
- Gute (interne oder externe) Service-Organisation sowie hochwertiges Know-how
- Wirtschaftliche Lebenszyklen der Produkte
- Kosten und Effizienz des Beschaffungsprozesses, sowie
- Wettbewerb bei Produkten und Dienstleistungen

Erst ein optimales Zusammenspiel all dieser Faktoren über einen längeren Betrachtungszeitraum bedingt und beeinflusst die Wirtschaftlichkeit insgesamt, so dass eine vereinfachte Betrachtung von Einzelkosten das Gesamtbild in der Regel nicht korrekt widerspiegeln kann.

Neben der Ermittlung und dem Vergleich von Kosten bedeutet auch die Beurteilung der möglichen Nutzwerte einen wesentlichen Aspekt der Wirtschaftlichkeitsbetrachtung. Insbesondere in diesem Bereich spielen strategische Überlegungen und prognostizierte Vorteile eine wichtige Rolle, um sowohl die Ausgangssituation als auch die Perspektive ganzheitlich beurteilen zu können. Beispiel: Die auf eine vereinzelte Komponente bezogenen Mehrkosten können in der strategischen Betrachtung durch die erreichte Herstellerunabhängigkeit eine bessere Verhandlungsposition bei Softwarelizenzpreisen zu einem insgesamt deutlich günstigeren Gesamtergebnis führen. Diese Zusammenhänge einer Gesamtbetrachtung von Kosten und Nutzwert werden besonders deutlich im Ergebnis der „Client Studie der Landeshauptstadt München“[1], die im Ergebnis der monetären Wirtschaftlichkeitsbetrachtung eine Migration nach Windows XP und Office XP als wirtschaftlicher sieht und dagegen in der Gesamtbetrachtung von monetärer Wirtschaftlichkeit und Nutzwertbetrachtung ein Zielsystem mit Linux und Open Office.org präferiert[2].

---

1 Erstellt durch Unilog Integrata Unternehmensberatung GmbH, Unilog Managment, unterstützt durch die Landeshauptstadt München, Direktorium AfID, Abt. 5, München 2003 http://www.muenchen.de/vip8/prod2/mde/_de/rubriken/Rathaus/40_dir/limux/publikationen/clientstudie_kurz.pdf

2 Bei der Betrachtung der Ergebnisse der Studie lohnt es sich genau hin zu sehen. Zu einem wo die Gründe für die Vorteile von XP bei der monetären Wirtschaftlichkeit herrühren und zum anderen, woraus sich die Gründe Vorteile von Linux und OSS in einer Nutzwertbetrachtung herleiten lassen.

Sowohl die Methode als auch das Ergebnis kann aus diesen Gründen lediglich als Hilfe bei der Ermittlung der eigenen Wirtschaftlichkeit und somit bei der Formulierung der eigenen IT-Strategie dienen.

5.3 Methodische Grundsätze

Kapitel 2.1 der Verwaltungsvorschrift zu § 7 Bundeshaushaltsordnung (BHO) besagt: " Wirtschaftlichkeitsuntersuchungen in der Planungsphase bilden die Grundlage für die begleitenden und abschließenden Erfolgskontrollen. Wirtschaftlichkeitsuntersuchungen müssen mindestens Aussagen zu folgenden Teilaspekten enthalten:

- Analyse der Ausgangslage und des Handlungsbedarfs,
- Ziele, Prioritätsvorstellungen und mögliche Zielkonflikte,
- relevante Lösungsmöglichkeiten und deren Nutzen und Kosten (einschl. Folgekosten), auch soweit sie nicht in Geld auszudrücken sind,
- finanzielle Auswirkungen auf den Haushalt,
- Eignung der einzelnen Lösungsmöglichkeiten zur Erreichung der Ziele unter Einbeziehung der rechtlichen, organisatorischen und personellen Rahmenbedingungen,
- Zeitplan für die Durchführung der Maßnahme,
- Kriterien und Verfahren für Erfolgskontrollen (vgl. Nr. 2.2, VV zu § 7 BHO)."

Diese Anforderungen stellen prinzipiell den Rahmen und die Struktur für die Wirtschaftlichkeitsbetrachtungen (vgl. Bild 69, S. 405) dar. Ein wesentlicher Bestandteil sind die Zielvorstellungen der Behörde, in diesem Zusammenhang auch mögliche Zielkonflikte sowie Rahmenbedingungen in Form von Vorgaben und Annahmen. Die Abstimmung des Modells der Wirtschaftlichkeitsbetrachtung gehört auch in diesen Bereich. Daneben ist die Ist-Situation der zu migrierenden IT-Landschaft zu erheben, wobei Informationen zur Infrastruktur, der Hard- und Softwareprodukte, der IT-Fachverfahren sowie behördenspezifischer Dokumentvorlagen ermittelt werden. Auf dieser Basis werden technische Lösungsmöglichkeiten eruiert und mit Kostenansätzen unterlegt. Dazu gehören neben den Kosten für Hard- und Software auch die Aufwendungen für externes und internes Personal. Die sich nun anschließende Ermittlung der Wirtschaftlichkeit berechnet Kosten und Nutzen der IT-Maßnahme und die liquiditätsmäßigen Auswirkungen auf den Haushalt. Zur Einschätzung der Personalkosten wird eine grobe Projektplanung erforderlich, die auch einen Zeitplan für die Durchführung der IT-Maßnahme beinhaltet.

Bild 69: Regelkreis der Wirtschaftlichkeitsbetrachtung

5.3.1 Ziele und Rahmenbedingungen

5.3.1.1 Ziele

Vor der Durchführung einer jeden IT-Maßnahme sollten die im IT-Rahmenkonzept festgelegten oder aus strategischen Vorgaben abgeleiteten operativen Behördenziele festgestellt werden. Ein Abgleich dieser Ziele mit dem IT-Vorhaben reduziert mögliche Konflikte mit den Zielvorgaben und anderen Projekten. Weiterhin wird hiermit der Grundstein für in Kapitel 2.2 der VV zu § 7 BHO geforderten Zielerreichungskontrolle gelegt.

Die Erstellung eines grundsätzlichen Ziel- und Anforderungssystems für die IT-Maßnahme hilft, mögliche Lösungen unabhängig von der Wirtschaftlichkeit auf ihre Eignung hin zu prüfen. Hiermit wird konkret die Definition von Anforderungskriterien angesprochen, die für die einzelnen Lösungsalternativen in Form von Nutzwertanalysen[1] zu bewerten sind. Einzelne dieser Kriterien oder Kriteriengruppen können im Rahmen der Zielerreichungskontrolle als Messgröße dienen.

An dieser Stelle sei der Hinweis gegeben, dass die Definition der Zielsetzungen der Behörde und die damit verbundenen notwendigen Aktivitäten in einem sepa-

[1] Vgl. WiBe 4.0, Empfehlung zur Durchführung von Wirtschaftlichkeitsbetrachtungen in der Bundesverwaltung, insbesondere beim Einsatz der IT, Version 4.0 – 2004, "Berechnung der erweiterten Wirtschaftlichkeit", S. 80 ff

raten Strategieprozess gefunden werden sollten. Hierfür sind in der Praxis erprobte Methodiken verfügbar, die die Gesamt-Strategie einer Behörde definieren helfen und die strategische Ableitung für die IT unterstützen.

5.3.1.2 Prämissen und Annahmen

Jede IT-Maßnahme muss im Kontext einer vorhandenen IT-Landschaft, einer existenten Organisation und bestehender Gesetze, Vorschriften und Vorgaben durchgeführt werden. Daher wird es für den Erfolg der IT-Maßnahme zwingend notwendig, diese externen Einflussfaktoren zu identifizieren und zu dokumentieren. Auch die Ausgestaltung der Durchführung der Wirtschaftlichkeitsberechnung beinhaltet i.d.R. spezifische Festlegungen, die einmal generell genannt und kurz beschrieben werden sollten. Grundsätzliche Wertansätze, die nicht in der Wirtschaftlichkeitsrechnung selbst ermittelt werden, sondern von außerhalb des Systems übernommen werden (z.B. Personalkostenansätze). Solche Informationen, die eine wichtige Grundlage für die Berechnung darstellen, sind festzuhalten. Als Beispiel sind nachfolgend einige als "Annahmen" bezeichnete Rahmenbedingungen dargestellt.

Der Wirtschaftlichkeitsbetrachtung können z.B. folgende Prämissen zugrunde liegen:

Tab. 54: Beispiele für Annahmen einer Wirtschaftlichkeitsbetrachtung

1. Die Potenziale werden getrennt für Betrieb, Projekte und Ersparnisse dargestellt. Bezüglich Betrieb werden die Veränderungen der Kosten (Steigerungen, zusätzliche Kosten, Investitionen) angegeben. Für Projekte werden ausschließlich die Kosten zur Durchführung der Projekte aufgeführt, keine Investitionen. Die Ersparnisse leiten sich aus nicht mehr benötigten Betriebsaufwendungen her. Dies kann auch künftig erforderliche Aufwendungen betreffen, die heute noch nicht real sind (z.B. notwendige Vertragsaufstockungen, etc.).
2. Zur Berechnung von Kapitalwerten wird ein Diskontierungssatz in Höhe von 4,6% entsprechend dem empfohlenen Nominalzins aus dem Papier zu den Personalkostensätzen des BMF von 2004 verwendet.
3. Personalkosten intern: durchschnittliche Personalkosten in diesem Bereich dividiert durch 204 Arbeitstage/Jahr ergibt nnn €/ Personentag (PT)
4. Personalkosten extern: durchschnittlich 1.000 €/PT
5. Der Abschreibungszeitraum für Hardware und Software wird auf 5 Jahre festgelegt.
6. Der Betrachtungszeitraum ist auf 8 Jahre definiert von 2005-2012.
7. Eine Inflationsrate wird nicht explizit berücksichtigt (da sie sich auf Kosten und Nutzen gleichartig auswirkt).
8. Die Schätzungen zu Kosten und Nutzen basieren auf heutigen Preis- und Kostenangaben, marktbedingte Veränderungen während des Betrachtungs-

	zeitraums wurden nicht berücksichtigt.
9.	Die Betrachtung richtet sich auf Ist-Kosten.
10.	Prozessbezogene Produktivitätsveränderungen/-verbesserungen wurden nicht berücksichtigt.

5.3.2 Monetäre Analyse

Für die monetären Auswirkungen der Vorhaben wird die Kapitalwertmethode angewandt. Als dynamisches Verfahren beurteilt sie Investitionsprojekte nach ihrem Kapitalwert, d.h. durch wirklichkeitsnahe Erfassung der mit der Investition zusammenhängenden Finanzströme (Einnahmen und Ausgaben, haushaltswirksam und nicht haushaltswirksam), fokussiert auf einen gemeinsamen Bezugszeitpunkt. Einnahmen, Ausgaben und Ersparnisse, die mit dem Vorhaben zusammenhängen können für die Jahre der wirtschaftlichen Nutzungsdauer im Voraus geplant werden. Für die künftigen Werte wird der aktuelle Zeitwert durch Abzinsung mit dem vom Bundesministerium der Finanzen festgelegten Zinssatz ermittelt.

Hierfür stehen zwei Methoden zur Verfügung

- WiBe 4.0 (im Sinne § 7 BHO rechtlich belastbar)
  (siehe Kapitel 5.5)
- MiKoMa (im Sinne § 7 BHO rechtlich **nicht** belastbar)
  (siehe Kapitel 5.6)

5.3.3 Grundsätzliche Überlegungen zur Kostenerhebung

Nachfolgend werden grundsätzliche Überlegungen zur Erhebung der notwendigen Kosten durchgeführt. Dabei werden insbesondere die einzelnen Migrationsphasen und die damit verbundenen Maßnahmen sowie die Personalkosten und die Preisstrukturen der Anbieter in Augenschein genommen.

5.3.3.1 Migrationsphasen

Die Kosten für eine Migration lassen sich am besten identifizieren, wenn man sich ein Phasenmodell der Migration zugrunde legt und die mit den einzelnen Phasen verbundenen Maßnahmen definiert. Das Modell, das hier zugrunde gelegt wird, umfasst vier Hauptphasen (vgl. Bild 70, S.409):

- Qualifizierungsphase[1]
  - Workshops
    (Kick Off, betroffene Fachabteilungen und IT- Disziplinen beteiligen, Identifizieren aller relevanten Themen, Prioritäten setzen, Entschei-

[1] Die Wirtschaftlichkeitsbetrachtung begleitet dabei die gesamte Qualifzierungsphase

dungsbedarf identifizieren, Vorgehensweise und Projektplan festlegen, detaillierte Aufwandsschätzung, Teilprojekte festlegen und Arbeitsgruppen zuweisen)

- Ist-Aufnahme
  (Anwendungslandschaft, Kommunikationsbeziehungen, Netzwerkinfrastruktur, Zentrale Dienste, Betriebsverfahren, Zukünftige Anforderungen)
- Lösungsansätze/ Grob- und Feinkonzepte
  (Pflichtenheft erstellen, Projektplan verfeinern und Arbeitspakete definieren, Technische Machbarkeit, Aufbau einer Integrations- und Testumgebung, Abbildung der übrigen Produktionsumgebung, Anwendungsintegration, Hardware-Auswahl und Evaluierung)

❍ Entwicklungsphase

- Konzepte, Verfahren, Installationen
  (Detaillierte Festlegung des Funktionsumfangs, Integration in die übrige IT-Umgebung, Entwicklung der Installationsverfahren und Softwareverteilung, Integration in den Betrieb, Rollout-Planung, Pilotplanung, Ausbildung des DV-Personals)

❍ Pilot- / Testphase

- Erprobung von Verfahren und Überprüfung der Funktion von Installationen
  (Feature Stop, Repräsentative Benutzergruppe versorgen, Lasttests, Einbindung des UHD (User Help Desks), Erstmalige Sizing-Kontrolle, Rückkopplung in Feinkonzept)

❍ Roll-Out-Phase

- Bereitstellen von Funktionen im Netzwerk und Installationen in der Fläche
  (Inbetriebnahme der Installationsverfahren, Serversysteme vervielfältigen, Benutzerinformation und –Schulung, Begleitung durch Projektteam, Übergabe in den Regelbetrieb)

Qualifizierungsphase (Workshops, Lösungsansätze, Grob- und Feinkonzepte)	1	Feinkonzept / Pflichtenheft
	1	Migrationsplan Infrastruktur
	2	Migrationsplan Systemmanagement
	3	Migrationsplan Client
	4	Verabschiedung konsoliderter Migr.plan
Entwicklungsphase (Konzepte, Verfahren, Installationen)		Implementierung Basis Infrastruktur
	5	Infrastrukturdienste
	6	Systemmanagement
	7	GroupWare
	8	Terminalserver
	9	Design Desktop
		Paketierung für APC-Implementierung
	10	Installationsverfahren Desktop
	11	Migration Funktionen Systemmgmt.
	12	Paketierung: 1-2 Applikationen / 1MT
Pilot-/Testphase (Erprobung von Verfahren, Funktionstest von Installationen)	13	Pilotbetrieb 1 Monat / 20 - 50 Benutzer
	14	Testlauf Migrationsverfahren
	15	Dokumentation Migrationshandbuch
Roll-out (Funktionen im Netzwerk bereitstellen, Installationen in der Fläche)	16	Migration der Daten-/Rechte Strukturen
	17	Migration der Client Strukturen

Bild 70: Migrationsphasen

5.3.3.2 Personalbedarf für die Migration

Personalaufwand entsteht bei der Migration an den unterschiedlichsten Positionen. In Bild 70 sind die einzelnen Phasen in migrationstypische Aktivitäten untergliedert worden. Zu diesen Aktivitäten sind zusätzlich die Umstellung der Dokumente und Makros sowie Projektmanagement, Qualitätssicherung und vor allen Dingen die Anwenderbetreuung zu planen. Die nachfolgenden Tabellen geben einen Überblick über die prozentuale Verteilung der Personentage- und der Personalkosten-Planung[1]. In der Tab. 55 werden für drei Beispiel-Alternativen Anteile in den einzelnen Aktivitäten dargestellt[2]. In der nachfolgenden Tabelle werden diese Personalaufwendungen um die o. a. zusätzlichen Aktivitäten mit denen der Migrationsphasen zu einer Gesamtsicht zusammengeführt (vgl. Tab. 56).

Tab. 55: Prozentuelle Anteile der Personalaufwendungen in den Migrationsphasen

[1] Die hier abgebildeten Daten stehen beispielhaft für eine Behörde mit ca. 2.000 Anwendern.

[2] Zusammengehörige Zeilen summieren sich immer auf 100%; da die Anzeige keine Nachkommastellen enthält, werden aufgrund von Rundungsdifferenzen die 100% in manchen Fällen unter- oder überschritten.

Phase	Beschreibung	Variante 1 OSS Smart Client		Variante 2 Gemischt OSS Smart Client		Variante 3 Microsoft Terminal Server	
		intern	extern	intern	extern	intern	extern
Su Kosten Gesamt €		**100%**		**100%**		**100%**	
Su Kosten intern/extern €		**22%**	**78%**	**22%**	**78%**	**26%**	**74%**
Su Personentage (PT) Gesamt		**100%**		**100%**		**100%**	
Su Personentage (PT) intern/extern		**42%**	**58%**	**42%**	**58%**	**47%**	**53%**
Qualifizierungsphase		**28%**	**40%**	**33%**	**42%**	**24%**	**43%**
(Workshops,	Feinkonzept / Pflichtenheft	48%	25%	48%	28%	48%	25%
Lösungsansätze,	Migrationsplan Infrastruktur	16%	25%	16%	23%	16%	25%
Grob- und Feinkonzepte)	Migrationsplan Systemmanagement	16%	25%	16%	23%	16%	25%
	Migrationsplan Client	16%	25%	16%	23%	16%	25%
	Verabschiedung konsoliderter Migr.plan	3%	2%	3%	2%	3%	2%
Entwicklungsphase		**44%**	**41%**	**38%**	**39%**	**36%**	**35%**
(Konzepte,	Implementierung Basis Infrastruktur	**74%**	**78%**	**72%**	**77%**	**71%**	**77%**
Verfahren,	Infrastrukturdienste	21%	17%	16%	13%	23%	13%
Installationen)	Systemmanagement	28%	26%	20%	19%	31%	32%
	GroupWare	17%	16%	16%	16%	18%	16%
	Terminalserver	28%	36%	39%	45%	23%	39%
	Design Desktop	7%	5%	10%	6%	5%	0%
	Paketierung für APC-Implementierung	**26%**	**22%**	**28%**	**23%**	**29%**	**23%**
	Installationsverfahren Desktop	20%	26%	25%	30%	15%	30%
	Migration Funktionen Systemmgmt.	60%	56%	50%	48%	67%	48%
	Paketierung: 1-2 Applikationen / 1MT	20%	19%	25%	22%	19%	22%
Pilot-/Testphase		**18%**	**10%**	**21%**	**12%**	**16%**	**12%**
(Erprobung von Verfahren,	Pilotbetrieb 1 Monat / 20 - 50 Benutzer	63%	50%	63%	50%	63%	57%
Funktionstest von Installationen)	Testlauf Migrationsverfahren	25%	17%	25%	17%	25%	14%
	Dokumentation Migrationshandbuch	13%	33%	13%	33%	13%	29%
Roll-out (Funktionen im Netzwerk		**9%**	**10%**	**8%**	**8%**	**24%**	**10%**
bereitstellen, Installationen in der	Migration der Daten-/Rechte Strukturen	50%	67%	33%	50%	17%	67%
Fläche)	Migration der Client Strukturen	50%	33%	67%	50%	83%	33%

Tab. 56: Prozentueller Gesamtpersonalaufwand

Lösungen		Smart Client				Terminal Server	
Szenarien		1 OSS		2 Gemischt OSS		3 MS TS	
Personentage	Faktor	intern	extern	intern	extern	intern	extern
Su Kosten Gesamt €		100%		100%		100%	
Su Kosten intern/extern €		29%	71%	30%	70%	32%	68%
Su PT Gesamt		100%		100%		100%	
Su PT intern/extern		51%	49%	53%	47%	55%	45%
Migrationsphasen: Serveraufbau		27%	44%	24%	41%	25%	44%
Pilotierung/ Test		7%	5%	7%	6%	7%	7%
Client-Roll-Out		3%	5%	3%	4%	10%	6%
Dokumente/ Anwendungen		8%	9%	9%	10%	4%	5%
PM/ QS/ Anwenderbetreuung		55%	37%	57%	38%	54%	38%
- davon Projekt-Mgmt. (PM)	15,00%	12%	26%	11%	24%	13%	24%
- davon Qualitätssicherung (QS)	15,00%	12%	26%	11%	24%	13%	24%
- davonAnwenderbetreuung	0,00%	0%	0%	0%	0%	0%	0%
- davonAnwenderbetreuung[1)]	absolut	75%	48%	77%	52%	75%	52%

Für das Beispiel mit ca. 2000 Nutzern sind nachfolgend empirisch abgegriffene Minimal- und Maximalwerte für den Bedarf an internen und externen Personentagen dargestellt.

Bild 71: Bandbreite des Personaltagebedarfs in Prozent der Nutzer

5.3.3.3 Preisstrukturen der Anbieter

Einen weiteren wesentlichen Bereich stellen neben den Personalaufwenden die Kosten für Soft- und Hardware dar. Hier sind i. d. R. Preisinformationen bei den Herstellen / Lieferanten einzuholen. Diese Daten sollten für unterschiedliche Finanzierungsmodelle abgefragt werden. So kann es im Einzelfall zu spürbaren Unterschieden zwischen Kauf, Miete und Leasing kommen. Basis bilden generell die Preislisten der Anbieter. In jedem Fall sind für diese Informationen jedoch evtl. vorhandene Rahmenabkommen der Behörde mit den Anbietern zu verwenden. Auch zusätzlich spezielle Verhandlungen, die zu einer weiteren Reduzierung der Preisbasis führen, sind in der Wirtschaftlichkeitsbetrachtung zu berücksichtigen.

Da sich Migrationen grundsätzlich auf der Serverseite oder zusätzlich auch auf der Clientseite abspielen, wird die Erhebung der Preis-Informationen in diese beiden Bereiche gegliedert.

Server

In diesem Bereich wird folgende Struktur empfohlen (vgl. Tab. 66, S. 497):

Tab. 57: Erhebungsstruktur Preisinformationen Hard-/ Software "Server"

Server	
Software	
Infrastrukturdienste	Directory
	File
	Druck
	DNS/ DHCP/ BOOTP
Systemmanagement	Softwareverteilung

		Inventarisierung
		Help-Desk
		Systemüberwachung
		Netzwerküberwachung
	Groupware & Messaging	Groupware
		Mail
	Terminalserver	
Hardware		

APC

Auch auf der Seite der Arbeitsplatzrechner hat sich nachfolgende Strukturierung als hilfreich erwiesen (vgl. Tab. 66, S. 497):

Tab. 58: Erhebungsstruktur Preisinformationen Hard-/ Software "Arbeitsplatzcomputer"

Arbeitsplatzcomputer		
Software		
	Betriebssystem	Betriebssystem
	Standardsoftware	Dokumentenaustauschformat, PDF-Betrachter
		Webbrowser und Mailclient
		Büro
		Komprimierung
		Datenbank
		Tabellenkalkulation
		Präsentation
		Textverarbeitung
	Terminalserver (Client Zugriff)	
Hardware		

Diese Informationen sind wiederum in der Projektmatrix abzulegen, um sie der Berechnung der Wirtschaftlichkeit zugänglich zu machen.

5.3.4 Nutzwert-Analyse

Gilt es dagegen bei der Entscheidungsfindung nicht monetär erfassbare Auswirkungen mit einzubeziehen, steht nur die WiBe 4.0 zur Verfügung. Die Nutzwertanalyse der WiBe 4.0[1] bewertet einzeln und unabhängig voneinander gewichtete Zielkriterien, um sie anschließend zu einer Gesamtbewertung zusammenzufassen. Hier werden die so genannten "weichen" Faktoren über Bewertungsskalen quantifiziert.

Für die Ergebnisauswertung empfehlen wir in zwei Schritten vorzugehen:

1. Die Ergebnisse der monetären Wirtschaftlichkeitsbetrachtung haben Priorität. Hier werden Kosten und Ersparnisse der Vorhaben nach o.a. Methodik[2] in einer Rentabilitätskennzahl dargestellt, die sich in einem positiven Kapitalwert ausdrückt.
2. Die Ergebnisse der Nutzwertanalyse führen zu Kennzahlen für folgende Bereiche:
   - Dringlichkeit der IT-Maßnahme
   - Qualitativ-strategische Bedeutung der IT-Maßnahme
   - Externe Effekte der IT-Maßnahme

   Dieser zweite Schritt dient primär dem Fall, dass eine Wirtschaftlichkeitsbetrachtung nach monetären Gesichtspunkten grundsätzlich nicht ausreicht bzw. keine eindeutige Rentabilitätsaussage liefert. Aufgrund von Dringlichkeits-, Strategiekriterien oder Kriterien externer Effekte kann das Projekt stets unabhängig von monetären Kriterien eine hohe Priorität zur Durchführung erhalten.

Die Methodik der Nutzwertanalyse ist ausführlich in den Unterlagen der WiBe 4.0 beschrieben und wird aus diesen Gründen hier nicht mehr aufgeführt.

5.3.5 Vollkostenansatz

In der Wirtschaftlichkeitsbetrachtung ist grundsätzlich der Vollkostenansatz zu verwenden; d.h. alle unmittelbar und mittelbar monetär quantifizierbaren Kosten und Nutzen sind dem IT-Vorhaben zuzuordnen. Daraus ergibt sich die Erfordernis auch die nicht haushaltswirksamen[3] Kosten zu berücksichtigen.

Der TCO-Ansatz beinhaltet so genannte "Opportunitätskosten". Darunter werden fiktive Kostenanteile verstanden, die entsprechenden Folgewirkungen eines IT-

---

1 Vgl. WiBe 4.0, Empfehlung zur Durchführung von Wirtschaftlichkeitsbetrachtungen in der Bundesverwaltung, insbesondere beim Einsatz der IT, Version 4.0 – 2004, S. 80 ff

2 Vgl. die Kapitel zur WiBe 4.0 und zur Migrationskostenmatrix (MiKoMa) 2.0

3 Haushaltswirksame Kosten und Nutzen entstehen erst aufgrund des betrachteten Vorhabens und führen im kommenden Haushaltsplan zu Mehr- oder Minderbeantragungen. Nicht haushaltswirksame Kosten und Nutzen entstehen auch ohne das betrachtete Vorhaben in gleicher Höhe.

Systems oder einer IT-Landschaft gegenüberstehen. Konkret werden Kosten für nachfolgende Umstände ermittelt: "Downtime" des Systems, Eigenkonfiguration und Selbsttraining sowie Fehlerdiagnose und –analyse. Werden die hinter diesen Umständen stehenden Defizite des Altsystems mit dem IT-Vorhaben abgestellt, so können die hierfür ermittelten opportunen Kostenanteile bei der Betrachtung der Wirtschaftlichkeit als Ersparnis eingestellt werden.

Da eine solche Betrachtung aber in der Regel erst eine Prozessanalyse liefern kann, wird sich bei den Ersparnissen das Augenmerk eher auf konkrete Größen richten, wie z. B. nicht mehr benötigte Betriebskosten. Entfällt z. B. durch die Migration ein noch nicht aus der steuerlichen Abschreibungszeit hinausgelaufenes Hardwaresystem, so können dafür die noch ausstehenden Abschreibungen der restlichen geplanten Nutzungsjahre ebenfalls als Ersparnis angesetzt werden. Voraussetzung dafür ist jedoch, dass das Altsystem entweder umgenutzt (durch andere Abteilung oder Behörde) oder veräußert werden kann.

5.3.6 Vergleichbarkeit

Um Vergleichbarkeit der verschiedenen Auswertungen zu gewährleisten, wird die Wirtschaftlichkeitsbetrachtung in zwei Szenarien durchgeführt:

- **die Migration einzelner oder mehrerer Migrationsobjekte**[1] **(Teilmigration)**, bei klar abgrenzbaren Produkten oder Produktgruppen[2]
- **die Gesamtmigration, d.h. Migration einer kompletten DV-Umgebung -** Server, Clients, Infrastruktur, Fachanwendungen

Unter Migration sind generell zwei Möglichkeiten zu verstehen:

- Ablösende Migration – als Migration in eine komplett neue, Open Source basierte Software-Umgebung, unter Einsatz der Open Source Software (OSS) und/oder Commercial Linux Software (COLS) oder
- Fortführende Migration – als Migration im Rahmen der eingesetzten Produkte auf neue Versionen derselben

Für die Migration von Migrations-Objekten sowie bei einer Gesamt-Migration sind die allgemeinen Bewertungskriterien[3] der WiBe 4.0 anzuwenden. Da in letzterem Fall oftmals auch Fachanwendungen mit umzustellen sind, werden in der Regel neben reinen Umstellungsaktivitäten für Standardprodukte auch Entwicklungsarbeiten für die spezifischen Anwendungen anfallen.

Ein weiterer Aspekt wird dadurch hinzugefügt, dass vergleichende Wirtschaftlichkeitsanalyse nur bei technisch und funktional vergleichbaren Alternativen Sinn

---

[1] Siehe hierzu im Kapitel Vorgehensweise die Abgrenzung der Objekte.

[2] . B. Desktop-Anwendungen als Migrationsobjekte mit Textverarbeitung, Tabellenkalkulation, Grafik und Internetbrowser als Produkte.

[3] Vgl. WiBe 4.0, Empfehlung zur Durchführung von Wirtschaftlichkeitsbetrachtungen in der Bundesverwaltung, insbesondere beim Einsatz der IT, Version 4.0 – 2004, S. 71 ff

macht. Als vergleichbar im Sinne des Migrationsleitfadens können folgende Einsatzbereiche der OSS- und Microsoft-Technologie erachtet werden:

- Infrastruktur-Dienste
  - File-Server
  - Print-Server
  - Anmeldungs-Server
  - Netzwerke
- Messaging- und Groupware-Systeme
- Office-Pakete
- Datenbank- und Web-Anwendungsserver

5.3.7 Einsatzbereiche

Um ein aussagekräftiges Ergebnis zu erhalten wird die Analyse in einem aus mehreren Einsatzbereichen bestehenden Gesamtkontext durchgeführt. Die Gesamtbetrachtung der zu untersuchenden Kosten umfasst dabei folgende Einsatzfelder:

- Server-Infrastruktur
  - Datei-Dienste
  - Druck-Dienste
  - Anmeldedienste
  - Netzwerkdienste
- Desktop-Infrastruktur
  - Office
  - Web
- Messaging/Groupware
- DB- und Web-Anwendungen

Obwohl sicherlich nicht vollständig, bildet diese Aufzählung einen gemeinsamen Nenner für die meisten Infrastruktur-Bereiche der Behörden.

Die Migration der IT-Fachverfahren stellt unterschiedliche Anforderungen an Organisationseinheit und die Dienstleister/ Lieferanten der Software.

Werden die IT-Fachverfahren in verschiedene Technik-Cluster gegliedert (Terminal, Web, Dos, MS Access, Makros, Standalone), so bilden sich drei Risikoklassen für die Migration heraus (vgl. Tab. 59).

1. Einfache Migration möglich

2. Mittlerer Schwierigkeitsgrad; Migrationsweg variabel, Emulation, Terminal Server, Ablösung
3. Migration schwierig; in der Regel durch Hersteller

Die zu analysierenden Fachverfahren können entsprechend der Informationserhebung und auf Basis der Migrationsmatrix beispielhaft wie folgt beurteilt werden:

Tab. 59: Portierungsgruppen

Typ	Risiko	Migrationsszenario
Terminal	i.d.R. vernachlässigbar	nicht zutreffend
Web	i.d.R. browserabhängig	z.T. Standard-Konformität herstellen
DOS	Einfacher Schwierigkeitsgrad	z.B. Dos-Emulation, Terminalserver und Ablösung
MS Access	Mittler bis hoher Schwierigkeitsgrad möglich; vornehmliche Risikobereiche: hohe Anzahl, keine Dokumentation, kein Hersteller, kaum Akzeptanz	z.B.: Neuentwicklung durch Entwickler (ggf. Web, Access2WEB), Emulation (WINE),Terminalserver, Ablösung
Sonstiges (Vorlagen, Makros, Formulare)	Alle Schwierigkeitsgrade möglich, abhängig von Situation, vornehmliche Risikobereiche: Anzahl und Komplexität der Makros	z.B.: Beibehaltung der Office-Anwendungen durch Emulation, Portierung nach OpenOffice.org, Ablösung
C/S	Migration i.d.R. schwierig Portierung nur durch Hersteller möglich	Portierung durch Hersteller, Möglichkeiten: Web, Emulation, Terminalserver, Ablösung
Stand Alone	Migration i.d.R. schwierig Portierung nur durch Hersteller möglich	Portierung durch Hersteller, Möglichkeiten: Web, Emulation, Terminalserver, Ablösung

5.4 Analyse der Ausgangssituation

Die Analyse der Ausgangssituation beschäftigt sich zum einen mit der hardwaretechnischen Infrastruktur (Server, APC, Netzwerk und Druck) und andererseits mit den vorhandenen Softwarediensten und -systemen zum Betrieb der IT-Landschaft und zur Unterstützung der Geschäftsprozesse. Zur Erhebung hat sich folgende Struktur in verschiedenen Projekten bewährt:

- Infrastruktur Server
- Infrastruktur APC

- Infrastruktur Netz
- Infrastruktur Druck
- Serverdienste
- Standardsoftware
- Office
- IT-Fachverfahren
- Dokumentvorlagen

5.4.1 Infrastruktur Server

Die Datenerhebung für die eingesetzten Server soll Aufschluss darüber geben, ob mit dem vorhandenen Material eine Migration bewerkstelligt werden kann, oder ob auch hier neue Hardware benötigt wird. Folgende Informationen (vgl. Bild 72) sind erforderlich: Dienst/ Einsatz, Distribution, Version, Erstinstallation, Anzahl gesamt, Alter (< 1 Jahr, 1 – 3 Jahre, > 3 Jahre), Investitionskosten, Anmerkungen.

RZ - Infrastruktur
- Server

Name	Dienst/ Einsatz	Distribution	Version	Erstinstallation	Anzahl Gesamt	Alter			Invest. Kosten	Anmerkungen
						< 1Jahr	1 - 3 Jahre	> 3 Jahre		
	Verwendung									
Server 1	http	Debian	x.y	1998						
Server2	http	Debian	x.y	1998						
Server 3	bootp, NFS	Suse	9.0	III/2003						
Server 4	http (eGroupware)	Suse	9.0	III/2003						

Bild 72: Beispiel Erhebungsbogen "Infrastruktur der Server"

5.4.2 Infrastruktur APC

Die existenten Clients befinden sich in vielen Fällen nicht auf einem einheitlichen Niveau. Beispielsweise werden neben Rechnern mit aktuellen Systemumgebungen auch Geräte mit einem Alter von bis zu 8 Jahren (und den entsprechend alten Systemumgebungen) eingesetzt. Da bestimmte Migrationsszenarien in diesem Bereich enorme Auswirkungen haben (z.B. muss für neue Microsoft-Produkte neue Hardware beschafft werden, da diese auf älteren Systemumgebungen nicht laufen), kommt den hier zu erhebenden Informationen recht große Bedeutung zu.

Die vorhandenen Clients können nun – wenn das nicht bereits schon geschehen ist – in Gruppen zusammengefasst werden. In manchen Fällen wurde dies schon im Rahmen einer Inventarisierung und der Aufnahme der Informationen in eine Anlagenbuchhaltung durchgeführt. Ist dies nicht der Fall, so können sinnvolle Gruppen für die Clients gebildet werden, die sich vornehmlich an Majoritäten der

zu erhebenden Informationen (vgl. Bild 73) ausrichten können. Diese sind folgendermaßen strukturiert: Betriebssystem, Anzahl Arbeitsplatzcomputer (APC) im Netz, zentrale Installation, zentrale Administration, Leistungsfähigkeit (z.B.: Alter > 5 - 8 Jahre, Prozessor < 100 MHz, Memory < 32MB; Alter > 3 - 5 Jahre, Prozessor 100-400 MHz, Memory < 64MB; Alter > 2 - 3 Jahre, Prozessor 400 - 700 MHz, Memory 64 - 128 MB; Alter bis zu 2 Jahre, Prozessor > 700 MHz, Memory > 128MB), Eingabehilfen und Anmerkungen

RZ - Infrastruktur
- Arbeitsplatzrechner

Erhebungs-bereich	Bezeichnung	Betriebs-system	Anzahl APCs im Netz	Zentrale Installation	Zentrale Adminis-tration	Leistungsfähigkeit: Alter 8 Jahre, Prozessor < 100 MHz, Memory < 32MB	Leistungsfähigkeit: Alter 5 Jahre, Prozessor 100-400 MHz, Memory < 64MB	Leistungsfähigkeit: Alter 3 Jahre, Prozessor 400 - 700 MHz, Memory 64 - 128 MB	Leistungsfähigkeit: Alter 2 Jahre, Prozessor > 700 MHz, Memory > 128MB	Eingabe-hilfen	Anmerkungen
	Summen		3.800		3.300	500	800	1.000	1.000		
	APC-Kat. 1	Win NT	500	x	500	500					
	APC-Kat. 2	Win NT	800	x	800		800				
	APC-Kat. 3	Win NT	1.000	x	1.000			1.000			
	APC-Kat. 4	Win NT	1.000	x	1.000				1.000		
	Einzelplatz-PC	Win NT,2000, XP, DOS, sonstige	500								

Bild 73: Beispiel Erhebungsbogen "Infrastruktur der Arbeitsplatz-Computer"

5.4.3 Infrastruktur Netzwerk

Die vorhandene Netzwerkausstattung (vgl. Bild 74) stellt die Basis für die Zusammenarbeit der APCs mit den Servern dar. Zur Definition von Migrationsszenarien stellt dieser Bereich eine nicht zu vernachlässigende Größe dar.

- Netzausstattung
  - - Ethernet
  - - ATM
  - - Tokenring
- Geschwindigkeit
- Router
- Switches

RZ - Infrastruktur
- Netzwerk

Erhebungsbereich	Anzahl eingesetzte Systeme	Betriebs-System	eingesetztes Produkt	Hersteller	Anzahl Lizenzen	Anzahl Clients	Schnittstellen zu Office-Anwendungen	Anmerkungen
Netzwerkinfrastruktur								
Netzausstattung								
- Ethernet								
- ATM								
- Tokenring								
Geschwindigkeit								
Router								
Switches								

Bild 74: Beispiel Erhebungsbogen "Infrastruktur des Netzwerks"

5.4.4 Infrastruktur Druck

Drucker ergänzen die Informationen zu der bisher erhobenen Hardware. Manche Softwareprodukte sind nicht mit allen Druckertypen kompatibel. Daher ist zur Verifizierung möglicher Migrationsszenarien auch deren Erhebung notwendig. Folgende Daten (vgl. Bild 75) sind zu ermitteln: Anzahl gesamt, Alter (< 1 Jahr, 1 – 3 Jahre, > 3 Jahre), Investitionskosten, Anmerkungen.

RZ - Infrastruktur
- Drucker

Erhebungs-bereich	Bezeichnung	Anzahl Gesamt	Alter < 1Jahr	Alter 1 - 3 Jahre	Alter > 3 Jahre	Invest. Kosten	Anmerkungen
Netzwerkdrucker							
Faxgeräte							
Netzwerkarten							
Grafikkarten							
Beschleunigung							
Scanner							
Arbeitsplatzdrucker							
Aufstellung der Treiber für Arbeitsplatzdrucker							

Bild 75: Beispiel Erhebungsbogen "Drucker-Infrastruktur"

5.4.5 Serverdienste

In diesem Bereich werden die zentralen auf Servern im Rechenzentrum verfügbaren Dienste erhoben – z.B.:

- Infrastrukturdienste
  - Dateiablage (File-Server)
  - Druckdienste (Print-Server)
  - Netzwerkdienste
    - DNS
    - DHCP
    - WINS
    - RAS
    - VPN
    - BOOTP
  - Authentisierungsdienste
- System und Managementdienste
  - Softwareverteilung
  - System- und Netzwerküberwachung

- Datensicherungssysteme
- Verzeichnisdienste
  - NDS
  - OpenLDAP
- Messaging und Groupware
- Terminalserver
- Dokumentenmanagementsysteme

Die Erhebung wird in folgende Bestandteile (vgl. Bild 76) gegliedert: Anzahl eingesetzte Systeme, Betriebssystem, eingesetztes Produkt, Hersteller, Anzahl Lizenzen, Anzahl Clients, Schnittstellen zu Office-Anwendungen, Anmerkungen.

RZ - Infrastruktur
- Zentrale Serverdienste

Erhebungsbereich	Anzahl eingesetzte Systeme	Betriebs-System	eingesetztes Produkt	Hersteller	Anzahl Lizenzen	Anzahl Clients	Schnittstellen zu Office-Anwendungen	Anmerkungen
Infrastrukturdienste								
Dateiablage (File-Server)								
Druckdienste (Print-Server)								
Netzwerkdienste								
- DNS								
- DHCP								
- WINS								
- RAS								
- VPN								
- BOOTP								
…								
…								
Authentisierungsdienste								
System- und Managementdienste								
Softwareverteilung								
System- und Netzwerküberwachung								
Datensicherungssysteme								
Verzeichnisdienste								
NDS								
OpenLDAP								
Messaging & Groupware								
eGroupware								
Terminalserver								
Dokumentenmanagementsysteme								

Bild 76: Beispiel Erhebungsbogen "Erhebungsbogen für Serverinfrastrukturdienste"

5.4.6 Standardsoftware

Standardsoftware stellt häufig einen erheblichen Anteil an den Softwarelizenzen dar. Die eingesetzten bzw. lizenzierten Produkte werden in folgender Strukturierung (vgl. Bild 77) erhoben: Hersteller, Verwendungszweck, Lizenzen (Anzahl heute, künftig benötigt), Kosten heute und künftig (Lizenzen und Insurance), Anmerkungen.

Standard-Software

Name	Version	Hersteller	Verwendungs-Zweck	Lizenzen		Kosten heute		Kosten künftig		Anmerkungen
				Anzahl heute	künftig benötigt	Lizenzen	Insurance	Lizenzen	Insurance	
Acrobat Reader	5	Adobe								
Mozilla	1.6	Mozilla								
Open Office	1.1	OpenOffice.org								
Outlook	2000	Microsoft								
WinZip	8.1	WinZip								
Access	97	Microsoft								
Excel	97	Microsoft								
Powerpoint	97	Microsoft								
Word	97	Microsoft								

Bild 77: Beispiel Erhebungsbogen "Standardsoftware"

5.4.7 Dokumentvorlagen und Makros

Ein sehr wesentlicher Faktor für die Migrationsaufwände stellen die umzustellenden Dokumentvorlagen (z.B. in der Textverarbeitung, der Tabellenkalkulation, etc.) und Makros dar. Hier baut die Praxis bei der Erhebung oftmals recht große Hürden auf – in vielen Fällen existieren keine Übersichten über diese Dokumente. Dies betrifft neben den serverbasierten Dateien vor allem die, die auf den Arbeitsplatzrechnern der Anwender liegen.

In Abhängigkeit der Güte und Akzeptanz eventuell vorhandener Standard-Verfahren für Prozessunterstützung nutzen die Anwender diese oder haben sich eben auf ihren Rechnern eigene Anwendungen (je nach Programmierkenntnissen) erstellt.

Soll die Migration für die gesamte Behörde zu einem Erfolg werden und vor allen Dingen von den Anwendern vor Ort akzeptiert werden, so ist es unerlässlich, diesen Bereich "in den Griff" zu bekommen. Das bedeutet, dass ernsthafte Versuche unternommen werden sollten, die Dokumentvorlagen und Makros zu erheben und in nachfolgend vorgeschlagene Klassifizierung (vgl.

Bild 78 S. 422) einzuordnen.

Tab. 60: Klassifizierung von Dokumentvorlagen und Makros

Dokumente	Klassifizierung
Dokumentvorlagen:	geringe Komplexität, Erstellung < 0,5 Tage
	mittlere Komplexität, Erstellung 0,5-2 Tage
	hohe Komplexität, Erstellung 2-4 Tage sehr hohe Komplexität, Erstellung > 4 Tage
	sehr hohe Komplexität, Erstellung > 4 Tage
Makros	geringe Komplexität, Erstellung < 0,5 Tage
	mittlere Komplexität, Erstellung 0,5-2 Tage

Dokumente	Klassifizierung
	hohe Komplexität, Erstellung 2-4 Tage sehr hohe Komplexität, Erstellung > 4 Tage
	sehr hohe Komplexität, Erstellung > 4 Tage

Office
- Dokumentvorlagen und Makros

Erhebungsbereich	Dokumentvorlagen				Makroanwendungen				Anmerkungen
	geringe Komplexität, Erstellung < 0,5 Tage	mittlere Komplexität, Erstellung 0,5-2 Tage	hohe Komplexität, Erstellung 2-4 Tage	sehr hohe Komplexität, Erstellung > 4 Tage	geringe Komplexität, Erstellung < 0,5 Tage	mittlere Komplexität, Erstellung 0,5-2 Tage	hohe Komplexität, Erstellung 2-4 Tage	sehr hohe Komplexität, Erstellung > 4 Tage	
Summen									
Word									
Excel									
PowerPoint									
Access									
Unverzichtbare, produktive ...									

Bild 78: Beispiel Erhebungsbogen "Office"

5.4.8 IT-Fachverfahren

Für die Fachverfahren treffen die gleichen Einschätzungen zu wie für die Dokumentvorlagen und Makros. Diese Verfahren sollen die tägliche Arbeit der Anwender unterstützen. Bietet die Migration die Chance, diese in manchen Punkten zu verbessern (wenn z.B. neu oder umprogrammiert werden muss), so wird sich automatisch eine Akzeptanz der Anwender einstellen. Andernfalls muss nach der Migration mindestens der vorhandene Standard wieder hergestellt werden. Die Fachverfahren sollten in folgenden Informationsclustern aufgenommen werden:

Tab. 61: Informationscluster für die Erhebung der IT-Fachverfahren

Architektur	Nutzer	Client-/ Serverbetriebssysteme
Datenbanksysteme	Applikationsserver	Benutzerverwaltung
Rechteverwaltung	Schnittstellen	Hosting
Verfahrensentwicklung	Ausprägung	Ausblick
Kosten	Anmerkungen	

Architektur und Nutzer

Bei der Architektur sollte nach einschichtig und 2 bis n-schichtig unterschieden werden. Als Erhebungskriterien bei einer 2- und mehrschichtigen Architektur kommen in Frage: Client-Sever, Terminal, Host und Web.

Die Erhebung der Nutzer je IT-Fachanwendung liefert Informationen zur Verbreitung der Anwendung. Die Anzahl der Nutzer bezogen auf deren Gesamtheit hilft, die Anwendungen zu priorisieren. An dieser Stelle sind auch wieder die Ziele und

die Rahmenbedingungen zu berücksichtigen. Es kann durchaus sein, dass Anwendungen, die nur von sehr wenigen Mitarbeitern genutzt werden, trotzdem einen hohen strategischen Wert haben und somit automatisch zu priorisieren sind. Im Erhebungsbereich der Nutzer sollten Angaben erfragt werden, zum Einsatzbereich der Anwendung in der Behörde, zu der Gesamtzahl der Nutzer je Anwendung, zu Anzahl der Nutzer in den einzelnen Abteilungen und ob die Anwendung abteilungsübergreifend im Einsatz ist. (Vgl. zu beiden Bereichen Bild 79, S.423)

IT-Fachverfahren

Bezeichnung	Architektur					Nutzer														
		2-/ n-schichtig					Einsatz-bereiche													
Produkt-Name	1-schichtig	Client-Server	Terminal	Host	Web	Gesamt Anzahl	Abteilungen	Abteilung 01	Abteilung 02	Abteilung 03	Abteilung 04	Abteilung 05	Anzahl	Fachbereich	Anzahl	abteilungsübergreifend	Anzahl	...	Anzahl	...	Anzahl

Bild 79: Beispiel Erhebungsbogen "IT-Fachverfahren – Architektur und Nutzer"

Client-/ Serverbetriebssysteme, Datenbanksysteme und Applikationsserver

An dieser Stelle sollen die Betriebssysteme , Datenbanken und Applikationsserver erhoben und ermittelt werden, unter welchem Betriebssystem-Produkt/ -Version das jeweilige IT-Verfahren laufen kann bzw. im Hause eingesetzt wird.

Hierfür bietet sich die Gliederung in folgende zurzeit verbreitete Betriebsystemumgebungen(vgl. Bild 80) an: Windows NT, Windows 2000/ 2003/ XP, Linus und Unix.

IT-Fachverfahren

Bezeichnung	Client-Betriebssystem(e)								Server-Betriebssystem(e)												Datenbanksysteme								Applikationsserver							
	eingesetzt				verfügbar				eingesetzt					verfügbar					eingesetzt				verfügbar				eingesetzt				verfügbar			
Produkt-Name	WinNT	Win 2000/ 2003/ XP	Linux	Unix	WinNT	Win 2000/ 2003/ XP	Linux	Unix	WinNT	Win 2000/ 2003/ XP	Linux	Unix	Netware	WinNT	Win 2000/ 2003/ XP	Linux	Unix	Netware	WinNT	Win 2000/ 2003/ XP	Linux	Unix	WinNT	Win 2000/ 2003/ XP	Linux	Unix	WinNT	Win 2000/ 2003/ XP	Linux	Unix	WinNT	Win 2000/ 2003/ XP	Linux	Unix

Bild 80: Beispiel Erhebungsbogen "IT-Fachverfahren – Client-/ Serverbetriebssysteme, Datenbanksysteme und Applikationsserver"

Benutzer-/ Rechteverwaltung und Schnittstellen

Für die Benutzer- und Rechteverwaltung (vgl. Bild 81, S. 424) soll ermittelt werden, ob sie innerhalb der Anwendung, einen Verzeichnisdienst oder sonstig erfolgt.

Schnittstellen können existieren zu: anderen IT-Verfahren, Standard-Software, Dokumentvorlagen und Makros. Bei letzteren stellt sich die Frage nach der Komplexität der Applikation, daher gibt es folgende Eingruppierungsmöglichkeit: geringe Komplexität, Erstellung < 0,5 Tage; mittlere Komplexität, Erstellung 0,5-2 Tage; hohe Komplexität, Erstellung 2-4 Tage; sehr hohe Komplexität, Erstellung > 4 Tage.

IT-Fachverfahren																
Bezeichnung	Benutzer-Vw			Rechte-Vw			Schnittstellen									
							zu anderen IT-Verfahren	zu Standard-Software	zu Dokumentvorlagen				zu Makros			
Produkt-Name	innerhalb der Anwendung	über Verzeichnisdienst	sonstiges	innerhalb der Anwendung	über Verzeichnisdienst	sonstiges	Name des Verfahrens	Name des Verfahrens	geringe Komplexität, Erstellung < 0,5 Tage	mittlere Komplexität, Erstellung 0,5-2 Tage	hohe Komplexität, Erstellung 2-4 Tage	sehr hohe Komplexität, Erstellung > 4 Tage	geringe Komplexität, Erstellung < 0,5 Tage	mittlere Komplexität, Erstellung 0,5-2 Tage	hohe Komplexität, Erstellung 2-4 Tage	sehr hohe Komplexität, Erstellung > 4 Tage

Bild 81: Beispiel Erhebungsbogen "IT-Fachverfahren – Benutzer-/ Rechteverwaltung und Schnittstellen"

Hosting, Verfahrensentwicklung und Ausprägung

Für nicht eigene IT-Verfahren ist es wichtig die Verfahrensverantwortung und die Verfahrensbetreiber (Hosting durch externe Firma, externe(r) Abteilung/ Bereich, eigene IT-Abteilung) zu kennen.

Die Verfahrensentwicklung (vgl. Bild 82, S. 425) soll Aufschluss über den Kostenrahmen des Verfahrens geben. Hier stellen sich folgende Fragen: handelt es sich um eine Eigen- oder Fremdentwicklung, wie hoch gestaltete sich der Aufwand der Entwicklung in internen und externen Personentagen und den entsprechenden Kosten, wie heißt das Produkt (Name und Version) und durch wen (Firma, Abteilung) kann Support geliefert werden.

Für eine eventuelle Neuprogrammierung im Rahmen der Migration sind folgende Ausprägungsinformationen von Bedeutung: Komplexität, Anforderungen an die Verfügbarkeit und Betreuungsaufwand (jeweils in den Stufen hoch mittel gering).

IT-Fachverfahren

Bezeichnung	Verfahrens-Verantwortung	Hosting				Verfahrens-Entwicklung						Ausprägungen								
		Verfahrens-Betreiber				Art	Aufwand			Entwicklungs-Umgebung		Komplexität			Anforderung Verfügbarkeit			Betreuungs-Aufwand		
Produkt-Name		Betreiber A	Betreiber B	Betreiber C	selbst	e = eigen, f = fremd	Kosten	Tage intern	Tage extern	Produktname, Version	Support durch:	Hoch	Mittel	Gering	Hoch	Mittel	Gering	Hoch	Mittel	Gering

Bild 82: Beispiel Erhebungsbogen "IT-Fachverfahren – Hosting, Verfahrensentwicklung und Ausprägung"

Ausblick, Kosten und Anmerkungen

Mit dem Ausblick (vgl. Bild 83) sollen Informationen zur Zukunft des Verfahrens erhoben werden, z.B. wird es eingestellt, fortgeschrieben oder abgelöst durch ein anderes Produkt. Bei Verfahren, die zurzeit noch nicht unter Linux verfügbar sind, wird die geplante Linux-Verfügbarkeit abgefragt. Auch die Plattformunabhängigkeit und seit neuestem auch die SAGA-Konformität stellen in diesem Zusammenhang wichtige Kriterien dar.

Im Bereich der Kosten wird der jährliche Aufwand für folgende Kostenarten erhoben: interne und externe Betreuung, Lizenzen (aus internen Umlagen und/ oder externen Lizenzen), Miete Wartung, Schulung, sonstiges.

IT-Fachverfahren

Bezeichnung	Ausblick					Kosten								Anmerkungen
						Betreuung		Lizenzen						
Produkt-Name	Fortschreibung	Ablösung	Einstellung	Linux-Verfügbarkeit	Plattform-Unabhängigkeit	Intern in Euro/Jahr	Extern in Euro/Jahr	interne Umlagen	externe Lizenzen	Miete	Wartung	Schulung	Sonstiges	

Bild 83: Beispiel Erhebungsbogen "IT-Fachverfahren – Ausblick, Kosten und Anmerkungen"

5.5 Wirtschaftlichkeit nach WiBe

5.5.1 Überblick

Die **WiBe 4.0** ist die aktualisierte Version der von der KBSt herausgegebene Methodik[1] zur Ermittlung der Wirtschaftlichkeit von IT-Maßnahmen. Zuerst kommen die monetären Daten zum Tragen, d.h. Aufwendungen und Erträge bzw. Ersparnisse werden zu einem Projektnutzen saldiert und letztendlich ein diskontierter Kapitalwert errechnet. Ist der Kapitalwert positiv (d.h. die Ersparnisse (oder Erträge) sind größer als die Aufwendungen), so ergibt sich daraus eine Empfehlung für die Durchführung der IT-Maßnahme[2]. Zur Risikoabsicherung der künftigen Planwerte beinhaltet die WiBe 4.0 die Möglichkeit Risikofaktoren für die einzelnen Kriterien zu benennen, die den Kapitalwert letztendlich reduzieren. Lässt sich im Monetären Bereich keine Wirtschaftlichkeit darstellen (Aufwendungen sind größer als die Ersparnisse), so verfügt dieses Tool über drei ergänzende Bereiche, eine erweiterte Wirtschaftlichkeit zu ermitteln. Dazu zählen Dringlichkeitskriterien, Qualitativ-strategische Kriterien und solche zur Ablösedringlichkeit aus der Perspektive des externen Kunden. Diese Kriterien werden in Form von Nutzwertanalysen bearbeitet, die für jeden der drei Bereiche einen Punktwert zwischen 0 und 100 als Ergebnis liefern. Im Fall eines negativen Kapitalwertes der IT-Maßnahme kann mit Punktwerten größer 50 die Durchführung der IT-Maßnahme befürwortet werden[3].

5.5.2 Monetäre Wirtschaftlichkeit

5.5.2.1 Systematik

In der Bundesverwaltung richten sich Wirtschaftlichkeitsbetrachtungen nach den Vorschriften des § 7 der BHO und nach den hierzu erlassenen Verwaltungsvorschriften, die seit 1995 vor allem betriebswirtschaftliche Verfahren berücksichtigen. Um diese Vorschriften auf die speziellen Erfordernisse der Informationstechnik anzupassen, hat die Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung (KBSt) bereits in 1992 eine Handlungsanweisung mit dem Titel „Empfehlung zur Durchführung von Wirtschaftlichkeitsbetrachtungen beim Einsatz der IT in der Bundesverwaltung (IT-WiBe)“ erarbeitet. 2004 ist sie in einer völlig überarbeiteten Fassung erschienen. Im Wesentlichen beinhaltet die IT-WiBe drei Schritte:

- Einflussgrößen festlegen (Kriterien selektieren)

---

1 Die WiBe wurde ausgearbeitet von Dr. Peter Röthig, Organisations- und Personalberatung, D-35096 Weimar/Lahn und in der aktuell vorliegenden Version 4.0 überarbeitet durch Dipl. Kfm. Knut Bergmann und Dipl. Kfm. Christian Müller, D-12623 Berlin, kontakt@institut-puma.de

2 Vgl. WiBe 4.0, Empfehlung zur Durchführung von Wirtschaftlichkeitsbetrachtungen in der Bundesverwaltung, insbesondere beim Einsatz der IT, Version 4.0 – 2004, S. 71 ff

3 Vgl. WiBe 4.0, Empfehlung zur Durchführung von Wirtschaftlichkeitsbetrachtungen in der Bundesverwaltung, insbesondere beim Einsatz der IT, Version 4.0 – 2004, "Berechnung der erweiterten Wirtschaftlichkeit", S. 80 ff

- Daten erheben/ bewerten
- Kennzahlen ermitteln

Bild 84: Methodik WiBe 4.0

Eine ausführliche Beschreibung der Methodik und der Anwendung dieser Methode ist der überarbeiteten WiBe 4.0 "Empfehlung zur Durchführung von Wirtschaftlichkeitsuntersuchungen in der Bundesverwaltung insbesondere beim Einsatz der IT[1]" zu entnehmen. Dies empfehlen wir umso mehr, als in der nachfolgenden Erörterung der Kriterien die spezifische Beschreibung nicht mehr mitgeliefert wird. Dort wird unter dem besonderen Gesichtspunkt der Migrationsvorhaben auf die monetären Kriterien eingegangen. Die Erläuterungen sind als Ergänzung zu den Ausführungen in der Beschreibung der Methodik zu verstehen.

Einen Gesamtüberblick der monetären Kriterien sowie die Zuordnung der Kosten/ Nutzen zu den Bereichen „haushaltswirksam“ und „nicht haushaltswirksam“ liefern die Tabellen Tab. 64 und

[1] Vgl. WiBe 4.0, Schriftenreihe der KBSt, ISSN 0179-7263, Band 68, August 2004

Tab. 65 im Anhang.

Behörden sind grundsätzlich nicht vorsteuerabzugsberechtigt, so dass alle Werte in der WiBe brutto, d.h. inklusiv Mehrwertsteuer zu berechnen sind.

WiBe-Kriteriengruppe 1
Entwicklungskosten/Einführungskosten und Entwicklungsnutzen

WiBe-Kriteriengruppe 1.1
Entwicklungs-/Einführungskosten für das neue IT-Verfahren

WiBe-Kriteriengruppe 1.1.1
Planungs- und Einführungs-/ Entwicklungskosten

WiBe-Kriterium 1.1.1.1 Personalkosten (eigenes Personal)

Darstellung von Kosten *nicht haushaltswirksam*

Aufwände, die im Rahmen der Projektphasen (vgl. Kapitel 5.3.3.1 und Kapitel 5.3.3.2) für das eigene Personal entstehen.

Ein Projektplan in der Struktur der Migrationsphasen sowie deren Einzelaktivitäten erleichtert die Aufwandskalkulation (vgl. Bild 15, Tab 6 und 7). Die Aufwände sollten der einfachen Zuordnung halber getrennt nach Vergütungsgruppen geplant werden. Dies erscheint im ersten Moment als zu detailliert, in der Praxis hat sich jedoch schon oft gezeigt, dass eine detaillierten Planung zum einen die spätere Nachvollziehbarkeit erleichtert sowie zum anderen die in der Umsetzungsphase beginnende Fortschrittsverfolgung wesentlich vereinfacht. Ist dies nicht möglich oder nicht gewünscht, so sollte aus den anteilig involvierten Vergütungsgruppen ein Durchschnittswert gebildet werden, mit dem dann einheitlich die Personalanteile bewertet werden. Die entsprechend angewandte Methode sollte in den *Annahmen und Prämissen* beschrieben werden (vgl. Kapitel 5.3.1.2).

Alternativ bietet sich auch an, diese Aufwände anhand des benötigten Projektteams zusammen zu stellen. Dabei sollte dann die zeitanteilige Mitarbeit in dem Projektteam des betroffenen Personals abgeschätzt werden.

Der Aufwand lässt sich in beiden Vorgehensweisen anhand der Vergütungsgruppe aus dem Rundschreiben des BMF[1] ermitteln.

WIBe-Kriterium 1.1.1.2 Kosten externer Beratung

Darstellung von Kosten *haushaltswirksam*

Hier werden die externen Personalaufwände dargestellt. Auch hier dient als Basis der Projektplan. Es empfiehlt sich, die Aufwände der einfachen Zuordnung halber getrennt nach Lieferanten zu planen. In Fällen von Zusatz- oder Neuprogrammierung kann es durchaus Überschneidungen zu dem *Kriterium 1.1.2.2*

[1] vgl. Rundschreiben des BMF vom 15. März 2004 zu „Personalkostemsätze für Kostenberechnungen/ Wirtschaftlichkeitsbetrachtungen, Sachkostenpauschalen und Kalkulationszinssätzen“. Dieses Rundschreiben wird jährlich erneuert und kann kostenlos aus dem Internet abgerufen werden (http://www.bundesfinanzministerium.de/Anlage29543/ Personalkostensaetze_-Sachkostenpauschale-und-Kalkulationssaetze-2004.pdf).

Softwarekosten geben. In diesem Fall sollte eine Abgrenzung vorgenommen werden und hier die gesamtprojektbezogenen externen Personalaufwände erfasst werden. Die für die Softwareerstellung oder –überarbeitung anfallenden Kosten sind dann unter dem Kriterium 1.1.2.2 zu planen.

WIBe-Kriterium 1.1.1.3 Kosten der Testumgebung

Darstellung von Kosten haushaltswirksam

In seltenen Fällen entstehen hier Kostenansätze.

WIBe-Kriterium 1.1.1.4 Sonstige Kosten für Sach-/Hilfsmittel

Darstellung von Kosten haushaltswirksam und/ oder nicht haushaltswirksam

Hier können die Kosten für ein Projektbüro dargestellt werden (z.B. Notebooks, PCs, Drucker, Monitore, Beamer, Flipchart, Metaplantafeln, Moderatorenkoffer, Büromöbel, Miete für externe oder Mietverrechnungssätze für interne Räumlichkeiten, etc.). Soweit diese Kostenansätze zu externen Rechnungen führen, sind sie haushaltswirksam darzustellen. Bei Kosten, die im internen Bereich entstehen, also bei internen Verrechnungsätzen für zeitweilig überlassene Räume, sind sie im nicht haushaltswirksamen Bereich zu zeigen.

WIBe-Kriterium 1.1.1.5 Reisekosten (eigenes Personal)

Darstellung von Kosten haushaltswirksam

Werden Besichtigungs- oder Informationsreisen zu anderen Behörden oder Lieferanten im Rahmen des Projektes erforderlich, so sollen die anfallenden Reisekosten (Reisekosten wie Flugtickets, Bahntickets, Kosten für öffentliche Verkehrsmittel, Kilometergelder, Taxi- und Parkkosten, Übernachtungskosten, Tagegelder, etc.) hier aufgeführt werden.

WIBe-Kriteriengruppe 1.1.2 Systemkosten

WIBe-Kriteriengruppe 1.1.2.1 Hardwarekosten

WIBe-Kriterium 1.1.2.1.1 Host/ Server, Netzbetrieb

Darstellung von Kosten haushaltswirksam

In der Regel wird eine Migration vor dem Hintergrund notwendiger und umfangreicher Hardwareerneuerung geplant, die dann nicht mehr in dem Maße erforderlich ist. Somit entstehen in jedem Fall durch die Migration Hardwareausgaben. Dazu können gehören: Datenbank-Server, Applikations-Server, Firewall, Web-Applikationen, Infrastruktur/ Netz, Router, Drucker (soweit serverseitig), etc.

WIBe-Kriterium 1.1.2.1.2 Arbeitsplatzrechner

Darstellung von Kosten haushaltswirksam

Auch bei den Arbeitsplatzrechnern kann es zu Neuinvestitionen kommen. Die entstehenden Kosten (z.B. für PCs, Notebooks, Drucker, etc.) sind unter diesem Kriterium aufzuzeigen.

WIBe-Kriteriengruppe 1.1.2.2 Softwarekosten

WIBe-Kriterium 1.1.2.2.1 Kosten für Entwicklung bzw. Beschaffung von Software

Darstellung von Kosten haushaltswirksam

Hier werden Kostenansätze für Lizenzen, Miete und/ oder Kauf ausgewiesen.

WIBe-Kriterium 1.1.2.2.2 Kosten für Anpassung von Software und/ oder Schnittstellen

Darstellung von Kosten haushaltswirksam

Sind für die Software Anpassungen erforderlich, so können die Aufwände hier erfasst werden. Dabei ist unerheblich, ob es sich um Personentageaufwände[1] oder um Festpreisverträge handelt.

WIBe-Kriterium 1.1.2.2.3 Kosten für Evaluierung, Zertifizierung und Qualitätssicherung

Darstellung von Kosten haushaltswirksam

Sind z. B. bisherige Softwareprodukte zertifizert, deren Ersatzprodukte bis zum jetzigen Zeitpunkt noch nicht über ein vergleichbares Zertifikat verfügen und im Rahmen der Migration Software-Nachfolgeprodukte zertifiziert werden müssen, so werden diese Kosten hier erfasst.

WIBe-Kriteriengruppe 1.1.2.3 Installationskosten

Für IT-Migrations-Vorhaben fallen erfahrungsgemäß keine projektspezifischen zusätzlichen Installaitionskosten an. Aufwendungen für bauliche, technische und sonstige Einrichtungen sind in der Regel in allgemeinen IT-Infrastrukturprojekten enthalten, die für die speziellen Migrations-Vorhaben genutzt werden können. Damit entfallen für die Kalkulation Aufwendungen bei den nachfolgenden Positionen:

- WIBe-Kriterium 1.1.2.3.1 Bauseitige Kosten
- WIBe-Kriterium 1.1.2.3.2 Verlegung technischer Infrastruktur
- WIBe-Kriterium 1.1.2.3.3 Büro-/Raumausstattung, Zubehör

WIBe-Kriterium 1.1.2.3.4 Personalkosten der Systeminstallation

Darstellung von Kosten haushaltswirksam/ nicht haushaltswirksam

Installiert das eigene Personal z.B. die neu beschaffte Hardware oder Software in Eigenregie, so sind die entsprechenden Aufwände hier zu erfassen.

[1] Interne Personentageaufwände sind nach der eingangs beschriebenen Methode zu ermitteln. Dabei wird die Projektplanung zugrunde gelegt und die betreffenden Personentage mit den jeweiligen Kostenansätzen bewertet. In den Prämissen und Annahmen ist festgelegt, ob mit einem durchschnittlichen Verrechnungspreis oder nach Vergütungsgruppen bewertet wird.

WIBe-Kriteriengruppe 1.1.3 Kosten der Systemeinführung

WIBe-Kriterium 1.1.3.1 System- und Integrationstest(s)

Darstellung von Kosten *haushaltswirksam*

Migrationen werden in aller Regel mit externen Anbietern bzw. Standardsoftware von Lieferanten durchgeführt. Somit werden keine speziellen System- und Integrationstests anfallen.

WIBe-Kriterium 1.1.3.2 Übernahme von Datenbeständen

Darstellung von Kosten *haushaltswirksam*

Im Rahmen der Migration wird es zu Datenübernahmen kommen. Die dafür notwendigen Aufwendungen sind hier zu planen. Die Aufnahme der Ist-Situation ermöglicht bietet eine Basis um die entsprechenden Aktivitäten abzuschätzen. Diese können entweder in Personentagen ausgedrückt werden oder in Festpreisangeboten von externen Lieferanten, die für spezielle Datenbereiche Übernahme- oder Umstellungsarbeiten anbieten.

WIBe-Kriterium 1.1.3.3 Erstschulung Anwender und IT-Fachpersonal

Darstellung von Kosten *haushaltswirksam/ nicht haushaltswirksam*

Zunächst werden hier die externen Kosten aufgrund von vorliegenden Angeboten oder Verträgen für die Schulungen erfasst. Hinzu kommen die sonstigen Kosten, die entstehen für Raummiete, Reisen, Bewachung, etc.. Dies bis hierher aufgeführten Kostenteile sind dem haushaltswirksamen Bereich zuzuordnen.

Die den Ausfallzeiten der zu schulenden Mitarbeiter gegenüberstehenden Kosten sind hier ebenfalls zu planen. Dieses Kosten werden nicht haushaltswirksam erfasst.

WIBe-Kriterium 1.1.3.4 Einarbeitungskosten Anwender und IT-Fachpersonal

Darstellung von Kosten *haushaltswirksam*

Die in diesem Kriterium zu erhebenden Kostenanteile für die durch die Einarbeitung der Mitarbeiter entstehenden Prozessverlangsamungen sind in der Regel kaum ermittelbar.

WIBe-Kriterium 1.1.3.5 Sonstige Umstellungskosten

Darstellung von Kosten *haushaltswirksam*

Hier können sonstige nicht eindeutig zuordbare Kosten der Migration erfasst werden.

WIBe-Kriteriengruppe 1.2 Entwicklungs-/Einführungsnutzen aus Ablösung des alten Verfahrens

WiBe-Kriterium 1.2.1 Einmalige Kosteneinsparungen (Vermeidung von Erhaltungs-/ Erweiterungskosten Altsystem)

Darstellung von Kosten/ Nutzen haushaltswirksam/ nicht haushaltswirksam

In der Beschreibung der Methodik der WiBe heißt es zu diesem Kriterium: „*Mit dem Entwicklungsnutzen sind zunächst die eher seltenen Fälle von Einsparungen gemeint, die sich aus vermeidbaren Investitionen in das vorhandene Alt-System aufgrund des IT-Vorhabens ergeben können. Soweit Investitionen bzw. Erhaltungsaufwände für das Alt-System fest eingeplant oder technisch unumgänglich sind, können diese Beträge als Einsparungen eingerechnet werden. Sachkosten für die Erhaltung umfassen beispielsweise anstehende Ersatzinvestitionen in Hardware-Komponenten u. ä. Sachkosten für die Erweiterung wären beispielsweise Zukauf von Speicherkapazität, Peripheriegeräten sowie Kauf von Fremdsoftware mit erweitertem Funktionsumfang. Personalkosten für die Erhaltung bzw. Erweiterung fallen z.B. an bei Änderungen der technischen oder softwaremäßigen Eigenschaften, wenn dies intern geleistet wird. Wenn das IT-Vorhaben derartige Kosten vermeiden hilft, sind diese Beträge in der WiBe anzusetzen. Sofern im Haushaltsplan dafür bereits ein Ansatz erfolgt ist, sind diese Einsparungen auch haushaltswirksam. In jedem Fall aber sind die Berechnungswege solcher Kosteneinsparungen präzise zu begründen und zu dokumentieren.*“

In diesem Sinne ist zu prüfen, welche Investitionen ohne Migration angestanden hätten.

WIBe-Kriterium 1.2.2 Einmalige Erlöse (aus Verwertung Altsystem)

Darstellung von Nutzen haushaltswirksam

Dieses Kriterium wird für Migrationsvorhaben nicht genutzt.

WIBe-Kriteriengruppe 2 Betriebskosten und Betriebsnutzen

In dieser Kriteriengruppe werden die laufenden Betriebskosten und die zu erwartenden Nutzen in Form von Einsparungen bei den bisherigen Betriebskosten bzw. bei den Kernprozessen der Behörde aufgezeigt. Sämtliche Kriterien bieten daher die Möglichkeit, Kosten und Nutzen getrennt auszuweisen.

Bei den folgenden Kriterien ist immer zu prüfen, ob für die angesetzten Kosten aus dem bisherigen Kostenvolumen Anteile entfallen können. Diese sind dann als Ersparnisse in den Nutzenzeilen einzutragen.

WIBe-Kriteriengruppe 2.1 Laufende Sachkosten/Sachkosteneinsparungen

In der Kriteriengruppe der laufenden Sachkosten/ -einsparungen (Kriterien 2.1.1 bis 2.1.5) wird regelmäßig der so genannte Nettoeffekt dargestellt. Das bedeutet, das nur die Kosten ausgewiesen werden, die über dem heutigen Niveau liegen, bzw. die Kostendifferenz der künftigen zu den heutigen Kosten als Ersparnis aufgezeigt. Bei den meisten Migrationsvorhaben wird es aber bei einem ausgegli-

chenen Effekt bleiben, so dass in dieser Gruppe keine Einträge vorgenommen werden. Grundsätzlich gilt aber: Prüfen, ob Effekte erzielbar sind.

WIBe-Kriterium 2.1.1 (Anteilige) Leitungs-/Kommunikationskosten

Darstellung von Kosten/ Nutzen nicht haushaltswirksam/ nicht haushaltswirksam

WIBe-Kriterium 2.1.2 (Anteilige) Host-, Server- und Netzkosten

Darstellung von Kosten/ Nutzen nicht haushaltswirksam/ nicht haushaltswirksam

WIBe-Kriterium 2.1.3 (Anteilige) Kosten für Arbeitsplatzrechner

Darstellung von Kosten/ Nutzen nicht haushaltswirksam/ nicht haushaltswirksam

WIBe-Kriterium 2.1.4 Verbrauchsmaterial zur Hardware

Darstellung von Kosten/ Nutzen nicht haushaltswirksam/ nicht haushaltswirksam

WIBe-Kriterium 2.1.5 Energie- und Raumkosten

Darstellung von Kosten/ Nutzen nicht haushaltswirksam/ nicht haushaltswirksam

WIBe-Kriteriengruppe 2.2 Laufende Personalkosten/ Personalkosteneinsparungen

WIBe-Kriterium 2.2.1 Personalkosten aus Systembenutzung

Darstellung von Kosten/ Nutzen nicht haushaltswirksam

Die Methodik besagt, dass unter diesem Kriterium auch die bewerteten Ausfallzeiten des Systems („downtime“) dargestellt werden sollten. In der Regel ist aber die Ermittlung gerade dieser Zeiten mit einem unverhältnismäßig hohen Aufwand verbunden, so dass sie in den meisten Fällen unterbleibt.

Hingegen sind in diesem Kriterium die Nutzen durch eine Migration (bestimmter Systeme oder gesamter Plattformen) bezogen auf die Kernprozesse der Behörde durchaus darzustellen. In vielen Fällen liegt hierin auch das wesentliche Potenzial, um zu einem positiven Kapitalwert zu gelangen.

WIBe-Kriterium 2.2.2 Kosten/ Nutzen aus Dienstpostenumstufung

Darstellung von Kosten/ Nutzen haushaltswirksam

Die Aktivitäten zur Administration einer Open Source Architektur sind umfangreicher und erfordern zurzeit noch einen intensiveren Ausbildungsstand des Personals als die für eine Microsoft-Windows-Architektur. Hier kann sich im Einzelfall die Notwendigkeit ergeben, eine Höherqualifizierung der betroffenen IT-Mitarbeiter zu zulassen. Da jedoch die Budgetlage der öffentlichen Haushalte generell sehr eng ist, wird dies in vielen Fällen kein gangbarer Weg sein. Viel-

mehr werden die Behörden bei spezifischen Problemfällen, die sie nicht mit dem derzeit verfügbaren Personal lösen können, auf externe Unterstützung zurückgreifen. Diese Aufwände sind spitz kalkulierbar. Eine Höherstufung von eigenem Personal bedeutet eine langfristige Kostensteigerung.

WIBe-Kriterium 2.2.3 Systembetreuung und –administration

Darstellung von Kosten/ Nutzen haushaltswirksam/ nicht haushaltswirksam

Soweit die laufende Betreuung des Systems mit dem vorhandenen Personal, auch umgesetztes Personal, erfolgt, sind dafür anzusetzenden Kosten im nicht haushaltswirksamen Bereich aufzunehmen. Werden jedoch neue Dienstposten erforderlich, so sind die dafür anzusetzenden Aufwände haushaltswirksam zu planen.

WIBe-Kriterium 2.2.4 Laufende Schulung/ Fortbildung

Darstellung von Kosten/ Nutzen haushaltswirksam/ nicht haushaltswirksam

In vielen Fällen ergibt sich die Notwendigkeit nach der Migration im ersten Jahr des Betriebes der migrierten Architektur den Anwendern eine Nachschulung anzubieten. Die in der Erstschulung erworbenen Kenntnisse werden nur in Abhängigkeit der Möglichkeiten zur regelmäßigen Nutzung der jeweiligen Anwendung oder Anwendungsplattform auch weiterhin präsent sein. Externe Schulungskosten werden haushaltswirksam, die Zeiten der zu schulenden Mitarbeiter bewertet nicht haushaltswirksam dargestellt. In Abhängigkeit des grundsätzlichen Ausbildungsstandes der betroffenen Mitarbeiter sowie der Komplexität und der Wichtigkeit der Anwendung sollte hier der in der Beschreibung der Methodik vorgeschlagene Wert von 10% der Erstschulung durchaus variiert werden.

WIBe-Kriteriengruppe 2.3 Laufende Kosten/Einsparungen bei Wartung /Systempflege

WIBe-Kriterium 2.3.1 Wartung/ Pflege der Hardware

Darstellung von Kosten/ Nutzen haushaltswirksam/ nicht haushaltswirksam

In der Regel wird eine Gewährleistung auf Hardware vom Hersteller/ Lieferanten geboten. In vielen Fällen auch schon 36 Monate. Ist der Betrachtungszeitraum der WiBe länger, so sind hier für die Zeit ab dem 4. Jahr Kosten zu veranschlagen. Diese können entweder aufgrund eines vorliegenden Angebotes direkt angegeben werden oder mit marktüblichen Ansätzen von 10% – 20% auf den Kaufpreis geschätzt werden. Hier sollte jedoch in jedem Fall eine Recherche durchgeführt werden, um diesen Ansatz auf den wahrscheinlichsten Wert einzugrenzen. Diese Kosten werden haushaltswirksam dargestellt.

Wird die Wartung hausintern durchgeführt, so sind in diesem Fall die Kosten für das eigene Personal anzusetzen. Dabei sind auch Kosten für die Infrastruktur bzw. für die Ausrüstung der Mitarbeiter zu berücksichtigen, mit der sie die Wartungsarbeiten erst bewerkstelligen können. Wenn es sich um normale IT-Arbeitsplätze handelt kann hier durchaus auch die Sachkostenpauschale mit Zu-

schlag für Bildschirmarbeitsplätze des BMF angewandt werden. Diese internen Kosten werden nicht haushaltswirksam ausgewiesen.

WIBe-Kriterium 2.3.2 Wartung/ Update der Software

Darstellung von Kosten/ Nutzen haushaltswirksam/ nicht haushaltswirksam

Für Fremdsoftware, die einer dynamische Entwicklung im Zeitablauf unterworfen ist, verlangen die Hersteller grundsätzlich Update-, Pflege- oder Wartungsbeiträge. Diese sind ebenfalls konkret beziffert oder bewegen sich marktüblich in einem Bereich von 15% - 20% des Kaufpreises. Bei Wartung der Software durch eigene Mitarbeiter gelten die Ausführungen wie unter 2.3.2.

WIBe-Kriterium 2.3.3 Ersatz-/ Ergänzungskosten

Darstellung von Kosten/ Nutzen haushaltswirksam/ nicht haushaltswirksam

Werden Hard- und/ oder Software nach der üblichen Abschreibungsfrist ersetzt und reicht der Betrachtungszeitraum der WiBe über diesen Zeitpunkt hinaus, so sind hier Kostenansätze für den geplanten Ersatz der Systeme vorzunehmen. Gleiches gilt auch bei heute schon bekannten und vorgesehenen Erweiterungen für das in der Wirtschaftlichkeit begutachtete Verfahren.

WIBe-Kriteriengruppe 2.4 Sonstige Laufende Kosten und Einsparungen

WIBe-Kriterium 2.4.1 Datenschutz-/ Datensicherungskosten

Darstellung von Kosten/ Nutzen haushaltswirksam/ nicht haushaltswirksam

In der Regel wird eine Migration auf der Basis der vorhandenen Sicherheitseinrichtungen durchgeführt. Damit ergeben sich hier keine Kostenansätze. Wird im Rahmen der Migration jedoch auch in die IT-Sicherheit investiert so ist dieser sicherheits-spezifische Teil der Kosten hier darzustellen.

WIBe-Kriterium 2.4.2 Kosten begleitender Externer Beratung

Darstellung von Kosten/ Nutzen haushaltswirksam/ nicht haushaltswirksam

Hier kann die Nachbetreuung der Migration durch externes Personal dargestellt werden.

WIBe-Kriterium 2.4.3 Versicherungen u.ä.

Darstellung von Kosten/ Nutzen haushaltswirksam/ nicht haushaltswirksam

Dieses Kriterium wird regelmäßig nicht ausgewählt.

WIBe-Kriterium 2.4.4 Sonstige laufende Kosten und Nutzen

Darstellung von Kosten/ Nutzen haushaltswirksam/ nicht haushaltswirksam

Dieses Kriterium wird regelmäßig nicht ausgewählt.

5.5.2.2 Migrations- und Anbieterszenarien

Eine Migration wird grundsätzlich verschiedene Szenarien zur Auswahl haben und unterschiedliche Anbieter werden für unterschiedliche Szenarien oder Teile davon Angebote abgeben. Die Wirtschaftlichkeitsbetrachtung sollte dies in jedem Fall berücksichtigen. Die Ausführungen in Kapitel 5.5.2.1, Systematik, S. 426 stellen die Basis für das Grundgerüst der WiBe dar.

Eine Versionierung der WiBe hilft, die verschiedenen Szenarien und Angebotssituationen abzubilden. Die Kriterien, die von eventuell unterschiedlichen Angeboten betroffen sind, werden in verschiedenen Versionen der Wirtschaftlichkeitsbetrachtung, mit den jeweiligen Angebotswerten gefüllt. Somit liefern die verschiedenen Versionen der WiBe eigenständige Aussagen zu Kapitalwert und Rentabilität. Eine Kostenvergleichsrechnung kann dann die einzelnen Versionen zueinander in Relation setzen und eine Entscheidungsbasis liefern.

Die folgenden Abbildungen zeigen exemplarisch eine monetäre WiBe für die Bereiche der Einführungs- und Betriebs-Kosten/ Nutzen (vgl. die beiden nachfolgenden Abbildungen).

IT-Vorhaben: Migration von Server- und Clientarchitekturen

Pos. WiBe	Kriterium, Erläuterung zur Selektion Hinweis: Startjahr = 2005, Laufzeit = 8 Jahre, Diskontierungs-Zins = 3,8%, Break even gesamt im 7. Jahr, 2011	Nominal Gesamt, 8 Jahre			Barwerte Gesamt, 8 Jahre		
		gesamt	hh.wirks.	n.hh.wirks.	gesamt	hh.wirks.	n.hh. wirks.
KN	**Kosten + Nutzen - Entwicklung/ Einführung und Betrieb**	1.920.440	-1.125.764	3.046.204	1.168.082	-1.265.080	2.433.162
	...davon Kosten	-5.862.187	-4.496.124	-1.366.063	-5.564.806	-4.258.273	-1.306.533
	... davon Nutzen	7.782.627	3.370.360	4.412.267	6.732.888	2.993.193	3.739.695
	KN Kumuliert	1.920.440	-1.125.764	3.046.204	1.168.082	-1.265.080	2.433.162
1	**Entwicklungs-/Einführungskosten und Entwicklungsnutzen**	-3.509.501	-2.580.546	-928.955	-3.509.501	-2.580.546	-928.955
	...davon Kosten		-2.785.866	-928.955	-3.714.821	-2.785.866	-928.955
	... davon Nutzen		205.320	0	205.320	205.320	0
1.1	Entwicklungs-/Einführungskosten für das neue IT-Verfahren	-3.714.821	-2.785.866	-928.955	-3.714.821	-2.785.866	-928.955
1.1.1	Planungs- und Einführungskosten	-1.596.038	-1.071.363	-524.675	-1.596.038	-1.071.363	-524.675
1.1.1.1	Personalkosten (eigenes Personal)	-568.175	-43.500	-524.675	-568.175	-43.500	-524.675
1.1.1.2	Kosten externer Beratung	-882.760	-882.760	0	-882.760	-882.760	0
1.1.1.3	Kosten der Entwicklungsumgebung	0	0	0	0	0	0
1.1.1.4	Sonstige Kosten für Sach-/Hilfsmittel	-139.303	-139.303	0	-139.303	-139.303	0
1.1.1.5	Reisekosten (eigenes Personal)	-5.800	-5.800	0	-5.800	-5.800	0
1.1.2	Systemkosten	-1.375.231	-1.373.753	-1.477	-1.375.231	-1.373.753	-1.477
1.1.2.1	Hardwarekosten	-380.480	-380.480		-380.480	-380.480	
1.1.2.1.		0	0	0	0	0	0
1.1.2.1.	Host/Server, Netzbetrieb	-160.080	-160.080	0	-160.080	-160.080	0
1.1.2.1.	Arbeitsplatzrechner	-220.400	-220.400	0	-220.400	-220.400	0
1.1.2.2	Softwarekosten	-993.273	-993.273		-993.273	-993.273	
1.1.2.2.		0	0	0	0	0	0
1.1.2.2.	Kosten für Einführung bzw. Beschaffung von Software	-717.773	-717.773	0	-717.773	-717.773	0
1.1.2.2.	Kosten für Anpassung von Software und/oder Schnittstellen	-275.500	-275.500	0	-275.500	-275.500	0
1.1.2.2.	Kosten für Evaluierung, Zertifizierung und Qualitätssicherung	0	0	0	0	0	0
1.1.2.3	Installationskosten	-1.477		-1.477	-1.477		-1.477
1.1.2.3.		0	0	0	0	0	0
1.1.2.3.	Bauseitige Kosten	0	0	0	0	0	0
1.1.2.3.	Verlegung technischer Infrastruktur	0	0	0	0	0	0
1.1.2.3.	Büro-/Raumausstattung, Zubehör	0	0	0	0	0	0
1.1.2.3.	Personalkosten der Systeminstallation	-1.477	0	-1.477	-1.477	0	-1.477
1.1.3	Kosten der Systemeinführung	-743.552	-340.750	-402.802	-743.552	-340.750	-402.802
1.1.3.1	System- und Integrationstest(s)	0	0	0	0	0	0
1.1.3.2	Übernahme von Datenbeständen	-224.750	-224.750	0	-224.750	-224.750	0
1.1.3.3	Erstschulung Anwender und IT-Fachpersonal	-518.802	-116.000	-402.802	-518.802	-116.000	-402.802
1.1.3.4	~~Einarbeitungskosten Anwender und IT-Fachpersonal~~	0	0	0	0	0	0
1.1.3.5	Sonstige Umstellungskosten	0	0	0	0	0	0
1.2	Entwicklungs-/Einführungsnutzen aus Ablösung des alten Verfah	205.320	205.320		205.320	205.320	
1.2.1	Einmalige Kosteneinsparungen (Vermeidung von Erhaltungs-	205.320	205.320	0	205.320	205.320	0
1.2.2	~~Einmalige Erlöse (aus Verwertung Altsystem)~~	0	0	0	0	0	0

Bild 85: WiBe - Beispielhafte WiBe Kalkulation 1, Einführungskosten/ -nutzen

IT-Vorhaben: Migration von Server- und Clientarchitekturen

Pos.	Kriterium, Erläuterung zur Selektion Hinweis: Startjahr = 2005, Laufzeit = 8 Jahre, Diskontierungs-Zins = 3,8%, Break even gesamt im 7. Jahr, 2011	Nominal Gesamt, 8 Jahre			Barwerte Gesamt, 8 Jahre		
WiBe		gesamt	hh.wirks.	n.hh.wirks.	gesamt	hh.wirks.	n.hh. wirks.
KN	**Kosten + Nutzen - Entwicklung/ Einführung und Betrieb**	1.920.440	-1.125.764	3.046.204	1.168.082	-1.265.080	2.433.162
	...davon Kosten	-5.862.187	-4.496.124	-1.366.063	-5.564.806	-4.258.273	-1.306.533
	... davon Nutzen	7.782.627	3.370.360	4.412.267	6.732.888	2.993.193	3.739.695
	KN Kumuliert	1.920.440	-1.125.764	3.046.204	1.168.082	-1.265.080	2.433.162
1	**Entwicklungs-/Einführungskosten und Entwicklungsnutzen**	-3.509.501	-2.580.546	-928.955	-3.509.501	-2.580.546	-928.955
2	**Betriebskosten und Betriebsnutzen**	5.429.942	1.454.782	3.975.159	4.677.583	1.315.466	3.362.117
	...davon Kosten		-1.710.258	-437.108	-1.849.985	-1.472.407	-377.578
	... davon Nutzen		3.165.040	4.412.267	6.527.568	2.787.873	3.739.695
2.1	~~Laufende Sachkosten/ Sachkosteneinsparungen~~	1.948.800	1.948.800		1.716.568	1.716.568	
2.1.1	(Anteilige) Leitungs-/Kommunikationskosten	1.856.000	1.856.000		1.634.827	1.634.827	
2.1.1.0		0	0	0	0	0	0
2.1.1.1	Lfd. Kosten aus IT-Verfahren NEU	0	0	0	0	0	0
2.1.1.2	Lfd. Nutzen aus Wegfall Verfahren ALT	1.856.000	1.856.000	0	1.634.827	1.634.827	0
2.1.2	~~(Anteilige) Host-, Server- und Netzkosten~~						
2.1.3	~~(Anteilige) Kosten für Arbeitsplatzrechner~~						
2.1.4	Verbrauchsmaterial zur Hardware	92.800	92.800		81.741	81.741	
2.1.4.0		0	0	0	0	0	0
2.1.4.1	Lfd. Kosten aus IT-Verfahren NEU	0	0	0	0	0	0
2.1.4.2	Lfd. Nutzen aus Wegfall IT-Verfahren ALT	92.800	92.800	0	81.741	81.741	0
2.1.5	~~Energie- und Raumkosten~~						
2.2	Laufende Personalkosten/-einsparungen	3.882.359	-92.800	3.975.159	3.280.375	-81.741	3.362.117
2.2.1	Personalkosten aus Systembenutzung	4.412.267		4.412.267	3.739.695		3.739.695
2.2.1.0		0	0	0	0	0	0
2.2.1.1	Lfd. Kosten aus IT-Verfahren NEU	0	0	0	0	0	0
2.2.1.2	Lfd. Nutzen aus Wegfall Verfahren ALT	4.412.267	0	4.412.267	3.739.695	0	3.739.695
2.2.2	~~Kosten/Nutzen aus Dienstposten-Umstufung~~						
2.2.3	Systembetreuung und -administration	-437.108		-437.108	-377.578		-377.578
2.2.3.0		0	0	0	0	0	0
2.2.3.1	Lfd. Kosten aus IT-Verfahren NEU	-437.108	0	-437.108	-377.578	0	-377.578
2.2.3.2	Lfd. Nutzen aus Wegfall Verfahren ALT	0	0	0	0	0	0
2.2.4	Laufende Schulung/Fortbildung	-92.800	-92.800		-81.741	-81.741	
2.2.4.0		0	0	0	0	0	0
2.2.4.1	Lfd. Kosten aus IT-Verfahren NEU	-92.800	-92.800	0	-81.741	-81.741	0
2.2.4.2	Lfd. Nutzen aus Wegfall Verfahren ALT	0	0	0	0	0	0
2.3	Laufende Kosten/Einsparungen bei Wartung /Systempflege	-1.051.858	-1.051.858		-892.466	-892.466	
2.3.1	Wartung/Update der Hardware	-318.800	-318.800		-266.598	-266.598	
2.3.1.0		0	0	0	0	0	0
2.3.1.1	Lfd. Kosten aus IT-Verfahren NEU	-452.400	-452.400	0	-384.277	-384.277	0
2.3.1.2	Lfd. Nutzen aus Wegfall IT-Verfahren ALT	133.600	133.600	0	117.679	117.679	0
2.3.2	Wartung/Update der Software	-733.058	-733.058		-625.868	-625.868	
2.3.2.0		0	0	0	0	0	0
2.3.2.1	Lfd. Kosten aus IT-Verfahren NEU	-1.165.058	-1.165.058	0	-1.006.388	-1.006.388	0
2.3.2.2	Lfd. Nutzen aus Wegfall IT-Verfahren ALT	432.000	432.000	0	380.520	380.520	0
2.3.3	~~Ersatz-/Ergänzungskosten~~						
2.4	Sonstige Laufende Kosten und Einsparungen	650.640	650.640		573.105	573.105	
2.4.1	Datenschutz-/Datensicherungskosten						
2.4.1.0		0	0	0	0	0	0
2.4.1.1	Lfd. Kosten aus IT-Verfahren NEU	0	0	0	0	0	0
2.4.1.2	Lfd. Nutzen aus Wegfall Verfahren ALT	0	0	0	0	0	0
2.4.2	Kosten begleitender externer Beratung	650.640	650.640		573.105	573.105	
2.4.2.0		0	0	0	0	0	0
2.4.2.1	Lfd. Kosten aus IT-Verfahren NEU	0	0	0	0	0	0
2.4.2.2	Lfd. Nutzen aus Wegfall Verfahren ALT	650.640	650.640	0	573.105	573.105	0
2.4.3	~~Versicherungen u.ä.~~						
2.4.4	~~Sonstige laufende Kosten und Nutzen~~						

Bild 86: WiBe - Beispielhafte WiBe Kalkulation 2, Betriebskosten/ -nutzen

Ergebnis einer WiBe sollte auch ein Überblick der liquiditätswirksamen also der haushaltswirksamen Kosten sein. Dieser Überblick wird punktuell in den Zeilen obiger WiBe-Darstellung mit der Bezeichnung „davon Kosten“ gegeben. Die nachfolgende Grafik zeigt diesen Zusammenhang für die Jahre des Betrachtungszeitraumes.

Bild 87: WiBe – Entwicklung externer Kosten (haushaltswirksam)

Die Betrachtung der kumulierten Salden aus Kosten und Nutzen der diskontierten Werte zeigt den Break even Punkt. Dieser liegt dort, wo die Salden das erste Mal in der Zeitreihe in den positiven Bereich gelangen (siehe nachfolgende Grafik).

Bild 88: WiBe - Break even Übersicht

5.5.3 Erweiterte Wirtschaftlichkeit nach WiBe

Der Teil der erweiterten Wirtschaftlichkeit – also Nutzwertanalysen der Kriterien für Dringlichkeit, Qualität/ Strategie und externe Effekte von IT-Vorhaben wird in der nächsten Version des MLF vorgestellt. Hintergrund ist die notwendig gewordene Überarbeitung der speziell auf Migrationen zugeschnittenen Kriteriengruppen nach der Fortschreibung der Wibe.

5.5.4 Strategische Dimension

Neben der unmittelbar monetären Analyse der Vollkosten der einzelnen Alternativen ist es notwendig, eine strategische Betrachtung (in der WiBe-Terminologie *Dimension*) mit einzubeziehen.

Die Notwendigkeit einer strategischen Betrachtung ergibt sich durch die direkten monetären Auswirkungen des strategischen Faktors „Herstellerabhängigkeit“. Diese hat sowohl aus der makro- als auch mikroökonomischen Sicht Bedeutung.

5.5.4.1 Makroökonomische Betrachtung

In dieser Betrachtung spielen die wettbewerbsbedingten Aspekte die Hauptrolle. Wesentliche Vorteile eines funktionierenden Wettbewerbs sind:

- Bessere Produktqualität
- Niedrigere Produktpreise
- Höhere Innovationsrate

Obwohl alle SW-Hersteller im Regelfall für sich sowohl die höhere Produktqualität als auch die technologische Innovation beanspruchen, kann eine Pauschalaussage in der Realität nur selten getroffen werden. Insbesondere die World Wide Web Entwicklung zeigt, dass beispielsweise Microsoft diese wichtigste Innovation der letzten Dekaden lange Zeit „verschlafen“ hat.

Die makroökonomische Betrachtung hat zwar einen grundsätzlichen Charakter, ist jedoch nicht direkt beeinflussbar durch die Empfänger des Migrationsleitfadens und wird daher im Migrationsleitfaden nicht vertieft.

5.5.4.2 Mikroökonomische Betrachtung

Wesentlich hierfür ist die Betrachtung der eigenen Abhängigkeit von Lieferanten von Produkten und Dienstleistungen. Obwohl die Abhängigkeit substantiell durch die Existenz von Monopolen oder Quasi-Monopolen gefördert und sichtbar wird, kann auch im funktionierenden Wettbewerb eine zu starke Abhängigkeit von Lieferanten auftreten und u.U. zu wirtschaftlichen Nachteilen führen. Diese können sich einerseits durch höhere Produktpreise, andererseits jedoch auch durch kürzere Lebenszyklen von Produkten manifestieren, verbunden mit zusätzlichen Einführungskosten bei fortführenden Migrationen.

Im Extremfall kann die Abhängigkeit zu Situationen führen, in denen keine preislich akzeptablen Handlungsalternativen mehr vorhanden sind. Im Gegensatz dazu führt eine auf strategischem Gleichgewicht aufgebaute Situation zu einer besseren Verhandlungsposition, in der im Problemfall auf Alternativen zurückgegriffen werden kann.

5.6 Alternative Wirtschaftlichkeitsbetrachtung im monetären Bereich nach MiKoMa

5.6.1 Überblick

Die **Migrationskostenmatrix** (MiKoMa) stellt immer dann für eine Behörde eine Alternative zur WiBe 4.0 dar, wenn die damit erlangten Ergebnisse im Sinne des § 7 BHO rechtlich **nicht** belastbar sein müssen.

Die ausschließlich monetären Kennzahlen der MiKoMa sind bei gleicher Datenbasis denen der monetären Dimension der WiBe vergleichbar. Werden Kennzahlen zu Dringlichkeit, Qualität und Strategie sowie zu externen Effekten von IT-Maßnahmen erforderlich, so ist für diesen Bereich der Teil der Nutzwertanalyse aus der WiBe anzuwenden.

Die MiKoMa bietet dem Anwender neben einer übersichtlichen Strukturierung auch eine erste Entscheidungshilfe. MiKoMa 2.0 nutzt zur Erhebung der Analysedaten eine in acht Kostenartengruppen gegliederte Struktur, getrennt für die Bereiche Projekt-, Betriebskosten und Ersparnisse. Diese Struktur zur Kostenerfassung orientiert sich an marktüblichen TCO-Analysen. Die Liquiditätswirksamkeit wird ebenfalls betrachtet. Die Ermittlung des Kapitalwertes wird für die gleichzeitige Berechnung des Break even mit genutzt, so dass die MiKoMa 2.0 eine Aussage liefert, wann die kumulierten Jahressalden der IT-Maßnahme in den positiven Bereich gelangen. Damit wird der Zeitpunkt dargestellt, an dem die kumulierten Ersparnisse der Investition erstmals die kumulierten Kosten übersteigen.

In der nachfolgenden Tabelle ist überblicksmäßig eine Auswahl von Eigenschaften der Methoden WiBe 4.0 und MiKoMa 2.0 dargestellt.

Tab. 62: Vergleichende Übersicht thematischer Eigenschaften von WiBe 4.0 und MiKoMa 2.0

Themen	WiBe 4.0	MiKoMa 2.0
Monetäre Wirtschaftlichkeit der IT-Maßnahme	Ja	Ja
Monetäre Wirtschaftlichkeit mit Risikoabschätzung	Ja	i.V.
Dringlichkeit der IT-Maßnahme	Ja	Nein
Qualitativ-stratregische Bedeutung der IT-Maßnahme	Ja	Nein
Externe Effekte der IT-Maßnahme	Ja	Nein
Kapitalwert (diskontierte Jahressalden)	Ja	Ja
Break even der IT-Maßnahme	Nein	Ja

Themen	WiBe 4.0	MiKoMa 2.0
Kriterienkatalog	Ja	Nein
Kostenartengruppenkatalog	Nein	Ja
Selektion relevanter Kriterien (Festlegung Grob-Layout)	Ja	Nein
Beschreibung der Kriterien/ Kostenartengruppen	Nach WiBe 4.0	Nach MiKoMa
Projektdefinition	Nein	Ja
Eigenständige Applikation mit Softwareschutz und Datenübertragungsmöglichkeit nach MS Excel	Ja	MS Excel ist Basis[1]
Einbindung der Anwendung in MS Excel	Nein	Ja
Durchführung und Verwaltung mehrerer Versionen	Ja	Ja
Investitions- und Folgeaufwand/ -nutzen getrennt darstellbar	Ja	Ja
Trennung zwischen haushaltswirksamen und nicht haushaltswirksamen Effekten	Ja	Ja
Getrennte Betrachtung für die Sichten Projekt, Haushalt und Betrieb	Bedingt	Ja
Vergleichende Betrachtung verschiedener Alternativen	Ja	Ja

5.6.2 Grundstrukturen

Zur strukturellen Gestaltung der Wirtschaftlichkeitsbetrachtung nach MiKoMa 2.0 kommt ein dreidimensionales Modell zur Anwendung (vgl.

Bild 89).

Die Dimensionen gliedern sich in:

- Kostenbereiche
- Kostenartengruppen

[1] Auch auf Basis OpenOffice Calc.

- Zeitraum

Bild 89: Modell der Wirtschaftlichkeitsbetrachtung nach MiKoMa

1. Dimension: Kostenbereiche

- Projektkosten
- Betriebskosten
- Neue Betriebskosten
- Ersparnisse
- Opportunitätskosten

Projektkosten betreffen die durch die Implementierung verursachten einmaligen Kosten. Dazu gehören im Wesentlichen die internen und externen Personalaufwände, die für die Umsetzung erforderlich sind.

Betriebskosten werden in Form der Wartung und des direkt mit der Betreuung des Softwaresystems befassten Personals dargestellt. Die Betriebskosten stellen hier nur eine Ausgangsbasis für die künftige Kostenentwicklung dar. Künftige Betriebskosten werden im Kostenbereich „Neue Betriebskosten“ (auch: Betriebskostenveränderung) dargestellt.

Neue Betriebskosten beinhalten die durch die einzuführende Software zusätzlich zu berücksichtigenden laufenden jährlichen Kosten. Hier fließen die Investitionen in Hard- und Software in Form von Abschreibungen sowie Wartungskosten für Software ein.

Ersparnisse lassen sich in der Regel als Ableitung aus einer Prozessanalyse heraus darstellen.

Opportunitätskosten stellen die Kostenäquivalente für Arbeitsausfall beim Endnutzer durch Stillstands- und Fehlerbehebungszeiten dar.

2. Dimension: Kostenartengruppen

- Personalkosten
- externe Leistungen
- Software
- Hardware
- Kommunikation (Netz)
- Raum und Gebäude
- Sonstige Gemeinkosten
- Umlagen

Personal

Bei dieser Kostenart sind direkte und indirekte Kosten zu berücksichtigen.

Unter den direkten Personalkosten sind die Personalkosten des IT-Bereichs zu verstehen. Dazu zählen alle erfassbaren Kosten, z.B.:

- Löhne, Gehälter, Bezüge
- Personalnebenkosten
- Schulungen, Training, Seminare
- Reisekosten
- Umlagen

Die indirekten Personalkosten betreffen das Nicht-IT-Personal und setzen sich in der Regel aus Opportunitätskosten für folgende Umstände zusammen:

- Eigene Konfiguration und Selbsttraining (wenn der Mitarbeiter vor Ort selbst sein System konfiguriert oder Abläufe austestet)
- Fehlerbehebung und -diagnose (der Mitarbeiter am Arbeitsplatz versucht eigenständig Fehler zu erkennen und sie zu beheben)
- Ausfallzeiten (wenn das System nicht nutzbar ist)

Auch wenn der Mitarbeiter vor Ort auf einen User Help Desk (UHD) zur Problembehebung und Unterstützung zurückgreifen kann, zeigt die Praxis, dass er in der Regel erst einmal selbst versucht seine Konfigurationsanforderung (z.B. konfigurieren neuer lokaler oder Netzwerk-Drucker, konfigurieren Outlook, einrichten eigener Formate in OpenOffice, etc.) selbst oder mit Hilfe eines Kollegen zu lösen. Dies wird umso mehr der Fall sein, als seine Kostenstelle im Falle der Inan-

spruchnahme des UHD mit entsprechenden Service-Kosten belastet wird. Die hierfür verbrauchten Zeiten sind zusätzlich als Opportunitätskosten zu berücksichtigen.

Auch wenn Probleme mit dem System auftreten, wird der Mitarbeiter in aller Regel erst einmal versuchen zu analysieren, ob es sich tatsächlich um einen Fehler handelt, oder er das System falsch bedient hat. Auch diese Zeiten müssen als Opportunitätskosten in Betracht gezogen werden.

Die IT-gestützten Prozesse der öffentlichen Verwaltung sind i. d. R. nicht zeitkritisch. Darüber hinaus ist sehr schwer zu ermitteln, welcher Anteil der Arbeitszeit eines Mitarbeiters vom Ausfall der IT betroffen ist, bzw. in welchem Maße er den Ausfall durch Mehrarbeit kompensieren muss. In der Praxis werden die Vorgänge oft händisch weiter bearbeitet, bzw. die IT-Bearbeitung zu einem späteren Zeitpunkt nachgeholt. Treten diese Probleme jedoch massiert auf, so sollten an dieser Stelle entsprechende Kostenansätze eingestellt werden. Dazu kann die Summe der ausgefallenen Minuten mit den durchschnittlichen Personalvollkosten der jeweiligen betroffenen Laufbahnstufe bewertet werden.

Externe Leistungen

Externe Leistungen stellen grundsätzlich direkte Kosten dar und können folgendermaßen gegliedert werden:

- Externes Personal, z.B.
  - Freie Mitarbeiter für normale Geschäftsprozessunterstützung,
  - Externe Beratung
- Externe projektbezogene Leistungen, z.B.
  - Ausführung von projektbezogenen Leistungen durch externe Mitarbeiter,
  - Bereitstellung temporärer Testumgebungen inkl. Hardware, Software, Service (intern oder extern)
- Outgesourcte Leistungen, z.B.:
  - IT-Support
  - Druck-/ Kopier-/ Schreibservice
  - Kuriere
  - Reiseservice
  - Gebäudereinigung
  - Gebäudesicherung
  - Gebäudebewirtschaftung
  - Kantine
  - Ärztliche Betreuung

In dieser Gruppe sind nur externe Leistungen, die nicht in zu aktivierende Wirtschaftsgüter geflossen sind, zu erfassen. Fremdleistungen für z.B. die Erstellung einer neuen Anwendung inkl. Software, Hardware und Netzkomponenten werden aktiviert und über Abschreibungen wieder dem Kostengefüge zugeführt. Diese Aufwendungen sind nicht hier sondern in den Gruppen "Software", "Hardware" oder "Kommunikation" zu berücksichtigen.

Software

Hierunter fallen Kosten für System-, Standard- und Individualanwendungssoftware. Folgende Gruppierungen können als Hilfestellung zur Erfassung dienen:

- Host
- Server
- Netzwerk
- Arbeitsplätze
- Telefonanlagen
- Sonstiges

Kostenarten dieser Gruppe: Abschreibung, Miete, Leasing, Nutzungsgebühr, Nebenkosten, Wartung

Hardware

Unter diese Gruppe fallen sämtliche Kosten im Zusammenhang mit der Hardware-Ausstattung. Auch hier kann für die Erfassung folgende Gruppierung hilfreich sein:

- Mainframe
- Mainframe Peripherie (Druck-, Schneide-, Sortiermaschinen, etc.)
- Server
- Arbeitsplätze und Peripherie (Drucker, Monitore, Faxgeräte, TV, Tuner, Videoanlagen, etc.)
- Netzkomponenten (Datenübertragungseinrichtungen, Modem, Verkabelung, etc.)
- Telefonanlagen (Fernsprecheinrichtungen, Mobiltelefone)
- Sonstiges

Bei einigen Wirtschaftsgütern in diesem Bereich können Abgrenzungsprobleme zu der Kostenartengruppe "Gebäude" auftreten. Hier ist strikt zwischen selbst erstellten und angemieteten Räumen zu unterscheiden. In ersterem Fall sind die Abschreibungen sämtlicher hardware-technischen Ausstattungen in dieser Gruppe zu erfassen.

Sind die Räume angemietet, so können die hier zu erfassenden Einrichtungen im Mietpreis bereits enthalten sein. Ist dies der Fall, sollte der entsprechende Anteil am Mietpreis hier erfasst werden – notfalls mittels Schätzung.

Sind die angemieteten Räume nachträglich durch den Mieter mit hardware-technischen Einrichtungen ergänzt worden, so sind diese als Abschreibungen hier zu erfassen.

Kostenarten dieser Gruppe: Abschreibung, Miete, Leasing, Nutzungsgebühr, Nebenkosten, Wartung, Energie

Kommunikation

Unter diese Gruppe fallen

- Laufende Telekommunikationskosten
- Netzkosten

Die hardware-technischen Einrichtungen für die Kommunikation (Netzwerkverkabelung, Router, etc.) werden in der Kostenartengruppe "Hardware" erfasst. In dieser Gruppe werden nur die laufenden Kosten für die Telekommunikation und das Netz (z.B. Kosten des Providers, Telekomrechnung, etc.) erfasst.

Gebäude

Diese Gruppe enthält direkte und indirekte Kostenanteile. Folgende grobe Bereiche sind subsumiert:

- Büro inkl. Ausstattung ohne DV-Equipment
- Sonstige Räume (Lager/Archiv/etc.)
- Sonstige Gebäudekosten

Kostenarten dieser Gruppe: Abschreibung, Miete, Leasing, Nebenkosten und Energie.

Sonstige Kosten

Alle Kosten, die nicht in den anderen Kostenartengruppen zugeordnet werden können, werden in dieser Gruppe erfasst.

Grundsätzlich ist jedoch zuerst die Zuordnung zu einer der vorangegangenen Kostenartengruppen zu eruieren. Je genauer die Zuordnung durchgeführt wird, desto wahrhaftiger wird auch das Ergebnis von TCO-Bund sein.

Kostenarten dieser Gruppe: Versicherungen, Verbände, Verbrauchsmaterial, Gebühren

Umlagen

In der Regel werden Umlagekosten bereits in den jeweiligen Kostenartengruppen (wie oben beschrieben) enthalten sein. Sollte eine Behörde jedoch einen anderen Ansatz gewählt haben und ihre Umlagen separat in einem gesonderten Block ausweisen, so besteht mit dieser Gruppe die explizite Möglichkeit, diese auch hier separat zu bearbeiten. Auch in dem Fall, in dem zu verteilende Kosten nicht

eindeutig den jeweiligen Kostenartengruppen zugeordnet werden können, kann diese Gruppe dafür verwendete werden.

Eine Datenerhebung ist für beide Methodiken - WiBe 4.0 und MiKoMa 2.0 - erforderlich. Um hier dem Anwender im Nachgang zur Erhebung der Daten die Gestaltungsfreiheit bezüglich der Methodik zu überlassen, ist im Anhang eine Überleitungstabelle von den Kriterien der WiBe 4.0 zu den Kostenartengruppen der MiKoMa 2.0 angefügt.

3. Dimension: Zeitraum

Der Betrachtungszeitraum kann in der Version 2.0 bis zu 10 Jahre betragen.

Sämtliche dargestellten Kosten werden nach ihrer Haushaltswirksamkeit[1] sortiert. Kosten für eigenes Personal sind nicht haushaltswirksam, d.h. sie führen zu keinem von dem Projekt verursachten Mittelabfluss aus der Kasse. Investitionen und laufende Betriebskosten, für die Rechnungen von Lieferanten oder Dienstleistern zu bezahlen sind, stellen haushaltswirksame Kosten dar und führen zu einem Mittelabfluss.

Ausgaben für Investitionen fallen zu einem Stichtag an. Sie werden in der Wirtschaftlichkeitsbetrachtung nach betriebswirtschaftlichen Regeln über den Nutzungszeitraum linear abgeschrieben. Dadurch ergibt sich in der Wirtschaftlichkeitsbetrachtung eine duale Sichtweise. Zum einen werden die Investitionen als Betriebskostenveränderung in den betrachteten Jahren dargestellt und zum anderen stellen sie Liquiditätsabfluss im ersten Jahr des Betrachtungszeitraumes dar.

5.6.3 Migrations- und Anbieterszenarien

Die Anbieterszenarien weisen im Rahmen der 1. Dimensionen des Modells der Wirtschaftlichkeitsbetrachtung die einzelnen Kostenbereiche zusammengefasst in drei Sichtweisen auf:

- Projektsicht
  Die Projektsicht liefert einen Projektsaldo als Projektnutzen, in dem die Bereiche der Projektkosten, der zusätzlichen Betriebskosten und der durch das Projekt generierten Ersparnisse zusammengeführt werden.
- Betriebssicht
  Die Betriebssicht zeigt schließlich die jährlichen Belastungen ausgehend von den heutigen Betriebskosten, ergänzt um die zusätzlichen Betriebskosten und den möglichen Einsparungen, die sich beide aus dem Projekt ergeben.
- Haushaltssicht
  Die Haushaltssicht zeigt die aus dem Projekt- und Betriebsteil abgeleite-

[1] Als haushaltswirksam werden Vorgänge bezeichnet, die zu einem Geldabfluss aus der Kasse führen (z.B. Bezahlen von Eingangsrechnungen); hingegen verursachen nicht haushaltswirksame Kosten keinen Mittelabfluss aus der Kasse (z.B. Personalabordnung oder -versetzung)

ten haushaltswirksamen und haushalts-nicht-wirksamen Anteile. Auch hier wird wieder in Kosten und Ersparnisse unterschieden. In der Position *„Liquiditätswirksam im 1. Jahr“* wird der Investitionsbedarf dargestellt. Hierin enthalten sind i. d. R. externe Personalkosten, Software- und Hardwarekosten, Schulung und Wartungskosten für das erste Jahr. Die Position *„Liquiditätswirksam ab dem 2. Jahr“* enthält die laufenden jährlichen Belastungen, die sich meistens aus der Software-Wartung ergeben.

Sämtliche Sichten werden auf der Basis der im Modell definierten Kostenartengruppen gefüllt und über einen bis zu 10-jährigen Zeitraum beginnend mit dem Startjahr gerechnet. In den Anbieterszenarien werden ausschließlich nominelle Werte[1] dargestellt. Diese Daten sind grundsätzlich kumulierte Werte über den Betrachtungszeitraum – es sei denn, in der jeweiligen Position deutet die Bezeichnung einen anderen Inhalt an.

Im Anhang (vgl. Tab. 67, S. 498 bis Tab. 70, S. 500) werden als Basis für die Berechnung der Wirtschaftlichkeit Beispielausschnitte aus der Projektmatrix abgebildet. Hier fließen sämtliche Kosten- und Ersparnis-Informationen ein. Diese Daten sind getrennt für die Bereiche Projekt, Betrieb und Ersparnis einzugeben. Auch eine Unterscheidung in haushaltswirksam und nicht haushaltswirksam ist hier vorgesehen.

Das nachfolgend dargestellte Beispiel enthält die drei Sichten. Die darin enthaltenen Ersparnisse resultieren aus einer angenommenen Optimierung der Kernprozesse und werden für alle Alternativen gleich gesetzt.

[1] Die für die jeweiligen Jahre geschätzten Kosten und Ersparnisse werden nominell ermittelt, d.h. sie werden nach den heute vorliegenden Preis- und Mengenstrukturen errechnet. Eine Diskontierung findet nicht statt.

Sicht	Bereich	Alt 1 Summe Betrachtg. Zeitraum	Alt 2 Summe Betrachtg. Zeitraum	Alt 3 Summe Betrachtg. Zeitraum
PS	**Projekt-Saldo Nominal**	**3.910.656**	**1.139.992**	**696.690**
PS Projekt-Sicht	**Projektkosten**	**-518.315**	**-1.116.261**	**-1.234.523**
	Personalkosten	-518.315	-1.116.261	-1.234.523
	Personalkosten - intern	-227.503	-206.821	-206.821
	Personalkosten - extern	-290.812	-909.440	-1.027.702
PS Projekt-Sicht	**Zusätzliche Betriebskosten**	**-602.096**	**-2.774.814**	**-3.099.855**
	Software Wartung	-438.536	-1.465.939	-1.938.465
	Software Invest (AfA)	-163.560	-1.308.874	-1.161.390
PS Projekt-Sicht	**Ersparnisse Projekte**	**5.031.067**	**5.031.067**	**5.031.067**
	Personalkosten	4.412.267	4.412.267	4.412.267
	Personalkosten - intern	4.412.267	4.412.267	4.412.267
	Externe Dienstleistungen	569.310	569.310	569.310
	Software Wartung	37.800	37.800	37.800
	Software Invest (AfA)	0	0	0
	Hardware Wartung	11.690	11.690	11.690
HS Haushalts-Sicht	**Kosten im Haushalt**			
	Liquiditätswirksam im 1. Jahr	**-509.189**	**-2.401.557**	**-2.431.400**
	Liquiditätswirksam ab 2. Jahr	-54.817	-183.242	-242.308
	Nicht Liquiditätswirksam	-227.503	-206.821	-206.821
HS Haushalts-Sicht	**Ersparnisse im Haushalt**			
	Liquiditätswirksam im 1. Jahr	0	0	0
	Liquiditätswirksam ab 2. Jahr	618.800	618.800	618.800
	Nicht Liquiditätswirksam	4.412.267	4.412.267	4.412.267
BS Betriebs-Sicht	**Ist-Betriebskosten**	**-2.321.600**	**-2.321.600**	**-2.321.600**
	Personalkosten	-1.614.400	-1.614.400	-1.614.400
	Personalkosten - intern	-1.614.400	-1.614.400	-1.614.400
	Externe Dienstleistungen	-650.640	-650.640	-650.640
	Software Wartung	-43.200	-43.200	-43.200
	Hardware Wartung	-13.360	-13.360	-13.360
BS Betriebs-Sicht	**Ersparnisse Betriebskosten**	**707.200**	**707.200**	**707.200**
	Externe Dienstleistungen	650.640	650.640	650.640
	Software Wartung	43.200	43.200	43.200
	Hardware Wartung	13.360	13.360	13.360
BS Betriebs-Sicht	**Neue Betriebskosten**	**-2.507.308**	**-5.298.654**	**-5.741.957**
	Personalkosten	-1.614.400	-1.614.400	-1.614.400
	Personalkosten - intern	-1.614.400	-1.614.400	-1.614.400
	Externe Dienstleistungen	-290.812	-909.440	-1.027.702
	Software Wartung	-438.536	-1.465.939	-1.938.465
	Software Invest (AfA)	-163.560	-1.308.874	-1.161.390

Bild 90: MiKoMa - Beispielhafte Übersicht dreier Alternativen

5.6.4 Vergleichs- und Rentabilitätsrechnung

Der Vergleich der Alternativen wird auf der Basis der im vorhergehenden Kapitel dargestellten Anbieterszenarien mit der gleichen Methodik vorgenommen. Zu-

nächst werden die verschiedenen Sichten auf der Basis nomineller Werte des Betriebes vorgestellt.

Anschließend folgt eine Break Even Grafik und die Rentabilitätsberechnung der einzelnen Projekte.

Nachfolgend einige Beispiele:

Bild 91: MiKoMa - Kosten Externer Anbieter

Bild 92: MiKoMa - Vergleich der nominalen Projektnutzen

Bild 93: MiKoMa - Rentabilitätsvergleich

Bild 94: MiKoMa - Break even Übersicht

5.7 Neueinführung vs. Migration von Systemen

Bei einer Kostenbetrachtung im Hinblick auf die Einführung neuer Technologien muss grundsätzlich zwischen der Neueinführung und der Migration von Verfahren und Systemen unterschieden werden. Dabei gilt als „Daumenregel“, dass eine Neueinführung grundsätzlich einfacher und preiswerter zu bewerkstelligen ist, als eine Migration, bei der verschiedene, zum Teil historisch gewachsene Architekturen abgelöst und Daten migriert werden müssen, ohne dass es zu einer wesentlichen Betriebsstörung oder zum Datenverlust der Altanwendung kommt.

Da ein Migrationsverfahren grundsätzlich von seiner Ausgangssituation abhängt, erweist sich eine allgemeingültige und allumfassende Aussage zu dessen Kosten als kaum möglich. Während eine Migration in einigen Fällen als problemlos und nahezu ohne Aufwand möglich ist, führt die Existenz von selbstentwickelten Anwendungen, die ebenfalls abgelöst werden müssen, Überführung von Altdaten, spezielle Nutzer- und Zugriffsrechtestrukturen oder andere Besonderheiten zu einem erheblichen Projektaufwand, der behördenspezifisch – auch unter Berücksichtigung der Kritikalität - beurteilt werden muss.

5.8 Gesamtergebnisse der Wirtschaftlichkeitsbetrachtung

Die meisten diesem Themenbereich gewidmeten Untersuchungen verwenden bei ihrer Analyse den Vollkostenansatz und erzielen Konsens in der Feststellung, dass ein wesentlicher Teil der Kosten nicht in den SW-Lizenzen, sondern in den mit der Einführung und mit dem Betrieb verbundenen Personalkosten liegt. Aufgrund der unterschiedlichen Annahmen – im Wesentlichen zur Administrierbarkeit von Systemen – kommen sie jedoch in ihrem Ergebnis zu gegensätzlichen Schlussfolgerungen, was die wirtschaftlichen Vorteile der Alternativen betrifft.

Die Untersuchungen im Rahmen des Migrationsleitfadens verweisen auf drei wesentliche und für die Überlegungen ausschlaggebende Faktoren der aus Sicht der Linux/OSS-Einführung notwendigen TCO-Betrachtung:

1. Anteil der Softwarelizenzkosten an den Gesamtkosten
2. Spezialisierungsgrad der in Frage kommenden IT-Systeme und Infrastrukturen
3. Automatisierungsgrad der in Frage kommenden IT-Systeme und Infrastrukturen

Der Anteil der Softwarelizenzen an den Gesamtkosten der IT-Systeme und Verfahren kann bis zu 50% betragen. In diesem Bereich bewegt sich somit zunächst einmal das unmittelbare und direkte Potenzial der Alternativen OSS und COLS gemessen in der rein monetären Dimension, unter der Prämisse einer gegebenen Vergleichbarkeit der erzielbaren Arbeitsergebnisse.

Neben der Aussage zum Anteil der SW-Lizenzen an den IT-Gesamtkosten ist es für die Betrachtung der tatsächlichen Spielräume der IT-Entscheider im weiteren Beurteilungsprozess hilfreich, zwei weitere Faktoren zu betrachten, einerseits den Index der direkt beeinflussbaren Kosten und andererseits die Analyse der haushaltswirksamen Kosten.

Zu den unmittelbar direkt beeinflussbaren Kostenarten zählen:

1. Beschaffungskosten Software:
   im Wesentlichen durch Wechsel auf preiswertere Produkte oder Verhandlung günstigerer Beschaffungspreise
2. Wartungskosten Software:
   im Wesentlichen durch Konsolidierung (Reduktion der Produktvielfalt) der Softwareprodukte oder Verzicht auf Update-Zyklen
3. Beschaffungskosten Hardware:
   durch Wechsel auf preiswertere HW-Plattformen
4. Wartungskosten Hardware:
   durch Konsolidierung (Reduktion der Produktvielfalt) der Hardware oder Verlängerung der Lebenszyklen

Anders als Hard- und Software gehört der größte Block der IT-Ausgaben, die Personalkosten, in der Regel nur zum Teil zu den unmittelbar direkt beeinflussbaren Kostenarten. Dies resultiert zunächst einmal aus der Tatsache, dass die Einführung und der Betrieb von IT-Infrastrukturen und –Systemen mit einer Grundlast verbunden ist, die weniger durch einzelne Lizenzmodelle und mehr durch Anforderungen an die Betreuungsintensität, Verfügbarkeit und Sicherheit der betriebenen Plattformen bestimmt wird. Die Reduktion existierender Personalkapazitäten oder deren Auslagerung und Konsolidierung stellt in der Regel keine kurzfristig mögliche Handlungsalternative dar.

In der Betrachtung der direkt beeinflussbaren IT-Kosten wird deutlich, dass die Lizenzkosten (SW-Beschaffung, -Wartung, -Updatedurchführung) den größten Teil und somit die größten Handlungsspielräume bilden.

An dieser Stelle sei einmal mehr darauf hingewiesen, dass sich pauschale Empfehlungen für das eine oder andere Migrationsszenario aus der Wirtschaftlichkeitsbetrachtung nicht belastbar ableiten lassen. Die Praxis zeigt sehr unterschiedliche Anforderungen bei vermeintlich gleichen Ausgangsbedingungen, so dass allgemeinverbindliche Aussagen hier keinen Sinn machen. Manche Orientierungen wurden trotzdem versucht zu geben (siehe Kapitel 5.3.3.2, S. 409), dort wo reale Projektinformationen verfügbar waren und sich entsprechende Trends ermitteln ließen. So ergibt sich die Notwendigkeit, jedes Migrationsprojekt nach den vorgeschlagenen Methodiken zu planen und die Wirtschaftlichkeit zu berechnen.

6 Migrationsempfehlungen

6.1 Grundsätzliche Aussagen

6.1.1 Weg der Entscheidungsfindung

Ausschlaggebend für eine Migrations- oder Weiterentwicklungsempfehlung sind die Ergebnisse einer langfristig angelegten Wirtschaftlichkeitsbetrachtung. Auch wenn aus technischer und juristischer Sicht der Weg für eine Komplett- oder Teilmigration ohne Einschränkungen möglich und gegeben ist, können wirtschaftliche Überlegungen ihn unter gegebenen Rahmenbedingungen als wenig sinnvoll erscheinen lassen. Aufgrund vielfältiger Zusammenhänge zwischen den einzelnen Komponenten und Systemen einer IT-Infrastruktur und der Anwendungswelt muss bei der Entscheidungsfindung daher stets eine langfristige Perspektive (vgl. Kapitel 5.2 Einleitung zu den Wirtschaftlichkeitsbetrachtungen) beachtet werden.

Dabei unterscheidet sich die Betrachtung aus dem Blickwinkel der Einführung der Open Source Software nicht von den üblichen Beurteilungsanalysen in der IT, beispielsweise im Kontext der Hardware- oder Softwarekonsolidierung. Die üblicherweise in den Verwaltungen und der Wirtschaft gleichermaßen verfolgten Strategien sind:

- Auf Basis von offenen Standards und Spezifikationen eng aufeinander abgestimmte System- und Anwendungsplattformen, gegebenenfalls unter zusätzlichem Einsatz von spezialisierten Integrationsprodukten
- Auf Basis von herstellerspezifischen (nicht oder nur zum Teil offen gelegten Schnittstellen und Spezifikationen) eng aufeinander abgestimmte System- und Anwendungsplattformen , ggf. unter Einsatz von herstellereigenen Integrationsprodukten
- (historisch) Einsatz von Insel-Lösungen zur punktuellen Abdeckung von Fachverfahren und –anwendungen.

Da die Open Source Software von ihrem Ursprung her häufig mit dem Einsatz von offenen Standards verbunden ist, bildet sie eine weitere besondere Variante hierzu:

- Auf Basis von offenen Standards und Spezifikationen aufeinander abgestimmte System- und Anwendungsplattformen mit Nutzung des offenen (wieder verwendbaren) Source Codes.

Während die Entscheidung zum punktuellen Einsatz eines weit verbreiteten quelloffenen Produktes wie beispielsweise des Webservers Apache in der Regel sehr pragmatisch und zügig entschieden werden kann, erfordert eine Entscheidung, beispielsweise zur flächendeckende Einführung von Open Source Software und Ablösung proprietärer Inseln, aufgrund ihrer langfristigen Tragweite eine methodische Vorgehensweise. Deren elementaren Meilensteine sind:

- Erarbeitung einer Gesamt-IT-Strategie unter Berücksichtigung der bestehenden finanziellen, organisatorischen, innovationsbedingten und personellen Zielsetzungen
- Definition der künftigen Open-Source-Plattform-Strategie unter Berücksichtigung der langfristigen Wirtschaftlichkeitsberechnungen im Hinblick auf den Einsatz von freien und kommerziellen Standardprodukten (OSS- vs. COLS-Modell, s. Abschnitt 6.1.2)
- Festlegung aller zur Sicherstellung der internen und externen Wiederverwendbarkeit sowie Interoperabilität notwendigen Standards in einem Blueprint-Katalog
- Auswahl der Produkte zur Abdeckung der Anforderungen
- Definition des Vorhabens mit dem dazugehörigen Zeit- und Aktionsplan, sowie Sicherstellung einer Budgetierung

Bei diesem Prozess kann für die einzelnen Phasen auf bereits gängige Methoden und Werkzeuge aus der Öffentlichen Verwaltung zurückgegriffen werden, wie die nachfolgende Abbildung darstellt.

Bild 95: Entscheidungsprozess zur Einführung von OSS

6.1.2 Grundsatzempfehlungen

Allgemeingültige Aussagen zu Wirtschaftlichkeitsvorteilen der Plattform-Strategien können aufgrund der unterschiedlichen Ausgangssituation (mit Existenz von Insel-Lösungen) und Produktqualität nur selten getroffen werden. Es gilt jedoch grundsätzlich, dass mit wachsendem Grad der Integration der Produkte einer Plattform die Wirtschaftlichkeit insgesamt aus mehreren Gründen zunimmt:

- durch höhere Produktivität, bei gut (ohne Systembrüche) aufeinander abgestimmten Produkten
- durch die wachsende Wiederverwendbarkeit von Komponenten und Lösungen, die mit gleicher Middleware-Technologie entwickelt wurden
- durch Einsparungen bei Vereinheitlichung von Beschaffungs- und Wartungsprozessen und gegebenenfalls -verträgen.

Darüber hinaus gilt, dass mit wachsendem Grad der Standardisierung auf Basis von offenen Standards die Wirtschaftlichkeit ebenfalls durch folgende Faktoren zunimmt:

- durch den einsetzenden Wettbewerb von Produkten und Lösungen
- durch eine geringere Herstellerabhängigkeit
- durch einen insgesamt breiteren Dienstleistungsmarkt.

Insbesondere (jedoch nicht ausschließlich) hat durch die Verabschiedung von SAGA (Standards- und Architekturen für e-Government Anwendungen) mit der verwaltungseigenen Hausstandardisierung die Investitionssicherheit für kommerzielle Anbieter der Linux-Software zugenommen. Dies spiegelt sich in einem wachsenden Softwareangebot für Basiskomponenten und Fachverfahren gleichermaßen wieder und macht das bis vor kurzem schwierige Szenario einer vollständigen Migration möglich.

Davon ausgehend können folgende Grundsatzempfehlungen zum Einsatz von quelloffenen Produkten formuliert werden:

- Empfehlung für die Verankerung der Wirtschaftlichkeit als Leitbild der Gesamt-IT-Strategie bei angemessener Berücksichtigung der Faktoren Innovation und Organisation
- Empfehlung für den Einsatz des Betriebssystems Linux als Grundlage der IT-Plattform für alle Anwendungsbereiche, falls die Voraussetzungen für eine Voll- oder Teilmigration zutreffen (s. Abschnitt 6.2 und 6.4)
- Empfehlung für den Einsatz von offenen, von IT-Industrie und Open Source Community gleichermaßen anerkannten Standards als Grundlage zur Auswahl und Integration von SW-Produkten zur Vermeidung extremer Herstellerabhängigkeiten
- Empfehlung zur Durchführung einer projektbezogenen Wirtschaftlichkeitsbetrachtung im Entscheidungsprozess für den Einsatz offener und kommerzieller Linux-Produkte (siehe hierzu Kapitel 4).

Grundsätzlich kann sich eine Umstellung auf die OSS-/COLS-Plattform als ökonomisch sinnvollere (rentablere) Variante erweisen gegenüber der fortführenden Migration auf eine neue Microsoft-Version.

Der Wegfall oder die Reduzierung von Lizenzkosten kann in mehreren Fällen zu direkten (monetären) Einsparungen führen, beispielsweise bei:

- Serverseitiger Teilmigration, verbunden mit einer HW- und SW-Konsolidierung, wenn Unix-Know-how und Unix-Systeme bereits vorhanden sind
- Punktueller Ablösung von Mitgliedern der ehemaligen Back-Office Familie (heute 2000/2003 Enterprise Server), beispielsweise Exchange oder SQL

Server, insbesondere mit größeren oder wachsenden Nutzer- und somit Lizenzzahlen

- Clientseitiger Teilmigration von MS Office Produkten, wenn die Nutzung von Office als Laufzeitumgebung für Makros oder Anwendungen die Ablösung nicht verhindert

In vielen anderen Einsatzszenarien müssen zur Beurteilung der Einsparungen die strategische Dimension herangezogen werden, auf die ausführlich im Kapitel Wirtschaftlichkeitsbetrachtung eingegangen wurde.

Bei der Umstellung der heutigen Plattformen in die Linux-Welt oder auf eine neue Microsoft-Ebene sind unter wirtschaftlichen Gesichtspunkten in jedem Fall Schulungsaufwendungen einzuplanen. Da diese realistischerweise für beide Alternativen anfallen, ist dieser Kostenblock als weitgehend neutral im direkten Vergleich der Alternativen zu betrachten. In jedem Fall, d.h. für beide Alternativen sind auch die Umstellungskosten der ggf. existierenden Fachanwendungen zu berücksichtigen[1].

Da die Grundsatzempfehlungen nicht die Anforderungen und Rahmenbedingungen einer konkreten Ausgangssituation berücksichtigen können, beziehen sich weitere Empfehlungen auf unterschiedliche Szenarien. Im Abschnitt 6.2 wird eine vollständige Migration, im Abschnitt 6.3 werden die Szenarien für die Fortführung der bisherigen Plattformen und im Abschnitt 6.4 die für eine gemischte Umgebung (Teilmigration) zusammengefasst.

6.2 Vollständig „Ablösende Migration“

Eine im Sinne dieses Migrationsleitfadens vollständige Migration findet mit dem Einsatz von Linux als Betriebssystem auf allen Komponenten der IT-Infrastruktur statt. Mit dem durchgängigen Wechsel der Betriebssysteme ist in der Regel auch eine Ablösung auf der Integrations- und Anwendungsebene durch SAGA-konforme Produkte verbunden, da insbesondere die dafür benötigten Java-Produkte auf Windows-Plattformen bisher nicht die erhoffte Verbreitung fanden[2].

Hier stehen für eine vollständige Migration grundsätzlich zwei Varianten der Software zur Verfügung, die häufig gemischt zum Einsatz kommen:

- OSS: Open Source Software (oder freie Software)[3]: quelloffene und kostenlose Software, entwickelt durch die OSS-Community

---

1 Dieser Kostenblock wird in die Betrachtungen des Migrationsleitfadens nicht mit einbezogen. In der Regel sind hierfür sehr spezifische Analysen bei den jeweiligen Behörden notwendig, die im Rahmen eines Leitfadens nicht geliefert werden können. Im Einzelfall können sich dargestellte Dimensionen im Rahmen der Wirtschaftlichkeitsbetrachtungen nach Einbezug von ermittelten Migrationskosten für Fachanwendungen verschieben.

2 Von der Notwendigkeit einer Ablösung sind die auch unter Windows verbreiteten Webanwendungen des (L)AMP-Modells in diesem Fall nicht betroffen

3 Siehe Definition in Kapitel 2

- COLS: COmmercial Linux Software: kommerzielle quelloffene oder proprietäre Software für Linux, als Angebot der SW-Hersteller.

Da in vielen Verwaltungsbereichen sowohl eigenentwickelte und auf Windows basierte Fachverfahren als auch ERP-basierte Anwendungssysteme intensiv genutzt werden, kann eine vollständige Abdeckung aller Anforderungen mit Open Source Software auf absehbare Zeit nur im Bereich der Infrastruktur erwartet werden. Unter Betrachtung der positiven Förderung von Linux durch die Verfügbarkeit großer Anwendungssysteme von Herstellern wie SAP oder Oracle, ist der Einsatz kommerzieller Software und das wachsende Linux-Softwareangebot für die Weiterentwicklung der Open Source Plattform insgesamt als positiv zu beurteilen und mit einem weiteren Schub für diese verbunden.

Die individuelle Ausprägung der möglichen und empfohlenen System- und Softwarearchitekturen unterscheidet sich in Abhängigkeit von der Größe, der IT-Intensität („Lastigkeit“) und dem Spezialisierungsgrad der Behörden. Hier spielen einerseits die Skalierbarkeit und Verfügbarkeit einzelner Komponenten als andererseits auch der mit der Einführung verbundene Aufwand eine ausschlaggebende Rolle.

Aus diesen Gründen werden die jeweiligen Schwerpunkte gesondert für <u>große</u> und <u>mittlere</u> sowie für <u>spezialisierte</u> und <u>kleine</u> Behörden betrachtet. Einleitend vorgestellt wird zunächst ein allgemeines und dadurch generisches Modell für Infrastruktur-Aufgaben.

6.2.1 Architekturmodell

Bei einem durchgängigen Einsatz von Linux als Plattform für Client- und Serveranwendungen können – analog zu den üblichen Unix- und Windows-Architekturen – zwei Typen von Client-Architekturen unterschieden werden: die Fat Clients und die Thin Clients.

Die im Bild 96 dargestellte Konfiguration ist stellvertretend für multifunktionsfähige Arbeitsplatzsysteme in einer dezentralen Architektur mit einem handelsüblichen PC (Fat Client). Die Server-Plattform deckt die üblichen Infrastrukturaufgaben ab, darüber hinaus vervollständigt ein Anwendungsserver in der 3-schichtigen Architektur das Bild.

Die ausgewählten Komponenten decken u.a. die folgenden Aufgabenbereiche ab:

- Arbeitsplatzrechner (Desktop und Office)
- Groupware (Mail & Kalender Server)
- Datenbanksysteme (DBMS Server)
- Webserver
- Dateiablage (File Server)
- Druckdienste (Print-Server)

- Authentisierungsdienste
- Netzwerkdienste (u.a. DNS & DHCP Server).

Bild 96: Systemarchitektur mit einem linuxbasierten Fat Client

Die in Bild 96 schraffiert dargestellten Bereiche können unabhängig von der Größe und dem Spezialisierungsgrad der jeweiligen Behörde eingesetzt werden. Die übrigen Systemkomponenten werden in den folgenden Abschnitten in Abhängigkeit der jeweiligen Einsatz-Szenarien betrachtet. Diese sind:

- Große und mittlere Behörden
- Spezialisierte Behörden mit IT-Dienstleistung
- Kleine Behörden.

Anmerkung: Für die betrachteten Migrationsszenarien sind generell einige Einschränkungen zu beachten:

Die technischen Betrachtungen zeigen, dass mit wenigen Ausnahmen zu allen Microsoft-Produkten, die Bestandteil der betrachteten Ausgangslage (siehe Kapitel 2.2.1) sind, alternative Lösungen aus dem Bereich der OSS bzw. der COLS-Produkte für eine Ablösende Migration zur Verfügung stehen. Als kritische Punkte erweisen sich:

- Die Kompatibilität zwischen OpenOffice.org/StarOffice und MS Office ist nicht vollständig gegeben. Dies hat insbesondere Auswirkungen für jene

Anwender, die häufig mit anderen Anwendern gemeinsame Dokumente erstellen müssen. Kommen in diesen Fällen beide Office-Varianten zum Einsatz, dann führt dies in der Regel zu Problemen bei der Formatierung.

- Die Chart-Engine von OpenOffice.org bzw. StarOffice weist nicht die gleiche Mächtigkeit auf wie die MS Excel Chart-Engine. Dies betrifft insbesondere die Erstellung von Charts auf Basis von Pivot-Tabellen.
- Zu einigen Produkten wie MS-Project oder Visio gibt es noch keine adäquate Alternative.

Einer Migration von Microsoft-Produkten zu OSS-Lösungen und COLS-Produkten können allerdings eher wirtschaftliche als funktionale Gründe entgegenstehen. Dies betrifft insbesondere die Migration des Desktops:

- MS Office
  Der Umfang und die Komplexität der zu migrierenden Makros, Skripte, Vorlagen und Dokumente kann eine Migration nach OpenOffice.org oder StarOffice unwirtschaftlich machen.
- MS Office Professional
  Analoge Konvertierungsproblematik gilt für MS Access und die zu migrierenden Access-Anwendungen, die häufig zur Abdeckung einfacher Vorgangsautomatisierung benutzt werden.
- Fachanwendungen
  Abhängig vom Grad der Nutzung von nativen Windows-Fachanwendungen kann im ungünstigen Fall eine ablösende Migration bis zur Verfügbarkeit von Alternativprodukten verhindert werden. (siehe Kapitel 6.3). Dies gilt auch für Anwendungen, die auf Basis von MS-Exchange erstellt wurden und es als Laufzeitsystem nutzen.

6.2.1.1 Arbeitsplatzrechner

Der Betrieb der Arbeitplatzrechner erfolgt auf Linux-Basis, eine Empfehlung für eine bestimmte Distribution (siehe Kapitel 2.2.4) kann an dieser Stelle nicht gegeben werden. Die Entscheidung ist im Einzelfall zu treffen und abhängig von den spezifischen Anforderungen der jeweiligen Verwaltung. Für den Einsatz im Office-Bereich kann sowohl OpenOffice als auch StarOffice empfohlen werden, die Entscheidung für das eine oder andere Produkt ist von den spezifischen Anforderungen der jeweiligen Behörde abhängig. Ebenso wie Microsoft Office bieten StarOffice und OpenOffice die für die tägliche Arbeit notwendigen Anwendungen (Textverarbeitung, Tabellenkalkulation, Präsentation) und decken die funktionalen Anforderungen ab. Für die als COLS-Produkt erhältliche StarOffice Suite hat die Firma Sun zusätzliche Komponenten (TrueType Fonts, eigene Rechtschreibprüfung, zusätzliche Vorlagen und eine Bildergalerie, ADABAS Datenbank) entwickelt bzw. hinzugenommen. OpenOffice.org dagegen ist ein Mit-

glied der OSS-Familie und erfordert keine Lizenzkosten. Die funktionalen und technischen Unterschiede zwischen den beiden Office-Paketen sind marginal.

Eine weitere wichtige Benutzerschnittstelle für den Anwender ist das eigentliche Desktopsystem. Innerhalb der Linux-Distributionen sind in der Regel für die Anwender fertige Desktops implementiert, die ebenso wie auf dem Windows-Desktop die wichtigsten Anwendungen beinhalten. Die beiden wichtigsten Vertreter der Desktop-Systeme sind KDE und GNOME. Die Auswahl des Desktop-Systems ist in erster Linie eine Frage des persönlichen Geschmacks und der jeweiligen Vorlieben für bestimmte Anwendungen.

6.2.1.2 Webserver

Der Apache-Webserver (siehe auch Kapitel 3.10.4) ist zurzeit der Maßstab für die Bereitstellung von Internet- und Intranetinhalten. Die Flexibilität durch den modularen Aufbau und die Anzahl der verfügbaren Module hat ihn zum Marktführer innerhalb des Webserver-Bereiches gemacht. Die Komponente zeichnet sich durch den langjährigen Einsatz in großen produktiven Umgebungen, die Stabilität, die umfassenden Sicherheitsfunktionalitäten und dem in großem Maße verfügbaren und frei wählbaren professionellen Support aus.

6.2.1.3 Dateiablage

Für die Dateiservices innerhalb einer linuxbasierten Systemlandschaft wird das bewährte Network File System (NFS) empfohlen. NFS wird traditionell für die netzwerkgestützte Dateiablage in UNIX-Netzwerken eingesetzt. NFS ist das Standardprotokoll, wenn Verzeichnisse von verschiedenen Unix-Systemen gemeinsam genutzt werden sollen. Den Nutzern können mittels zentraler oder dezentraler Server die benötigten Verzeichnisbereiche zur Verfügung gestellt werden. Die exportierten Verzeichnisbäume werden auf den entsprechenden Arbeitsplatzrechner der Mitarbeiter automatisch eingebunden.

Für eine physikalische Speicherung der Daten auf den Plattensystemen der eigentlichen Server werden die Dateisysteme XFS und EXT3 empfohlen. Beide Systeme unterstützen Journaling-Funktionalitäten, Quotas und die Vergabe von Zugriffberechtigungen auf Datei- und Verzeichnisebene.

6.2.1.4 Druckdienste

Für die Bereitstellung der Druckdienste wird ausschließlich das „Common UNIX Printing System (CUPS)“ empfohlen. Es ist auf praktisch allen Unix-Systemen etabliert und der de-facto Standard aller großen Distributionen (Suse, Debian, RedHat, usw.). Der Druckdienst CUPS bietet alle notwendigen Funktionalitäten für die Bereitstellung einer Druckinfrastruktur. CUPS unterstützt eine Vielzahl von unterschiedlichen Druckgeräten und ist in der Lage, die spezifischen Druckoptionen den jeweiligen Benutzern bereitzustellen. CUPS basiert auf dem Internet Printing Protocol, dem definierten neuen Standard für das Drucken sowohl im lokalen Netz (LAN) wie auch im großräumigen Netz (WAN, Internet).

6.2.1.5 Netzwerkdienste

Die infrastrukturbildenden Dienste für TCP/IP-basierte Netzwerke sind aufgrund ihres Unix-Ursprungs in Open Source Software standardmäßig vorhanden. Für die Realisierung des Domain Name System wird die Referenzimplementation BIND (Berkeley Internet Name Domain) empfohlen, für DHCP wird ebenfalls auf die Referenzimplementation vom Internet Software Konsortium verwiesen.

6.2.2 Mittlere und große Behörden

Mittlere und große Behörden zeichnen sich durch ihre besonderen IT-Architekturen aus und benötigen in einigen Einsatzgebieten andere Migration-Empfehlungen als kleinere Verwaltungen. Ab einer gewissen Größe verfügen die Behörden in der Regel sowohl über dezentrale als auch zentrale IT-Architekturen. Die ersten werden meist für zentrale Verfahren (ERP, KLR, usw.) der Behörden eingesetzt. An die einzelnen Systemkomponenten, auf deren Basis die zentralen Verfahren realisiert wurden, werden besonders hohe Anforderungen in Hinblick auf IT-Sicherheit, Leistungsfähigkeit und Skalierbarkeit gestellt. Die intern definierten Qualitätsstandards erfordern eine hohe Verfügbarkeit und bedingen eine intensive Betreuung der zentralen Komponenten und der Benutzer. Solche Aufgaben können nur durch einen intensiven Einsatz von Systemmanagement-Plattformen insbesondere zum Netzwerk- und Systemmonitoring gewährleistet werden.

Dezentrale Architekturen finden sich in erster Linie bei der Bürokommunikation, Dokumentbearbeitung und spezifischen Fachanwendungen innerhalb der Verwaltungen wieder. So werden häufig dezentrale Datenbank-, Mail- und Dateisysteme auf Abteilungsebene eingesetzt. Die dezentralen Systeme erfordern besondere Replikationsmechanismen und eine dezentrale Systemadministration.

Für die Realisierung der spezifischen technischen und architektonischen Anforderungen werden, neben den in Kapitel 6.2.1 genannten Komponenten, insbesondere Komponenten empfohlen, die an die besonderen Anforderungen großer Umgebungen angepasst sind.

Bild 97: Empfohlene IT-Architektur einer großen Behörde bei vollständiger „Ablösender Migration“

6.2.2.1 Datenbankmanagementsysteme

Die Anforderungen an Datenbankmanagementsysteme innerhalb großer zentraler IT-Architekturen unterscheiden sich insbesondere in Hinblick auf die Erhöhung der Stabilität, der Performance und der Sicherheit.

Von den reinen Open Source Datenbanksystemen ist die MaxDB in Hinblick auf die Anforderungen größerer Verwaltungen zu empfehlen. Die MaxDB wird nach wie vor von der SAP (siehe auch Kapitel 3.11.4) als zertifizierte Plattform für das R/3-System und dessen Nachfolger zur Verfügung gestellt und als Kerntechnologie in eigenen Produkten eingesetzt. Zum Funktionsumfang gehören neben Transaktionsunterstützung auch Trigger und Stored Procedures.

Sollten noch weitergehende bzw. ergänzende Funktionalitäten erforderlich sein, ist auch der Einsatz von kommerziellen Standardprodukten für Linux (COLS) empfehlenswert. Standardprodukte für Linux werden mittlerweile von vielen Herstellern angeboten. Dazu gehören die Produkte von IBM (DB2) oder Oracle.

6.2.2.2 Groupware

Eine gut skalierbare Groupware-Lösung auf Linux-Basis für große Umgebungen wird mit Samsung Contact (COLS-Produkt) geboten. Aufgrund seiner Architektur, die aus mehreren voneinander unabhängigen Komponenten besteht, die sich im Sinne einer horizontalen Skalierung auch auf mehrere Server verteilen lassen,

können die besonderen Anforderungen in großen Umgebungen gut bewältigt werden. Samsung Contact unterstützt, neben einer Single-Server Installation, auch eine verteilte Installation über mehrere Standorte hinweg und bietet somit auch für verteilte Standorte eine skalierbare Lösung.

Eine weitere potentielle Lösung für den Groupewarebereich auf Linux-Basis bietet OpenGroupware. Zur Unterstützung einer großen Anzahl von parallel arbeitenden Nutzern besteht die Möglichkeit der horizontalen Skalierung durch die Verwendung eines Software Loadbalancers[1]. Die Unterstützung des linuxbasierten Kontact-Clients, wird jedoch erst in der folgenden Version realisiert sein und schränkt die Nutzung in einer reinen Linux-Umgebung zurzeit noch ein. In einer vergleichbaren Situation befindet sich auch die Lösung von Scalix, die über ähnlich Skalierungsmöglichkeiten wie Samsung Contact verfügt, jedoch zur Zeit von keinen Linux-Client vollständig unterstützt wird.

6.2.2.3 Verzeichnisdienste

Aufgrund ihrer zentralen Rolle für die Sicherstellung der Effizienz des Systemmanagements und der IT-Sicherheit, erfüllen die Verzeichnisdienste eine entscheidende Rolle bei der Integration von Anwendungen und Systemen zu Plattformen.

Mit der wachsenden Bedeutung von Authentisierungsdiensten für Webanwendungen sowie wegen gestiegener Anforderungen an den Komfort der Authentisierung wurde das bereits aus der Vergangenheit bekannte Modell der Directories (Verzeichnisdienste) und Meta-Directories um weitere Komponenten ergänzt und in das häufig als Identity Management genannte Gesamtbild überführt (s. auch die nachfolgende Abbildung).

Bild 98: Anwendungsfelder der Directory-Services am Beispiel der SunOne Plattform

[1] Der Loadbalancer steht im Rahmen des Hersteller Maintenanceservice zur Verfügung.

Grundsätzlich können für Aufbau von Directory-Services sowohl OSS als auch COLS Produkte verwendet werden. Dabei sind zwei wesentliche Anwendungsszenarien erkennbar:

1. Realisierung von Basisfunktionen zur Authentisierung sowie Profil-Verwaltung auf Basis des LDAP-Protokolls.

   In diesem Fall ist die OSS-Alternative OpenLDAP in der Betrachtung in der Regel als ausreichend und wirtschaftlich zu sehen.

2. Realisierung von erweiterten Funktionen zur Steigerung der Management-Effizienz, z.B. durch eine anwendungsübergreifende Synchronisierung von Nutzerdaten oder Authentisierung.

   In diesem Fall kann generell davon ausgegangen werden, dass der Einsatz von kommerziellen Produkten zu Vorteilen bei der Wirtschaftlichkeitsbetrachtung gegenüber der Eigenentwicklung führen wird.

6.2.2.4 Systemmanagementdienste

Durch die erhöhten Anforderungen in Hinblick auf das Systemmanagement bietet sich beispielsweise der Einsatz der Systemmanagementprodukte Tivoli oder OpenView an. Neben den genannten kommerziellen Lösungen gibt es weitere Möglichkeiten, das Management mit den Betriebssystemwerkzeugen für bestimmte Aufgaben des Systemmanagement einzusetzen (siehe Kapitel 3.6).

6.2.3 Spezialisierte Behörden mit IT-Dienstleistung

Behörden, die unter anderem auch als spezialisierte IT-Dienstleister innerhalb der Verwaltungslandschaft auftreten, verfügen in der Regel über stark zentralisierte IT-Architekturen. Oftmals realisieren sie ihre Angebote im Rahmen von Rechen- und Datenzentren und übernehmen IT-Dienstleistungen für andere Verwaltungen, z.B. als so genannter „Application Service Provider“ (ASP). Die vorherrschenden zentralen Architekturen zur Realisierung der jeweiligen Fachverfahren (ERP, ...) sind häufig verbunden mit sehr hohen Anforderungen an die Leistungsfähigkeit und Skalierbarkeit der Systeme. Zum Einsatz kommen deshalb oft hochwertige und z.T. hochpreisige Hardware-Systeme, geeignet für den automatisierten Rechenzentrumsbetrieb, beispielsweise Storage Area Networks (SAN) zur Sicherung und Archivierung von Daten. Diese spezialisierten Behörden legen sehr hohe Maßstäbe an IT-Sicherheit, Leistungsfähigkeit und Skalierbarkeit. Die dort definierten Qualitätsstandards, die in der Regel auch vertraglich mit den jeweiligen Kunden festgeschrieben sind, fordern eine hohe System-Verfügbarkeit und eine intensive Nutzerbetreuung. Für ein effektives Systemmanagement werden spezielle Systemmanagement-Plattformen eingesetzt, die einen hohen Automatisierungsgrad bieten. Zusätzlich benötigen die Rechenzentren eine effektive Systemunterstützung beim First- und Second-Level Support inklusive eines umfangreichen Problemmanagements.

Bild 99: Empfohlene IT-Architektur einer spezialisierten Behörde bei vollständiger „Ablösender Migration“

6.2.3.1 Datenbankmanagementsystem

Für die Datenbankmanagementsysteme gelten die gleichen Empfehlungen wie in Abschnitt 6.2.2.1. Die Rechenzentren fordern ergänzend, dass Systeme für bestimmte Hardware (SAN) und Software zertifiziert sein müssen, damit sie zum Einsatz kommen dürfen. Viele linuxbasierte Datenbanksysteme (MaxDB, Oracle, DB2, usw.) verfügen mittlerweile über diese Zertifizierungen. Zusätzlich können Rechenzentrumsbetreiber auf zertifizierte Linux-Distributionen, als Betriebsystembasis für die jeweiligen Anwendungen, zurückgreifen.

6.2.3.2 Applikationsserver

Für komplexe Anwendungsszenarien werden häufig Applikationsserver eingesetzt. Diese realisieren innerhalb der Fachanwendungen komplexe Geschäftsvorgänge und -regeln sowie gleichzeitig den Zugriff auf externe Systeme. Der Applikations-Server muss in der Lage sein, das Session-Management für die Benutzer zu gewährleisten, passende Schnittstellen zu externen Anwendungen zu bieten und über die notwendige Hochverfügbarkeit-Lösungen (Cluster, Load-Balancing, Failover) zu verfügen. Neben den bekannten kommerziellen Produkten (COLS) wie z.B. IBM Websphere, BEA Weblogic, Oracle Application Server und einigen anderen besteht auch die Möglichkeit, eine OSS-Lösung einzusetzen. Das Projekt „JBoss“ bietet einen vollständigen Java-Applikations-Server auf

Open Source Basis an. Der Applikations-Server unterstützt die J2EE-Spezifikation beinhaltet einen integrierten Webserver, eine JSP und Servlet-Engine, Unterstützung von Enterprise Java Beans und eröffnet Clustering und zahlreiche weitere Funktionalitäten.

6.2.3.3 Systemmanagementdienste

Für die spezialisierten Behörden werden aufgrund der zum Teil vergleichbaren Anforderungen die gleichen Empfehlungen wie für die großen und mittleren Behörden gegeben (siehe Abschnitt 6.2.2.4).

6.2.4 Kleine Behörden

Kleine Verwaltungen verfügen i.d.R. aufgrund ihrer lokalen Konzentration über zentrale IT-Architekturen jedoch ohne Rechenzentrums-Charakter. Großverfahren werden in der Regel nicht im eigenen Haus betrieben. Häufig werden diese Leistungen im Miet-Modell über die Rechenzentren ausgelagert. Die definierten Qualitätsstandards innerhalb der Behörde entsprechen keinen besonderen Anforderungen an die Verfügbarkeit und Nutzerbetreuung (normale Arbeitszeiten). Für die Sicherung und Archivierung kommt normalerweise Standard-Hardware zum Einsatz. Selten werden Systemmanagement-Plattformen eingesetzt, bevorzugt werden die Aufgaben mittels einzelner Werkzeuge und mit Hilfe von Skripten gelöst. Die kleineren Verwaltungen weisen niedrige bis mittlere Anforderungen an die IT-Sicherheit, Leistungsfähigkeit und Skalierbarkeit auf. Der First- und Second-Level Support ist häufig zusammengeführt und erfolgt in der Regel ohne Unterstützung eines Problemmanagement-Tool.

Es ist nicht so, dass OSS-Produkte immer auf die Größe zugeschnitten werden müssen. Skalierbare Produkte wie Samsung Contact oder SunOne Directory Server können alle Anforderungen kleinerer Behörden abdecken. Es ist jedoch im Sinne einer Empfehlung zu bedenken, dass große Lösungen i.d.R. einen Mehraufwand an Installation und Konfiguration benötigen.

Bild 100: Empfohlene IT-Architektur einer kleinen Behörde bei vollständiger „Ablösender Migration“

6.2.4.1 Datenbankmanagementsysteme

Das Angebot an alternativen Datenbanksystemen im Open Source Bereich ist sehr vielfältig. Alle Datenbanksysteme, die detaillierter im Kapitel 3.11.4 betrachtet werden, eignen sich gut für den Einsatz innerhalb des skizzierten Rahmens.

Eine pauschale, einfache und eindeutige Empfehlung für MaxDB, Ingres, My SQL oder PostgreSQL lässt sich aus den funktionalen Eigenschaften nicht ableiten. Die Entscheidung für das eine oder andere Datenbanksystem muss im Einzelfall und jeweils in Abhängigkeit von der geplanten Entwicklungs- und/oder Laufzeitumgebung getroffen werden. Insbesondere im Kontext der Entwicklung von DB- und Web-Anwendungen mit PHP-Mitteln stellt jedoch aufgrund der engen Integration bekannter weise MySQL eine optimale Lösung dar.

6.2.4.2 Groupware

Für den Bereich der kleineren Verwaltungen stehen vielfältige Lösungen zur Verfügung. Eine pauschale und eindeutige Empfehlung kann an dieser Stelle nicht getroffen werden, unabdingbar ist im Falle einer Migrationsplanung eine entsprechende Detailprüfung. Sicherlich stellt die Kolab-Lösung (siehe Kapitel 3.12.4.2) für kleinere bis mittlere Organisationen eine adäquate Basis dar. Vorteil der Kolab-Lösung ist die tiefe Integration des GNU/Linux-Groupware-Client in den KDE-Desktop. Somit wird eine Lösung geboten, die unter der GPL steht und somit

auch in Hinblick auf die monetären Aspekte eine interessante Alternative darstellt. In diesem Zusammenhang muss darauf hingewiesen werden, dass dabei das Open Source Plug-In „Ägypten“, ein SPHINX-konformes Werkzeug zur Verschlüsselung und Signierung von E-Mails, eingesetzt werden kann. Weitere Varianten stellen die OpenGroupware- und OpenXchange-Lösungen dar. OpenXchange (siehe Kapitel 3.12.4.5) verfügt über eine Anbindungsmöglichkeit an den linuxbasierten Kontact-Client, diese wird in der zukünftigen Version des Groupwareclients auch für OpenGroupware (siehe Kapitel 0) zur Verfügung stehen.

Behörden, die keinen Bedarf hinsichtlich einer Offline-Nutzung der Groupware-Lösung haben, können auch einen Web-Client Zugang nutzen. In diesem Fall stellen phpGroupware, Scalix, OpenGroupware und Open-Xchange ebenfalls mögliche Lösungen dar.

6.2.4.3 Verzeichnisdienst

Für die Verwaltung von netzwerkrelevanten Informationen ist der OSS-Verzeichnisdienst OpenLDAP zu empfehlen. Der Dienst kann u. a. zur Nutzerverwaltung, der Benutzer-Authentifizierung, der Inventarisierung der vorhandenen Hardware und weiteren infrastrukturellen Einstellungen (DNS-Einträgen, DHCP-Konfigurationen, usw.) verwendet werden. OpenLDAP bietet alle gängigen und notwendigen Funktionalitäten (siehe Kapitel 3.7.4) eines vollwertigen Verzeichnisdienstes.

6.2.4.4 Systemmanagementdienste

Für kleinere Verwaltungen wird in erster Line der Einsatz der unter Linux zur Verfügung stehenden umfangreichen freien Bord-Mittel empfohlen. Die Werkzeuge (ssh, cron/at, mächtige Kommandozeileninterpretern, Utilities und interpretierten Programmiersprachen) können zur weitgehenden Automatisierung von Routinearbeiten herangezogen werden können. Weitere Werkzeuge und Produkte zur Systemverwaltung werden im Kapitel 3.6 vorgestellt.

6.3 Vollständig „Fortführende Migration“

Vollständig fortführend meint, dass in allen Bereichen die Produktlinie von Microsoft beibehalten werden sollte. Theoretisch lassen sich zwei Ausgangssituationen vorstellen, die eine solche Migration begründen.

In keiner der beiden nachfolgend beschriebenen Situationen sind jedoch technische Gründe ausschlaggebend. Mit wenigen Ausnahmen gibt es für jede der betrachteten Anforderungen technische Alternativen, die unter Linux betrieben werden können. Letztendlich sind es wirtschaftliche Gründe, die eine vollständige „Fortführende Migration“ bedingen.

Die erste hier betrachtete Ausgangssituation wurde im Kapitel 2 des Leitfadens beschrieben als eine NT 4 Systemumgebung mit Exchange 5.5, MS SQL Server 7, IIS 4 und Office 97 bzw. Office 2000. Sie ist bereits geprägt durch einen sehr hohen Grad an Integration. Kenngrößen für den Grad der Integration sind u.a.:

- Anzahl der Fachverfahren, die nur als Windows-Anwendungen verfügbar sind
- Die Verfügbarkeit der Quellcodes dieser Fachverfahren
- Integrationstiefe der einzelnen Fachverfahren, insbesondere in die MS Office-Umgebung
- Der Umfang der Verwendung Microsoft-spezifischer
  - Entwicklungsumgebungen
  - Schnittstellen
  - Programmiersprachen
- Anzahl der MS Office spezifischen Makros und Scriptings (z.B. Implementation von abteilungsübergreifenden Workflows).

Der Aufwand für eine ablösende Migration steigt mit zunehmenden Grad an Integration. Eine abschließende Aussage, welcher Grad an Integration letztendlich eine fortführende Migration begründet, kann nur durch eine detaillierte Einzelbetrachtung der zu migrierenden Komponenten und über die Ergebnisse einer tiefgehenden Wirtschaftlichkeitsbetrachtung herbeigeführt werden.

In der Praxis wird es durch die fortschreitende Entwicklung der .NET-Plattform eine Ausgangssituation geben, die einen so hohen Grad an Integration aufweist, dass eine Migration erheblich erschwert wird. Durch eine rechtzeitige Teilmigration (siehe Kapitel 6.4) kann dieser Entwicklung vorgebeugt werden.

Bild 101: Ausgangssituation für eine Fortführende Migration

Die zweite hier betrachtete Ausgangssituation beschreibt eine IT-Umgebung, die schon eine vollständige Migration nach Windows 2000 und eine umfassende Implementation von Active Directory vollzogen hat (siehe Bild 101). Die Umstellung wurde erst vor kurzem, z.B. im Jahre 2002, durchgeführt. Bezogen auf das in den Migrationsempfehlungen zugrunde liegende Architekturmodell (6.2.1) bedeutet dies, dass im Maximalfall folgende Ausprägung des Modells vorliegt:

- Arbeitsplatzrechner: Windows 2000 Clients mit Office 2000
- Webserver: Internet Information Server 5
- Datenbankserver: MS SQL Server 2000
- Groupware/Messaging: Exchange 2000
- Verzeichnisdienst: Active Directory Service
- Infrastrukturdienste:
  Windows 2000 Server (Advanced Server)
  (Dateiablage, Druckdienste und Netzwerkdienste).

Sollten einzelne Elemente dieser Architektur (noch) nicht im Einsatz sein, können im Rahmen der Teilmigration adäquate Lösungen dafür vorgeschlagen werden. Hierzu gibt das Kapitel 6.4 weitere Hinweise und Empfehlungen.

Der Grundsatz des Investitionsschutzes begründet für die o.g. Ausgangssituation, dass für bereits im Einsatz befindliche Komponenten keine ablösende Migration, auch nicht als Teilmigration, innerhalb der nächsten 4 - 5 Jahre empfohlen werden kann.

Aspekte warum eine solche Ausgangssituation in den Migrationsempfehlungen dennoch betrachtet wird, sind:

- Diesen Behörden werden nachfolgend Wege aufgezeigt, wie sie den oben erwähnten Grad an Integration und damit die Abhängigkeit von Microsoftprodukten minimieren können.
- Diesen Behörden werden nachfolgend weiterhin Empfehlungen bezüglich des späteren Migrationspfades gegeben, soweit das heute möglich ist.
- Unter langfristigen wirtschaftlichen Gesichtspunkten ist die fortführende Migration insbesondere vor dem Hintergrund der Herstellerabhängigkeit nicht besonders empfehlenswert. Die fortführende Migration kann vor allem dann sinnvoll sein, wenn die Umstellungskosten für Fachanwendungen, die auf der Microsoft-Plattform aufbauen und für eine Umstellung auf OS neu programmiert werden müssten, eine langfristige Rentabilität der Umstellung auf OS nicht darstellbar erscheinen lassen.

6.3.1 Minimierung des Grades an Integration, Bewahrung von Freiheitsgraden

Wie bereits ausgeführt, sollte das Ziel bei einer fortführenden Migration und Nutzung von Windows 2000/2003 einschließlich AD die Reduzierung der Abhängigkeiten von Microsoft-Produkten sein, um auch in Zukunft alle Möglichkeiten einer ablösenden Migration nutzen zu können. Es sollten folgende Empfehlungen berücksichtigt werden:

Verzeichnisdienst:

- Die Nutzung des Active Directory sollte, wenn überhaupt, nur als „Active Directory in minimaler Ausprägung“ vorgenommen werden (siehe Ausführung 3.7.5).
- Das AD sollte nicht als LDAP-Quelle für zusätzliche Anwendungen (z.B. Webanwendungen) eingesetzt werden.
- Personendaten des AD sind aus einer gesonderten Quelle z.B. einem MetaDirectory zu übernehmen bzw. zu füllen.
- Sofern Rollenkonzepte geplant sind, ist die Verwendung von Software, die ein AD voraussetzen oder als Hauptfokus haben, zu vermeiden.

Desktop

- Der Einsatz von MS Access-Anwendungen sollte vermieden werden. Die Nutzung einer zentralen Datenbank und Anwendungen, die z.B. mit PHP programmiert wurden, sind vorzuziehen.
- Es ist sinnvoll, die vorhandenen VBA-Anwendungen aufzunehmen, detailliert zu analysieren und zu konsolidieren, sofern dies nicht schon bei der Migration durchgeführt wurde. Neuentwicklungen in diesem Bereich sind nach Möglichkeit zu vermeiden.
- Die Auswahl von Anwendungen und Beauftragung von Anwendungsentwicklung ist unter dem Aspekt der SAGA-Konformität vorzunehmen.
- Anwendungen von Drittherstellern, die MS Office Produkte als einzige Laufzeitumgebung voraussetzen, sind nach Möglichkeit nicht zu verwenden. Ausgenommen davon sind Spezialanwendungen, wenn auch mittelfristig keine Alternativen vorhanden sind.
- (Fach)anwendungen die MS Office Produkte voraussetzen, sollten sukzessive umgestellt werden.

Dateiablage

- Die Reproduzierbarkeit der Rechtestruktur ist durch den Einsatz von Skripten (z.B. Perl) sicherzustellen. Bei der Verwendung der grafischen Oberfläche ist es zwingend notwendig, dass alle Konfigurationen detailliert und vollständig dokumentiert werden. Da dies aufgrund bekannter

menschlicher Schwächen nicht immer gewährleistet werden kann, ist die Skriptform der bessere Weg.

- Auf die Verwendung von lokalen Gruppen ist, wenn keine zwingende Notwendigkeit besteht, zu verzichten.

Groupware/Messaging

- Exchange 2000 Server sollten nicht als zentrale Mail-Router zum Einsatz kommen. Hierfür sollten OSS Produkte (z.B. Postfix, Sendmail) eingesetzt werden, um die Möglichkeit offen zu halten, mehrere Mail Systeme parallel betreiben zu können.
- In öffentlichen Ordnern von Exchange sollten keine Anwendungen eingesetzt werden.

Webanwendungen

- Mit Blick auf SAGA-Konformität und die Vielzahl der Alternativen sollten Microsoft Produkte nicht eingesetzt werden (siehe Kapitel 3.10)
- Domänen-Authentifizierung sind durch Einsatz einer zweiten Authentifizierungsinstanz zu vermeiden. Ein zusätzliches Kennwort kann i.d.R. akzeptiert und vor allem durch Sicherheitsaspekte begründet werden, bei Ausnahmesituationen kann auf eine Vielzahl von OSS-Produkten zurückgegriffen werden.

Systems Management

- Der Einsatz von Dritthersteller-Produkten, die auch Linux unterstützen (z.B. Tivoli) ist vorzuziehen.

Netzwerkdienste

- Bei den Netzwerkdiensten DHCP und DNS sind OSS-Lösungen zu bevorzugen.

Middleware

- Für Anwendungsentwicklung ist zur Erhöhung der Wiederverwendbarkeit die *tiefe Integration* mit Saga-konformen Standards zu bevorzugen.
- Für die Kommunikation und Datenaustausch mit externen Systemen sollten XML und Web-Service-Technologien zum Einsatz kommen.

6.3.2 Weitere Migrationspfade

Hinsichtlich einer weiteren Migration ist zunächst die Migration der Arbeitsplatzrechner nach Windows XP zu betrachten. Auch hier gilt der Grundsatz des Investitionsschutzes. Damit kann eine Migration der Arbeitsplatzrechner nach Windows XP allein schon aus diesem Grunde bei der oben beschriebenen Ausgangslage nicht empfohlen werden.

Unter Berücksichtigung des Investitionsschutzes steht eine weitere Migration frühestens nach 4-5 Jahren wieder an. Wenn also im Jahre 2002 migriert wurde,

könnte die nächste Umstellung frühestens im Jahre 2006 erfolgen. Insbesondere für die Behörden, die den zuvor aufgeführten Empfehlungen zur Minimierung der Abhängigkeit von Microsoft-Produkten gefolgt sind, besteht die Notwendigkeit zur Prüfung unter den dann gültigen technischen und wirtschaftlichen Bedingungen, ob eine ablösende oder eine fortführende Migration durchgeführt werden soll. Das Gleiche gilt für alle anderen Behörden, die sich in der gleichen Ausgangslage befinden.

6.4 Teilmigration

6.4.1 Punktuelle Migration

Die punktuelle Migration ist die dauerhafte Ablösung einer ausgewählten Systemkomponente weg vom Microsoft-Produkt hin zu einer OSS- bzw. COLS-Lösung, bei einer ansonsten Fortführenden Migration. In dem folgenden Abschnitt werden sinnvolle und machbare punktuelle Migrationen dargestellt.

Die wichtigste punktuelle Migration ist dabei die Ablösung von Exchange 5.5. Der Grund dieser Ablösung liegt darin, dass nach heutigem Stand der (Mainstream)[1] Support für Exchange 5.5 durch Microsoft eingestellt wurde. Die Alternative, die Microsoft im Rahmen einer fortführenden Migration bietet, ist Exchange 2003. Eine fortführende Migration nach Exchange 2003 kommt für viele Behörden aber nicht in Frage, weil diese Lösung zwingend den Einsatz von Active Directory fordert. Mit Exchange 2003 hat Microsoft eine Verlagerung des internen Verzeichnisdienstes von Exchange 5.5 nach außen vorgenommen und daraus das Active Directory entwickelt und zum Kern der Windows 2000 - Welt gemacht. Damit kann Exchange 2000 auch nur auf Windows 2000 Server betrieben werden.

Damit haben viele Behörden ein ernsthaftes Interesse an einer adäquaten alternativen Groupware/Messaging-Lösung, die einen ähnlichen oder gleichen Funktionsumfang bieten, die kein AD fordern und bei den MS Outlook als Client weitergenutzt werden kann.

Hier stehen insgesamt mehrere unterschiedliche Alternativlösungen zur Verfügung (s. auch die nachfolgende Abbildung). Bei höheren Anforderungen an die Kompatibilität kommen mehrere Lösungen für unterschiedliche Anforderungen in Frage:

- Scalix
- Samsung Contact
- Kolab
- Exchange4Linux
- OpenGroupware

[1] http://support.microsoft.com/default.aspx?scid=fh;en-us;lifesrvr

Der Einsatz der Lösungen ermöglicht, durch die Anbindbarkeit des Outlook-Client, diesen in seinen wesentlichen Funktionen weiter zu verwenden. Tiefergehende technische Betrachtungen und ein Vergleich der Funktionalitäten sind im Kapitel „Technische Betrachtungen“ zu finden.

Bild 102: Unterschiedliche Varianten einer Exchange-Ablösung bei Teilmigration

Samsung Contact und Scalix sind genau wie Exchange keine OSS sondern entfallen als proprietäre Software in die Kategorie COLS. Eine Migration nach Samsung Contact wurde bereits in den Empfehlungen zu einer vollständigen „Ablösenden Migration“ betrachtet siehe (Kapitel 6.2.2.2). Samsung Contact und Scalix eignen sich insbesondere für große und spezialisierte Behörden mit besonderen Anforderungen an die Skalierbarkeit und Ausfallsicherheit. Eine weitere Alternative stellt die OpenGroupware-Lösung (siehe 0) dar, die als OSS-Software verfügbar ist. Zur Anbindung der Outlook-Clients muss ein proprietärer und kommerzieller Connector beschafft werden.

Für kleinere bis mittlere Organisationen bietet Kolab 1 bzw. 2 eine adäquate Groupware-Basis bieten. Der Vorteil der Groupwarelösung liegt in dem modularen Aufbau des gesamten Systems, bei dessen Entwicklung auf bewährte und skalierbare Komponenten zurückgegriffen wurde. Durch die Unterstützung des Outlook-Clients bietet sich auch der Einsatz im Rahmen einer Teilmigration an.

Für Behörden mit bis zu 500 Anwendern kann ebenfalls die preislich günstige Lösung Exchange4Linux empfohlen werden. Hierbei handelt es sich im Wesentlichen um eine OSS-Lösung. Die Serverkomponente ist als Freie Software verfügbar, lediglich der MAPI-Connector ist proprietär und ausschließlich kostenpflichtig erhältlich. Näheres auch hierzu im Kapitel 3.12.4.4.

Für alle Lösungen wird serverseitig Linux als Betriebssystem benötigt. Die Durchführung einer punktuellen Migration bietet eine Reihe von Vorteilen:

- Übersichtlicher und gut planbarer Migrationsumfang.
  Notwendige Anpassungen halten sich in einem begrenzten Rahmen, was für Projektplanung und –steuerung einen essentiellen Vorteil bietet.
- Die Möglichkeit, stufenweise Betriebskonzepte und -erfahrungen mit einer neuen Betriebssystemplattform aufzubauen.
- Schulungsaufwand fällt nur für die jeweils fachlich involvierten Administratoren an. Die neu geschulten Administratoren können so auch als Multiplikatoren innerhalb der IT-Abteilung dienen.

Im Zusammenhang mit Groupware und Messaging muss an dieser Stelle auch erwähnt werden, dass in Fällen, wo keine Groupware-Funktionalitäten benötigt wird, die ausschließliche Migration der Mail-Funktionalität erheblich leichter zu bewerkstelligen ist. Tatsächlich ist dies eine bereits häufig erprobte und insofern bevorzugte Lösung.

Eine weitere Möglichkeit für die punktuelle Migration besteht in der Ablösung von MS Office durch OpenOffice.org oder StarOffice. Dabei sind die bereits genannten funktionalen Einschränkungen und insbesondere auch wirtschaftliche Konsequenzen, zu berücksichtigen. Eine Office-Migration wurde bereits im Kapitel zur vollständigen „Ablösenden Migration“ betrachtet (6.2).

6.4.2 Serverseitige Teilmigration

Im Folgenden soll am Beispiel einer flächendeckenden Servermigration ein sinnvolles und empfehlenswertes Szenario für eine serverseitige Teilmigration vorgestellt werden. Als Ausgangssituation für eine serverseitige Migration ist die in Kapitel 2.2.1 beschriebene Windows-NT-Umgebung angenommen.

Prinzipiell treffen die Empfehlungen aus der vollständigen Migration (siehe auch 6.2), auch auf die breite serverseitige Migration zu. Die Unterschiede begründen sich aus der Tatsache, dass die Client-Seite weiterhin aus windowsbasierten Systemen besteht.

Die Empfehlungen für:

- Datenbanksystem,
- Webserver,
- und Netzwerkdienste

können ebenfalls dem Abschnitt 6.2 entnommen werden.

Die zentrale Anforderung für eine serverseitige Migration besteht in der reibungslosen Zusammenarbeit zwischen den linuxbasierten Serversystemen und den windowsbasierten Client-Systemen nach der Migration. Die wichtigste Anforderung für die Durchführung der Migration selbst dürfte in der Ablösung der Dateiablage-, Druck-, Netzwerk- und Authentifizierungsdienste inkl. der Migration der

vorhandenen Datei- und Rechtestrukturen und der Übernahme der Konfigurationsdaten liegen.

6.4.2.1 Benutzerverwaltung und Authentifizierung

Für die Ablösung eines Windows NT 4.0 Domänen Controllers wird ein linuxbasierter Samba-Server in Kombination mit OpenLDAP empfohlen. Samba kann unter Linux einen weitgehend vollständigen Windows Domänen Controller abbilden. Insbesondere die Version 3.0 von Samba, die bereits erfolgreich in unterschiedlichsten Migrationsprojekten eingesetzt wurde, bietet nahezu uneingeschränkt die Möglichkeit der Anbindung von Windows 2000- und Windows XP-Clients. Näheres hierzu ist in den technischen Betrachtungen von Kapitel 3 zu finden.

6.4.2.2 Datei- und Druckdienste

Wie bereits dargelegt, kommt für Dateidienste nur Samba zur reibungslosen Einbindung der Windows-Clients in Frage. Samba ist in der Lage, die wesentlichen Funktionalitäten eines Windows NT-basierten Dateiservers unter Linux abzubilden. Die Benutzer von Windows-Clients können ihre Benutzerprofile und Logon-Scripts ebenso von einem Samba-Server beziehen, wie ihre Heimat- oder Gruppenverzeichnisse. Für physikalische Speicherung der Daten auf den Plattensystemen der eigentlichen Serversysteme werden die Dateisysteme XFS und EXT3 empfohlen. Beide Dateisysteme unterstützen POSIX-ACL, Journaling-Funktionalitäten und Quotas.

Die Druckdienste sollten mittels CUPS in Kombination mit Samba erfolgen. CUPS ist optimal in Samba integriert

6.5 Migrationswege

6.5.1 Schnelle Migration

In diesem Abschnitt werden die Gründe für eine schnelle Migration dargelegt und Ausgangssituationen analysiert, für die eine schnelle Migration zu empfehlen ist.

Die schnelle Migration steht im Gegensatz zur sanften Migration. Beide Migrationswege beziehen sich auf das Ziel einer vollständigen „Ablösenden Migration“, das heißt, bei beiden Wegen besteht das Ziel einer rein linuxbasierten Systemumgebung

Eine schnelle Migration ist nicht, wie der Name vermuten lässt, durch ihre Schnelligkeit geprägt sondern dadurch, dass die Migration in einem Schritt innerhalb eines überschaubaren und vor allem festgelegten Zeitraumes durchgeführt wird. Eine schnelle Migration hat einen definierten Beginn (Anfangsdatum) und ein definiertes Ende (Enddatum). Und am Ende steht der Beginn des vollständigen Wirkbetriebes einer rein linuxbasierten IT-Landschaft.

Die Durchführung einer schnellen Migration stellt hohe bis sogar sehr hohe Anforderungen an:

- die Organisation des Projektes
- die Organisation der betroffenen Behörde
- die Technik
- die Finanzen
- die Administratoren
- die Benutzer.

Insbesondere die Anforderungen an die Administratoren und die Benutzer dürfen dabei nicht unterschätzt werden. Dies gilt umso mehr, je weniger Know-how bezüglich der neuen IT-Landschaft bei den Administratoren und den Benutzern verfügbar ist. Andererseits besteht der Vorteil einer schnellen Migration darin, dass die Administratoren sich nicht über einen längeren Zeitraum mit zwei unterschiedlichen IT-Ausrichtungen auseinandersetzen müssen. Sie können sich innerhalb relativ kurzer Zeit (den Anforderungen des Projektes angemessen) nur auf die neuen Systeme konzentrieren.

Wichtig ist ferner, dass die benötigten Finanzen innerhalb eines relativ kurzen Zeitraumes verfügbar sein müssen. Letztendlich gibt der Umfang und vor allem die Komplexität und die Vielfalt der zu migrierenden Anwendungen und Systeme den Ausschlag dafür, wann und wie viel Finanzmittel bereitzustellen sind. Dieser Aspekt wird mit über die Machbarkeit einer schnellen Migration entscheiden.

Die hohen Anforderungen an die Organisation der Behörde konzentrieren sich zum einen auf die Qualifizierung der Mitarbeiter, die weiterhin ihren täglichen Pflichten nachgehen müssen. Das heißt, dass Störungen des Betriebes der Behörde unbedingt minimiert werden müssen. Zum anderen muss der laufende IT-Betrieb aufrecht erhalten bleiben. Insbesondere eine Umstellung der gesamten Serverlandschaft stellt hier hohe Ansprüche an alle Beteiligten, da sich die Migration der einzelnen Serverdienst nicht beliebig partitionieren lässt, die Administratoren den laufenden Betrieb garantieren und zugleich auf die neuen Systeme eingewiesen werden müssen.

Diese Anforderungen können durch geeignete Umstellungs- und Rollout-Konzepte gelöst werden. Auch der Aufbau einer parallelen IT-Landschaft hierfür ist möglich, wodurch jedoch erhöhte Anforderungen an die Technik und letztlich zusätzliche Kosten entstehen.

Aufgrund dieser hohen Anforderungen stellt sich natürlich die Frage, ob eine schnelle Migration überhaupt sinnvoll ist, bzw. für wen ist sie sinnvoll und zu empfehlen?

Gründe für eine schnelle Migration sind:

- Es besteht der Zwang zu einer Migration, das heißt, dass zum Beispiel der Support für die alten Systeme ausläuft.
- Die Administratoren und Benutzer werden zwar intensiv, dafür aber nur einmal mit Neuerungen konfrontiert und nicht jährlich fortlaufend.

- Die Administratoren müssen sich nicht über längere Zeiträume mit der Komplexität heterogener Welten auseinandersetzen.

Unter welchen Voraussetzungen und für wen ist eine schnelle Migration sinnvoll?

Liegt eine überschaubare und nicht übermäßig „verwobene“ Systemlandschaft vor, ist dies zunächst eine gute Voraussetzung für eine schnelle Migration. Das heißt, dass nur wenige Anwendungen und Dienste für die Aufgabenerfüllung eingesetzt werden. Dabei muss es sich nicht einmal nur um kleine und einfach strukturierte Verwaltungen und Organisationen handeln. Dies trifft zum Beispiel auch auf Behörden und Organisationen mit Sicherheitsaufgaben zu, bei denen der größte Teil der Benutzer mit wenigen großen Fachanwendungen ausgestattet ist, die meist serverbasiert sind, und mit denen der überwiegende Teil der Aufgaben erledigt wird. Dies trifft aber auch für kleine bis mittlere Behörden mit wenigen Fachanwendungen, Standardbürokommunikation und Office-Einsatz mit wenig komplexen Dokumenten und Vorlagen (wie z.B. die Monopolkommission).zu.

Eine weitere gute Voraussetzung ist in denjenigen Behörden gegeben, die bereits über das notwendige Know-how bei den Administratoren verfügen. Sei es, dass diese sich in ihrer Freizeit mit linuxbasierten Systemen auseinandersetzen oder bereits schon einzelne linuxbasierte Anwendungen und Dienste (z.B. Mail Server auf Linux) vorhanden sind. Ist außerdem bei den Mitarbeitern auch noch die nötige Offenheit für Neuerungen und Interesse an Linux vorhanden, sind dies ebenfalls ideale Voraussetzungen für eine schnelle Migration.

6.5.2 Sanfte Migration

In diesem Abschnitt werden nun die Gründe für und die Wege zu einer sanften Migration beschrieben. Doch was bedeutet eigentlich sanfte Migration? Mit sanfter Migration wird ein Migrationsweg beschrieben, bei dem das Ziel feststeht, jedoch ein nur grob definierter Zeitrahmen vorgegeben wird und die Migration komponentenweise in Anlehnung an das obige Architekturmodell vorgesehen ist.

Die Gründe für die Wahl eines sanften Migrationsweges werden deutlich bei einem Rückblick auf die Anforderungen und die Gründe für eine schnelle Migration:

- In Behörden und Verwaltungen mit knappen Budgets können die notwendigen Kosten der Haushaltslage angepasst verteilen.
- Fehlendes Know-how kann sukzessive aufgebaut und damit können Kosten eingespart werden. Bei der sanften Migration können einzelne Komponenten herausgenommen werden. Die dabei geschulten Administratoren dienen anschließend als Multiplikatoren, so dass bei der Migration der nächsten Komponente schon ein höherer Grad an Know-how verfügbar ist.
- Bestehende Widerstände können langsam abgebaut und Vorbehalte aufgelöst werden.
- Komplexe IT-Strukturen können Stück für Stück aufgelöst werden.

Migrationsempfehlungen

Die nachfolgende Abbildung skizziert, wie eine mögliche sanfte Migration aussehen könnte.

Bild 103: Sanfte Migration

Zu Beginn sollte eine einfach herauszulösende Komponente für die Migration gewählt werden. In dem obigen Beispiel steht dort zunächst der DBMS Server. Dabei geht es nicht um die Migration der Datenbankanwendungen, sondern um das Aufsetzen eines parallelen DBMS. Grundkenntnisse zu DBMS dürften vorhanden sein und spätestens bei der ersten Migration, nämlich der des Web Servers, wird in der Regel ein DBMS benötigt. Der Directory Server ist zunächst eine alleinstehende Komponente, kann aber evtl. schon im Zusammenhang mit dem Webserver genutzt werden und ist möglicherweise eine Voraussetzung für die folgende Groupware-Migration. Anschließend erfolgt die Migration der Datei-, Netz- und Druckdienste. Letztendlich wird der Desktop migriert, nachdem parallel zu den Komponentenmigrationen alle Fach- und Officeanwendungen im Hintergrund migriert wurden.

Bei einer sanften Migration können die Komponenten für die einzelnen Schritte nicht beliebig ausgetauscht und verschoben werden; was zusammen gehört, soll auch zusammen bleiben. Ferner ist wichtig, dass der Prozess zeitlich nicht überstrapaziert und ein realistischer Endtermin gesetzt wird. Der Realisierungszeitraum muss jedoch der Komplexität von Pflege und Wartung und damit dem Aufwand, der für die Administratoren anfällt, Rechnung tragen. Da der administrative Aufwand in einer bunten IT-Landschaft höher als in einer homogenen Landschaft anzusetzen ist, sollte der gesamte Umstellungsprozess auch bei einer sanften Migration 2 bis 3 Umstellungsphasen mit einem insgesamt zeitlich überschaubaren Horizont nicht überschreiten.

Bild 104: Phasen der Umstellung bei einer sanften Migration

Bild 104 zeigt die drei Phasen der Migration. Die serverseitige Migration kann dabei vor allem mit Hilfe von Samba, Terminalservices und auch der Möglichkeit Outlook als Groupware- und Messaging-Client weiterzuverwenden in einer heterogenen Umgebung relativ weit vorangetrieben werden.

Erst ganz am Ende, wenn alle Fach- und Officeanwendungen parallel zu diesem Prozess umgestellt wurden, kann die Migration des Desktops, heißt die clientseitige Migration nach Linux vorgenommen werden. Sofern die Umstellung der Fach- und Officeanwendungen dies zulassen, kann sogar überlegt werden in einem Zwischenschritt MS Office nach OpenOffice.org oder StarOffice auf einem Windows-Client zu migrieren.

6.5.3 Kritische Erfolgsfaktoren

Migrationsprojekte sind in der Regel komplexe und vielschichtige Vorhaben. Dies betrifft sowohl komplette Migrationen (Clients und Server) als auch teilweise (Server) oder nur punktuelle Migrationsvorhaben. Die nachfolgende Abbildung verdeutlicht den mehrere Phasen umfassenden Migrationsprozess mit seinen einzelnen Teilaspekten.

Damit Migrationsprojekte als IT-Projekte im Allgemeinen und als Innovationsprojekte im Besonderen zu einem erfolgreichen Abschluss geführt werden können, sind die kritischen Erfolgsfaktoren bereits im Vorfeld zu definieren und zu bewerten. Erfolgreich für alle Beteiligten ist ein Migrationsprojekt zunächst dann, wenn das gewünschte Ziel bzw. Ergebnis innerhalb des geplanten bzw. vereinbarten Zeit- und Budgetrahmens erbracht wird.

Hinzu kommen so genannte weiche Faktoren, die einen nicht zu unterschätzenden Beitrag zum Gesamterfolg leisten. Dazu zählen beispielsweise die Mitarbeiterzufriedenheit, eine reibungsfreie Kommunikation und damit Vermeidung bzw. Reduzierung von Misserfolg, Frust und Doppelarbeiten sowie die bedarfsgerechte Auswahl und natürlich Akzeptanz der neuen IT-Landschaft bei den Benutzern.

Bild 105: Modell: stufenförmiger Migrationsprozess

Unabhängig von der Behördengröße und unabhängig davon, ob es sich bei einem Migrationsvorhaben um eine ablösende oder auch um eine fortführende Migration handelt, tragen aus Sicht der Autoren die nachfolgend zusammengefassten Parameter zu einem nachhaltigen Projekterfolg bei.

- Formulierung eindeutiger Ziele des Migrationsprojektes
- Einbindung und Positionierung der Leitungs- und Entscheidungsebene
- frühe Informationen und Einbindung der Zielgruppen/Mitarbeiter
- Schaffung einer hohen Nutzerakzeptanz hinsichtlich der Ziel-Umgebung
- Strukturierte Zeit-, Projekt- und Ressourcenplanung mit Projekt-Controlling
- Organisatorische Maßnahmen zur Vorbereitung der Migration und Bildung eines qualifizierten Projektteams
- Detaillierte Bestandsaufnahme mit Definition der funktionalen Anforderungen

- optimale Produkt- und Dienstleistungsauswahl
- zeitnahe und nachhaltige Schulungen
- Qualitätsmanagement und Dokumentation

Aus den Erfolgsfaktoren leitet sich ab, dass Migrationsprojekte nicht mit dem Kauf und der Implementierung der entsprechenden Komponenten abgeschlossen sind. Sowohl im Vorfeld und während des eigentlichen Migrationsprozesses als auch in der Nachbereitung sind weitergehende Abhängigkeiten und Aktivitäten zu berücksichtigen.

Dabei sind Migrationsprojekte insgesamt nur dann als erfolgreich und wirtschaftlich einzustufen, wenn sie neben einer Minimierung der laufenden Kosten zumindest auch eine Verbesserung der Aufgabenwahrnehmung durch eine moderne, integrative und funktional zielgerichtete IuK-Unterstützung ermöglichen und zu einer allgemeinen Erhöhung von Flexibilität, Leistungsfähigkeit und Reaktionsbereitschaft bei vorhandenen und zukünftigen Aufgabenstellungen führen. Weitere Ziele wie das Erreichen einer Hersteller- und / oder Plattformunabhängigkeit sind zentrale Aspekte, die langfristig gesehen den Anforderungen einer Wirtschaftlichkeitsbetrachtung standhalten müssen.

In den nachfolgenden Abschnitten werden die wesentlichen der für Migrationsprojekte identifizierten Erfolgskriterien näher beschrieben.

6.5.3.1 Formulierung eindeutiger Ziele

Grundlage jedes Projekterfolges ist die Formulierung eindeutiger Ziele. Dabei ist zwischen strategischen Managementzielen (Motivationsebene) und Zielen auf der Ebene der Servermigration (Erscheinungsebene) zu unterschieden. Festzulegen ist, warum eine Migration überhaupt durchgeführt werden soll und in einem nächsten Schritt, was damit erreicht werden soll.

Den Betroffenen, der Behördenleitung und den einzubindenden Partnern ist vor Projektbeginn offen zu legen, worin das eigentliche Ziel des Migrationsvorhabens liegt. Diese Zielformulierung bildet die Basis für alles weitere Agieren, für die Projektgestaltung und die Auswahl der Zielsoftware genauso wie für die Auswahl der einzubindenden internen und externen Partner. Dabei ist das Erreichen einer gewissen Hersteller- bzw. Plattformunabhängigkeit ein eher allgemeines bzw. übergeordnetes Ziel.

Behördenspezifisch könnten zum Beispiel folgende detaillierte Zielvorgaben auf der Ebene der Servermigration bestehen:

- Servermigration ohne Anpassungen und Umstellungen an den Clients (vollständige Übernahme der Daten, Nutzerprofile, Datei- und Verzeichnisstrukturen mit bestehenden Zugriffsrechten)
- Vollständige Umstellung der Clients (gleichwertiger Ersatz von Anwendungen und Funktionen und Integration in das vorhandene Behörden-Rechnernetz ohne Beeinträchtigung desselben)

- Migration der Daten und Datenstrukturen unter Beibehalt der Datenbankanwendungen (entsprechende Auswahl freier Datenbanksysteme)
- Austausch vorhandener Applikationen auf Arbeitsplatzsystemen durch gleichwertige Anwendungen (Einrichtung einer einfach zu bedienenden zentralen Systemverwaltung; Berücksichtigung der IT-Sicherheitskomponenten gemäß Bund Online 2005, z.B. PKI, Authentifizierung über Zertifikat und biometrische Kennzeichen)
- Schaffung eines adäquaten Ersatzes für Benutzerverwaltung und Authentifizierung
- Reibungsfreie Konvertierung von Formatvorlagen

6.5.3.2 Einbindung und Positionierung der Leitungs- und Entscheidungsebene

Die Leitungs- und Entscheidungsebene ist jene Ebene, die die Schlüsselentscheidungen für das Migrationsprojekt trifft, ohne direkt in der Projektarbeit aktiv zu sein. Ihr gegenüber besteht eine Berichtspflicht der Projektleitung. Welche Ebene genau darunter zu verstehen ist, hängt von der spezifischen Behördensituation und der Priorisierung des Projektes innerhalb der Behörde ab.

Die Rolle der Leitungsebene für den Projekterfolg wird häufig unterschätzt. Erfahrungsgemäß herrscht stattdessen die Annahme vor, dass die Leitungsebene „von Informations- und Kommunikationstechnik wenig oder nichts versteht“. Gleichzeitig wird dann unterstellt, dass die Behördenleitung „nur“ ein primäres Interesse daran hat, „ein funktionierendes und bezahlbares System“ zu erhalten. Eine solche Annahme ist jedoch kontraproduktiv. Stattdessen ist eher die Leitungs- und Entscheidungsebene für die behördenspezifische Zielvorgabe des Migrationsprojektes als für die Etablierung und Umsetzung des Vorhabens verantwortlich. Sich daraus ggf. ergebende Vertragsänderungen bzw. -neugestaltungen fallen in der Regel ebenfalls in den Verantwortungsbereich der Behördenleitung.

Zunächst muss das Migrationsprojekt überhaupt in Gang gesetzt werden. Dazu ist es notwendig, dass die Entscheidungsebene anhand von erkannten Defiziten bzw. konkreten Projektzielen (z.B. Hersteller- und Plattformunabhängigkeit erreichen) einen Projektauftrag formuliert oder anhand von Anforderungen der nachgeordneten Mitarbeiter den Bedarf erkennt, einen Projektauftrag zu definieren.

Kommunikation des Projektes als Leitungsentscheidung

Die Leitungsebene trägt wesentlich zum Projekterfolg bei, in dem sie allen am Projekt Beteiligten sowie den Mitarbeitern insgesamt vermittelt, dass sie hinter diesem von ihr gewollten Projekt steht und es von ihr in allen Phasen seine Entwicklung nicht nur zur Kenntnis genommen, sondern auch unterstützt wird.

Frühzeitige und aktive Information der Beschäftigten

Eine weitere eindeutige und zentrale Führungsaufgabe, die bereits im Vorfeld eines Migrationsprojektes beginnt und wahrgenommen werden muss, ist die Verantwortung für Mitarbeiterkommunikation und -motivierung. Führen geschieht

über Kommunizieren und so sind Führungsstil und Kommunikationsstil untrennbar miteinander verbunden und erfordern eine besonders hohe soziale Kompetenz. Es gilt somit, allen Beschäftigten und Beteiligten die geplanten Vorhaben transparent zu machen. Dabei sind sowohl jene Bereiche zu benennen, die geändert werden, als auch jene, die beibehalten werden. (Zum Beispiel können auf der Basis des bestehenden Betriebskonzeptes zu erwartende Änderungen und die unveränderlichen Elemente genau beschrieben werden.)

Darüber hinaus sollten zur Information verschiedene Kommunikationskanäle etwa im Rahmen von allgemeinen Informationsveranstaltungen, Mitarbeitergesprächen, Workshops oder Rundschreiben bzw. Ankündigungen als auch das Behörden-Intranet genutzt werden (Vermeidung von Gerüchten). Möglichkeiten, um auf Fragen und Überlegungen, aber auch Sorgen und Ängste der Beschäftigten vor Veränderungen zu reagieren, sind frühzeitig einzuräumen Die Personal- und Gremienvertretungen sind ebenfalls frühzeitig in den Gesamtprozess einzubeziehen.

Prüfung rechtlicher Fragen

Zu den Aufgaben der Leitungsebene gehört des Weiteren die Prüfung der rechtlichen Fragen einer Migration. Hierbei sind unterschiedliche Prüfungsschritte in den verschiedenen Phasen der Migration vorzunehmen. Zunächst muss die Führungsebene eine grundsätzliche Bewertung der rechtlichen Chancen und Risiken vornehmen, die eine Nutzung von OSS im Vergleich zu proprietären Produkten mit sich bringt. Hierbei kann unter Umständen auch für einzelne Produkte zu prüfen sein, welche Befugnisse die Behörde als Nutzer nach der jeweils maßgeblichen OSS-Lizenz erwirbt. Sofern bei der Migration externe Dienstleister in Anspruch genommen werden, hat die Leitungsebene für einen gesetzeskonformen Ablauf des Vergabeverfahrens zu sorgen. Schließlich muss die Behördenleitung für eine interessengerechte Vertragsgestaltung mit den externen Dienstleistern sorgen. Die Leitungsebene sollte bei der Prüfung der rechtlichen Fragen gegebenenfalls auf behördeninterne Juristen (Rechtsämter, Rechtsabteilungen) oder externen Sachverstand (Rechtsanwälte) zurückgreifen.

Bereitstellung benötigter Finanzmittel

Die Leitungsebene muss sicherstellen, dass bereits zu Projektbeginn die erforderlichen Finanzmittel (für Sach- und Personalmittel) für die einzelnen Arbeitspakete und für die Beteiligten vorhanden sind. Dazu zählen neben den reinen Investitions- und Lizenzkosten zum Beispiel auch Kosten für Schulungen, ggf. externe Beratung und Projektunterstützung sowie interne Personalkosten. Darüber hinaus sind die benötigten Finanzmittel ggf. dem Projektfortschritt anzupassen.

Abnahme von Zwischen- und Endergebnissen

Zwischen der Leitungsebene, der Projektleitung und den Projektgruppenmitgliedern gibt es eine klare Aufgabenteilung. Die Entscheidungsebene muss mit den von der Projektgruppe vorbereiteten Unterlagen im Rahmen des Berichtswesens die Schlüsselentscheidungen am Ende der Projektphasen treffen und verantwor-

ten. Ggf. ist eine Modifikation der vorgegebenen strategischen Ziele durch veränderte Umstände notwendig.

6.5.3.3 Schaffung einer hohen Nutzerakzeptanz hinsichtlich der Ziel-Umgebung

Auf der Ebene der Mitarbeiter können Migrationsprojekte nur dann sinnvoll und erfolgreich sein, wenn ein klar erkennbarer Nutzen identifiziert und dieser auch als sinnvoll und notwendig kommuniziert wird. Dieser Nutzen leitet sich aus der Zieldefinition ab.

Letztlich sollten die betroffenen Beschäftigten weitestgehend von den Vorteilen des Migrationsvorhabens überzeugt sein, um das Projekt bereichs- bzw. behördenweit zu unterstützen und einzuführen. Gleichzeitig sind dabei die Grenzen von Open Source klar zu kommunizieren und es ist zu verdeutlichen, warum der Weg zu Open Source beschritten wird.

Ziel ist es, eine hohe Akzeptanz und damit in Konsequenz eine hohe Motivation und Zufriedenheit der Beschäftigten sicherzustellen. Es gilt zu verhindern, dass unzufriedene (nicht informierte, nicht motivierte oder mangels Schulung nicht qualifizierte) Beschäftigte den Gesamterfolg des Migrationsprojektes gefährden und ggf. Misserfolge kommunizieren. Langfristig gesehen kann dadurch die Effizienz und Leistungsfähigkeit der Behörde insgesamt beeinträchtigt werden. Über die „Pflicht“ zur fortlaufenden Information über den Projektverlauf hinaus sollten die Verantwortlichen auch die „Kür“ der kontinuierlichen Erfolgskontrollen hinsichtlich der Mitarbeiterzufriedenheit absolvieren, um ggf. Korrekturen vornehmen zu können.

Die Konzipierung und nachhaltige Umsetzung der Maßnahmen ist zwar zuerst eine Führungsaufgabe, kann aber letztlich nur gemeinsam mit den Mitarbeitern entwickelt, praktiziert und natürlich ständig verbessert werden. Gegebenenfalls kann hier in der Anfangszeit externe Unterstützung, Beratung und Coaching sinnvoll sein.

6.5.3.4 Schulungen für Benutzer und Administratoren

Im Bereich Schulungen sind zum einen die Administratoren frühzeitig und die künftigen Benutzer zeitnah zu integrieren. Ein zielgruppenspezifisches Schulungskonzept, das sowohl die Vorkenntnisse, Erfahrungen und Qualifikationen als auch die künftige arbeitsplatzspezifische Nutzung der Komponenten berücksichtigt, ist zu entwickeln. Dies beinhaltet auch die Einweisung der Benutzer am Arbeitsplatz sowie die fortlaufende Schulung besonders der Administratoren und Benutzerbetreuer im Bereich Open Source Software. Ferner empfiehlt es sich, die Erfahrungen aus Pilot- oder anderen Migrationsprojekten aktiv in die Schulungskonzeptionen einzubinden im Sinne von Lessons Learned Weitere konkrete Maßnahmen sind die Einrichtung von Test- und Simulationsumgebungen, Notfallübungen, Backup und Recovery.

Dies gilt umso mehr, wenn keine oder nur geringe Vorkenntnisse bzw. Erfahrungen vorhanden sind und im Anschluss an die Migration kein laufender bzw. bedarfsbezogner externer Support mehr zur Verfügung steht.

6.5.3.5 Organisatorische Maßnahmen zur Vorbereitung der Migration

Einrichtung einer Projektgruppe

Migrationsprojekte werden in der Regel nicht von einer Einzelperson, sondern von mehreren Beteiligten bzw. Akteuren durchgeführt. Sie sollten im Interesse eines erfolgreichen Abschlusses auch zeitlich begrenzt sein und einer klaren Zielstellung folgen. Damit sind die Merkmale klassischer Projektarbeit erfüllt, für die die Einrichtung einer projektorientierten Organisationsform zu empfehlen ist.[1]

Darauf aufbauend gilt es zu prüfen, ob und inwiefern die bisherige Organisationsstruktur, die erfahrungsgemäß vorgangsorientiert ausgerichtet ist, sich als geeignete, d.h. projektadäquate Organisationsform erweist. Gegebenfalls sind die organisatorischen Rahmenbedingungen temporär zu ändern und die Beteiligten – neben der behördlichen Organisationsstruktur – als Mitglieder der Projektgruppe organisatorisch neu zu fassen. Wobei die Arbeitsabläufe, Schnittstellen, Produkte und Ressourcen im Vorfeld unter Einbeziehung der Beteiligten zu erarbeiten und festzulegen sind. Dabei gilt:

- Projektorganisation vor Aufbauorganisation
- Klare Abgrenzung von Aufgaben, Zuständigkeiten und Verantwortlichkeiten
- Temporäre Reduzierung oder Übertragung von Routinetätigkeiten
- Festlegung der Kommunikations- und Berichtswege

Alle Planungen und Maßnahmen sind dahingehend kritisch zu bewerten, inwieweit sie die Erreichung des Projektzieles aus organisatorischer Sicht unterstützen. Im Zweifelsfall sind diejenigen Maßnahmen zu priorisieren, die ein höheres Unterstützungspotenzial beinhalten.

Zusammensetzung der Projektgruppe

Der Erfolg eines Projektes steht und fällt mit der Projektleitung und der Zusammensetzung der Projektgruppe. Eine falsche Auswahl kann auch bei ansonsten günstigen Voraussetzungen zu einem ungenügenden Projektergebnis führen, während eine gute personelle Besetzung auch bei dürftigen Rahmenbedingungen noch akzeptable Ergebnisse erarbeiten kann. Dies steht im Gegensatz zu der vereinzelnd auftretenden Meinung, dass „jeder ersetzbar“ sein solle.

Die Projektleitung: Der Projektleiter trägt die Gesamtverantwortung für ein Projekt. Er koordiniert, organisiert und kommuniziert die Gesamtprojektarbeit, damit das Projekt sachgerecht, termingerecht und kostengerecht realisiert wird. Er ist

[1] Vgl. Bundesministerium des Innern, Handbuch für Organisationsuntersuchungen in der Bundesverwaltung, Bonn, 5 Aufl. 1988, S. 23ff.

verantwortlich für die Vorgabe und die Überprüfung der Einhaltung von inhaltlichen Zielen und Meilensteinen (ggf. auch die Berichterstattung zum Lenkungsausschuss).

Abhängig von der Behördengröße und dem Charakter des Migrationsvorhaben kann es sinnvoll sein, neben dem Projektleiter noch weitere Teilprojektleiter zu benennen.

Die Projektgruppe: Die Erarbeitung der Projektinhalte bzw. Umsetzung der einzelnen Phasen und Stufen des Migrationsprozesses wird von den Mitgliedern der Projektgruppe realisiert. Dazu zählt in erster Linie die Gruppe der Administratoren. Hinzukommen können ausgewählte Benutzer und ggf. externe Dritte (Erfahrungs-/Betriebs-Know-how-Träger, Berater).

Die Einbindung externer Berater

Auch im Behördenumfeld wird zunehmend die Unterstützung externer Beratung im Projektumfeld genutzt. Zu den Gründen [1] für ihren Einsatz gehören:

- Professionelle, neutrale und objektive Problemanalyse
- Zeiteffizientes, planvolles Projektmanagement
- Laufende Kommunikation über das Projekt mit wirksamen Fortschritts- und Ergebniskontrollen
- Überzeugende, gut aufbereitete (Sitzungs-)Moderation, Präsentation und Ergebnisdokumentation
- Know-how Transfer bezogen auf die Vorbereitung und Durchführung von komplexen IT- bzw. Migrationsprojekten.

Festlegung der projektspezifischen Organisationsform

In Abhängigkeit von Migrationsumfang und Behördengröße ist die geeignete Projektorganisationsform für das Migrationsprojekt einzurichten. Dabei ist die Projektorganisation eine Parallelorganisation, die nicht in die bestehende Organisationsstruktur eingreift und auf die Projektdauer beschränkt ist. Aufgaben- und zielabhängig ist die Etablierung einer der drei nachfolgend aufgeführten Organisationsmöglichkeiten zu empfehlen:

Linien-Projektorganisation: Die Projektmitarbeiter werden aus der bestehenden Organisation herausgenommen und bilden eine eigene, von einem Projektleiter geführte Organisationseinheit. Dies führt zu einer höheren Identifikation mit dem Projekt und die Mitarbeiter können sich voll darauf konzentrieren. Gleichzeitig fehlen diese Mitarbeiter in ihrer Abteilung, was zu unterschiedlicher Auslastung (Überlastung) des Personals führen kann. Die Form der Linien-Organisation sollte bei umfangreichen und schwierigen Projekten verwendet werden.

[1] Bundesministerium des Innern, Handbuch für Organisationsuntersuchungen in der Bundesverwaltung, Bonn, 5 Aufl. 1988, S. 37 ff

Stabs-Projektorganisation: Das Projekt wird durch einen Projektkoordinator, der als Stabsstelle keine formalen Entscheidungsbefugnisse und somit begrenzte Kompetenzen hat, geleitet. Die Projektmitarbeiter bleiben in ihrer Abteilung und treffen sich nur zu Projektteamsitzungen, was die Stabs-Projektorganisation anfällig für Störungen und Ineffektivität macht.

Die Vorteile liegen hierbei bei dem geringen Organisationsaufwand (nur ein Koordinator muss neu gefunden werden) und der flexiblen Mitarbeiterauslastung (Einsatz im Projekt und Abteilung). Außerdem können mehrere Projekte gleichzeitig laufen. Generell eignet sich diese Organisationsform nur für kleinere Projekte, da sonst der Koordinations- und Abstimmungsaufwand zu hoch wird.

Matrix-Projektorganisation: Bei der Matrix-Projektorganisation wird neben der bestehenden hierarchischen Struktur eine horizontale Anordnungsbefugnis eingeführt. Die Mitarbeiter unterstehen in inhaltlichen Projektbelangen dem Projektleiter, personell und disziplinarisch jedoch weiterhin dem Linienvorgesetzten. Projekte dieser Art sind komplex und erfordern einen hohen Koordinationsaufwand.

Die Vorteile liegen darin, dass erforderliche Ressourcen nur bei Bedarf beansprucht werden. Der Projektleiter ist im Gegensatz zur Stabs-Projektorganisation mit Entscheidungskompetenzen und Weisungsbefugnissen ausgestattet.

Nachteile ergeben sich daraus, dass der Projektmitarbeiter „Diener zweier Herren“ ist. Insbesondere bei mehreren Projekten können Konflikte um Ressourcen oder durch widersprüchliche Vorgaben auftreten.

Zusammenstellung und Bewertung Projekt-Organisationsform für Migrationsprozesse

Zur Orientierung für die Auswahl der geeigneten Projekt-Organisationsform kann nachfolgende Tabelle dienen. Eine behördenspezifische Anpassung ist dennoch notwendig.

Tab. 63: Vorschlag Zusammenstellung Projekt-Organisationsformen

	Vollständige Migration	Teilweise Migration	Punktuelle Migration
Kleine Behörde	Linien-Organisation	Stabs-Organisation	Stabs-Organisation
Mittlere Behörde	Linien-Organisation	Matrix-Organisation	Matrix-Organisation
Große Behörde	Linien-Organisation	Linien/Matrix-Organisation	Matrix-Organisation

Kleine Behörde: bis 300 MA; mittlere Behörde: bis 1.000 MA; große Behörde: ab 1.000 MA

6.5.3.6 Einbindung ausgewählter Benutzerkreise

Im Rahmen der Projektvorbereitung ist – abhängig von der Komplexität des Migrationsvorhabens – auf organisatorischer Ebene zu entscheiden, welche Benutzergruppen in das Migrationsprojekt aktiv einzubeziehen bzw. lediglich zu informieren sind. Abhängig also davon, ob es sich um eine vollständige, eine teil-

weise oder eine punktuelle Migration handelt, sind die Benutzer aktiv von dem Änderungsprozess betroffen. Werden zum Beispiel im Rahmen einer teilweisen Migration die Server ausgetauscht, genügt in der Regel eine Information an die Benutzer, eine aktive Einbindung ist nicht erforderlich. Handelt es sich jedoch um eine Office-Migration, ist die aktive Einbindung und Betreuung der betroffenen Benutzer zwingend erforderlich.

6.5.3.7 Bestimmung der Ausgangssituation

Ein weiterer zentraler Erfolgsfaktor ist die genaue Bestimmung der Ausgangssituation. Dies ist in der Regel recht aufwändig, verlangt Personal-Ressourcen und entsprechend Zeit. Doch eine zu genaue Detailkenntnis von Dokumenten oder Datenbankanwendungen verhindert oder verzögert ggf. erforderliche Korrekturen während des Migrationsprozesses oder verzögert bereits im Vorfeld ein entsprechendes Vorgehen zu etablieren bzw. mit adäquaten Maßnahmen zu reagieren. Die Bestimmung der Ausgangssituation ist zudem die Grundlage, um die funktionalen Anforderungen an die Zielsysteme formulieren zu können. Wichtige Sachverhalte, die hierbei aufzunehmen sind u.a:

- Datenbanken und Datenstrukturen
- Dokumente und Dokumentenformate
- Anwendungen und ihre Schnittstellen
- Verfügbare Funktionalitäten
- Verfügbarkeit von Daten und Anwendungen
- Mängel und Probleme
- ...

6.5.3.8 Funktionale Anforderungen abdecken

Die Zielsoftware sollte (weitestgehend) die bestehenden Funktionalitäten und Anforderungen abdecken. Sie muss ggf. überprüfbaren Bewertungsmaßstäben standhalten. Eine Verschlechterung gegenüber der Ausgangssituation wäre kaum akzeptabel.

Zur Ermittlung der funktionalen Anforderungen dient zunächst die Beschreibung der Ausgangssituation. Darüber sind im Rahmen einer frühzeitigen Abfrage die konkreten Bedarfe und Anforderungen an die einzelnen Komponenten sowohl aus Benutzer- als auch aus Administratorensicht aufzunehmen, zu prüfen und in einer Anforderungs- oder Prioritätenliste zusammenzustellen. Dieses Vorgehen schließt auch die kritische Bewertung ein, ob vorhandene Funktionalitäten erforderlich und sinnvoll sind. Insbesondere die Kritikalität fehlender oder nicht vollständiger Funktionalitäten muss beurteilt und in die Auswahlkriterien aufgenommen werden. Fehlende Funktionalitäten in der Ziel-Umgebung können je nach Grad der Kritikalität zu einer Verschlechterung der Nutzerakzeptanz führen. Auf dieser Basis können Vergleiche mit den zur Auswahl stehenden Software-

Komponenten angestellt werden, um in einem nächsten Schritt dann die Zielsoftware bedarfsbezogen auswählen zu können.

Der Gesamtprojekterfolg wird sich an der Realisierung der Einzelanforderungen messen lassen müssen.

6.5.3.9 Nutzung von Erfahrungswerten

Die behördenübergreifende Nutzung von Erfahrungswerten im Kontext von Linux-Migrationen ist ebenfalls ein wesentlicher Erfolgsfaktor. Dies um so mehr, als es bislang (historisch gesehen) noch relativ wenige Erfahrungswerte in diesem Bereich gibt. Die Nutzung aktiver Erfahrungen aus Pilot- oder anderen Migrationsprojekten und die Einbindung in geplante Projekte und Vorhaben wird für Administratoren und Benutzer gleichermaßen gewinnbringend sein. Hierfür wäre beispielsweise die Einrichtung einer Projekt-Datenbank zu empfehlen.

6.5.3.10 Projekt- Zeit- und Ressourcenplanung

Für die Migration von durch Microsoft Software hin zu Open Source Software bestimmten Systemumgebungen gelten die Methoden klassischer Projektarbeit.

Der Projektplan: Beginn der Projektarbeit ist zunächst die Aufstellung eines Projektplanes, der den Weg zum Ziel beschreibt und für Dritte nachvollziehbar ist. Der Projektplan enthält mindestens Angaben zu Termin, Sach- und Personalressourcen, Einbindung externer Partner, Meilensteinen und Kosten. Er bildet gleichzeitig die Basis für eine funktionierende Projektsteuerung.

Im Rahmen des Projektplanes wird erarbeitet,

wer	Projektorganisation
Wann	Terminierung
Was	Projektgliederung
mit welchem Aufwand	Arbeitsaufträge
zu tun hat, um	Kalkulation
rasch und sicher	Projektstrategie
zum Projektziel zu gelangen	vorgeklärter Auftrag

Die erarbeiteten Ergebnisse werden im Projekthandbuch dokumentiert.

Der Zeitplan: Mittels einer Ablauf- und Zeitplanung erfolgt eine weitergehende Projektaufteilung. Solch ein verbindlicher Projektzeitplan dient dazu, eine realistische Terminierung der einzelnen Arbeitspakete vornehmen zu können. Der Projektzeitplan richtet sich nach den im Projektauftrag benannten Endtermin. Ebenso werden darin Beginn, Meilensteine und Abschluss der einzelnen Arbeitspakete festgelegt. Die Erstellung eines Projektzeitplanes bildet ferner die Basis für eine effektive Projektsteuerung und Projektkontrolle.

Der Aufwands- bzw. Ressourcenplan: Im Rahmen der Aufwandsschätzung werden Aussagen getroffen, welche Arbeitsmenge (Aufwand in Personentagen) sowie einzubeziehende Ressourcen voraussichtlich notwendig sein werden, um das vereinbarte Ergebnis zu erreichen. Dabei ist zwischen Aufwand (abhängig vom Arbeitsinhalt) und Dauer (abhängig von der Arbeitsintensität) zu unterscheiden.

In die Planung bzw. Schätzung der Einzelaufwände sollten jeweils die folgenden Kostenarten einfließen:

- Personalkosten (Personalressourcen multipliziert mit Verrechnungssatz)
- Einbindung der Community bei Migrationen hin zu Open Source Umgebungen
- Ressource für den Aufbau und den Betrieb von Testumgebungen
- Materialkosten (Verbrauchsmaterialien wie Druck- und Papierkosten)
- Gerätekosten (eventuell anzuschaffende Geräte oder SW)
- sonstige Kosten (Reisekosten, externe Dienstleistung).
- Anschaffungs- und Lizenzkosten
- Wartungs- Betreuungs- und Schulungskosten

6.5.3.11 Projektcontrolling und -steuerung

Das Projektcontrolling ist ein wichtiger Teilbereich der Projektorganisation. Die Aufgaben des Controllings beschränken sich nicht auf die reine Kosten- und Terminüberwachung. Gerade im Kontext von IT-Projekten ist Controlling keine Kontrolle im Sinn von rückschauender Revisionstätigkeit, sondern eine vorbeugende Steuerung, die rechtzeitig eingreift, wenn Abweichungen von den geplanten Ist-Werten erkennbar sind, damit die Projektziele bezüglich Qualität der Endprodukte, Fertigstellungstermin und Kosten der Projektarbeit eingehalten werden.

6.5.3.12 Dokumentation und Qualitätssicherung des Projektes

Bereits während des Verlaufes eines Projektes und vor allem nach seinem Abschluss müssen die einzelnen Arbeitsschritte jederzeit auch für Dritte nachvollziehbar sein, die nicht am Migrationsprozess beteiligt waren. Dies ist für eine spätere Pflege des Systems unbedingt notwendige Voraussetzung. Die Dokumentation kann mit Hilfe folgender Medien erfolgen:

- Konfigurationshandbücher
- Betriebshandbücher
- Schulungsunterlagen
- Bestandsverzeichnisse
- Projekthandbuch
- Protokolle/Statusberichte

- Qualitätssicherungs- bzw. Prüfbericht
- Abschlussdokumentation

Die Qualitätsprüfung muss sich neben der Kontrolle und Bewertung des Systementwurfes auch mit den Fragen der Analyse von möglichen Fehler und der Fehler-Folgenabschätzung beschäftigen, und zwar in jeder Projektphase. Diese Fehleranalysen müssen ebenso dokumentiert werden wie alle anderen Projektarbeiten.

Als Erfolgsfaktor im Rahmen der Qualitätssicherung hat sich z.B. in den Pilotprojekten der Aufbau von Testumgebungen erwiesen.

Bei großen Projekten bildet der Gesamtbereich der Qualitätssicherung ein eigenes Aufgabengebiet. Je nach Projektumfang und Qualifikation des Personals kann es vom Projektleiter oder u.U. von einem Projektcontroller mitbetreut werden.

Folgende Abbildung stellt die internen Schritte zur Qualitätskontrolle dar:

f

Bild 106: Stufen der Qualitätskontrolle

- Zum Ende eines Projektschrittes bzw. einer Projektphase werden durch den Qualitätssicherer die benötigten Checklisten und Prüfmethodiken vorbereitet.
- Wenn das Ergebnis der Qualitätskontrolle positiv ausfällt, wird die Freigabe für den nächsten Projektschritt erteilt. Entspricht ein Ergebnis nicht den definierten Qualitätsanforderungen, wird es zur Überarbeitung zurückgegeben. Die zu überarbeitenden Inhalte werden sodann konkret und detailliert benannt und in einem Prüfprotokoll schriftlich festgehalten. Schließlich wird ein Termin zur Wiedervorlage vereinbart, der im Projektplan eingetragen wird.

6.5.3.13 Betreuung während der Betriebsphase

Eine weitere Voraussetzung für den nachhaltigen Erfolg einer Migration ist eine Betreuung der Administratoren in einem angemessenem Umfang. Ein allgemein gültiger Richtwert zum Maß dieses Engagements kann an dieser Stelle allerdings nicht genannt werden. Wichtig ist jedoch, sofort zu reagieren, wenn ein entsprechender Bedarf besteht und erkannt wird. Aufgrund fehlender Routine im Migrationsumfeld ist auch für die Phase der Einarbeitung in die neuen Aufgabenfelder besonders den Administratoren eine Betreuung durch externe Vermittler von Know-how bzw. Support zur Verfügung zu stellen. Wichtig ist dies insbesondere

dann, wenn bei den Beteiligten bisher kaum oder keine Erfahrungen mit den neuen Systemen (Linux, OSS) bestehen. Die Anwesenheit eines Know-how Trägers vor Ort wäre in jedem Fall die vorteilhafteste Option.

7 Anhang

7.1 Anhang -WiBe

7.1.1 Überleitungstabellen Kriterien WiBe 4.0 zu Kostenartengruppen MiKoMa 2.0

Tab. 64: Überleitungstabelle Kriterien WiBe 4.0 zu Kostenartengruppen MiKoMa 2.0, " Entwicklungskosten/ Einführungskosten und Entwicklungsnutzen"

Pos. WiBe 4.0	Haush. wirks.	nicht Hh. wirks.	37	Kritierien-Bezeichnung nach WiBe 4.0	Kostenartengruppe nach MiKoMa 2.0	Personalkosten		Sachkosten						
						Intern	Extern	Externe Leistungen	Software	Hardware	Kommuni-kation	Raum und Gebäude	Sonst. Gem.kosten	Umlagen
				Kriterien Wirtschaftlichkeitsbetrachtung										
1	**h**	**n**		**Entwicklungskosten/Einführungskosten und Entwicklungsnutzen**										
1.1	**h**	**n**		**Entwicklungs-/Einführungskosten für das neue IT-Verfahren**										
1.1.1	h	n		Planungs- und Einführungs-/ Entwicklungskosten		x	x	x	x	x			x	
1.1.1.1		n	1	Personalkosten (eigenes Personal)	Personal intern	x								
1.1.1.2	h		1	Kosten Externer Beratung	Personal extern		x							
1.1.1.3	h		1	Kosten der Entwicklungsumgebung	Externe Leistungen, Hardware, Software			x	x	x				
1.1.1.4	h		1	Sonstige Kosten für Sach-/Hilfsmittel	Sonstige Gemeinkosten								x	
1.1.1.5	h		1	Reisekosten (eigenes Personal)	Personal intern	x								
1.1.2	h	n		Systemkosten										
1.1.2.1	h			Hardwarekosten					x	x	x			
1.1.2.1.1	h		1	Host/ Server, Netzbetrieb	Software, Hardware, Kommunikation				x	x	x			
1.1.2.1.2	h		1	Arbeitsplatzrechner	Software, Hardware, Kommunikation				x	x	x			
1.1.2.2	h			Softwarekosten				x						
1.1.2.2.1	h		1	Kosten für Entwicklung bzw. Beschaffung von Software	Externe Leistungen			x						
1.1.2.2.2	h		1	Kosten für Anpassung von Software und/ oder Schnittstellen	Externe Leistungen			x						
1.1.2.2.3	h		1	Kosten für Evaluierung, Zertifizierung und Qualitätssicherung	Externe Leistungen			x						
1.1.2.3	h	n		Installationskosten		x	x	x		x		x		
1.1.2.3.1	h		1	Bauseitige Kosten	Raum und Gebäude							x		
1.1.2.3.2	h		1	Verlegung technischer Infrastruktur	Hardware					x				
1.1.2.3.3	h		1	Büro-/Raumausstattung, Zubehör	Raum und Gebäude							x		
1.1.2.3.4		n	1	Personalkosten der Systeminstallation	Personal intern, - extern, Externe Leistungen	x	x	x						
1.1.3	h	n		Kosten der Systemeinführung		x	x	x						
1.1.3.1		n	1	System- und Integrationstest(s)	Personal intern, - extern, Externe Leistungen	x	x	x						
1.1.3.2	h		1	Übernahme von Datenbeständen	Personal intern, - extern, Externe Leistungen	x	x	x						
1.1.3.3	h	n	1	Erstschulung Anwender und IT-Fachpersonal	Personal intern, - extern, Externe Leistungen	x	x	x						
1.1.3.4		n	1	Einarbeitungskosten Anwender und IT-Fachpersonal	Personal intern, - extern, Externe Leistungen	x	x	x						
1.1.3.5	h	n	1	Sonstige Umstellungskosten	Personal intern, - extern, Externe Leistungen	x	x	x						
1.2				**Entwicklungs-/Einführungsnutzen aus Ablösung des alten Verfahrens**										
1.2.1	h		1	Einmalige Kosteneinsparungen (Vermeidung von Erhaltungs-/ Erweiterungskosten Altsystem)	Personal intern, - extern, Externe Leistungen	x	x	x						
1.2.2	h		1	Einmalige Erlöse (aus Verwertung Altsystem)	Hardware					x				

Tab. 65: Überleitungstabelle Kriterien WiBe 4.0 zu Kostenartengruppen MiKoMa 2.0, " Betriebskosten und Betriebsnutzen"

Pos. WiBe 4.0	Haush. wirks.	nicht Hh. wirks.	37	Kritierien-Bezeichnung nach WiBe 4.0	Kostenartengruppe nach MiKoMa 2.0	Personalkosten		Sachkosten							
						Intern	Extern	Externe Leistungen	Software	Hardware	Kommuni-kation	Raum und Gebäude	Sonst. Gem.kosten	Umlagen
				Kriterien Wirtschaftlichkeitsbetrachtung											
1	**h**	**n**		**Entwicklungskosten/ Einführungskosten und Entwicklungsnutzen**											
2	**h**	**n**		**Betriebskosten und Betriebsnutzen**											
2.1	**h**	**n**		**Laufende Sachkosten/Sachkosteneinsparungen**						x	x	x			
2.1.1	h	n	1	(Anteilige) Leitungs-/Kommunikationskosten	Kommunikation (Netz)						x				
2.1.2	h	n	1	(Anteilige) Host-, Server- und Netzkosten	Hardware					x					
2.1.3	h	n	1	(Anteilige) Kosten für Arbeitsplatzrechner	Hardware					x					
2.1.4	h	n	1	Verbrauchsmaterial zur Hardware	Hardware					x					
2.1.5	h	n	1	Energie- und Raumkosten	Raum und Gebäude							x			
2.2	**h**	**n**		**Laufende Personalkosten/ Personalkosteneinsparungen**		x	x	x							
2.2.1	h	n	1	Personalkosten aus Systembenutzung	Personal intern	x									
2.2.2	h	n	1	Kosten/ Nutzen aus Dienstpostenumstufung	Personal intern	x									
2.2.3	h	n	1	Systembetreuung und -administration	Personal intern, - extern, Externe Leistungen	x	x	x							
2.2.4	h	n	1	Laufende Schulung/ Fortbildung	Personal intern, - extern, Externe Leistungen	x	x	x							
2.3	**h**	**n**		**Laufende Kosten/Einsparungen bei Wartung /Systempflege**		x	x	x	x	x	x				
2.3.1	h		1	Wartung/ Pflege der Hardware	Personal intern, - extern, Hardware, Kommunikation, Externe Leistungen	x	x	x		x	x				
2.3.2	h		1	Wartung/ Update der Software	Personal intern, - extern, Software, Kommunikation, Externe Leistungen	x	x	x	x		x				
2.3.3	h	n	1	Ersatz-/ Ergänzungskosten	Personal intern, - extern, Externe Leistungen, Software, Hardware, Kommunikation	x	x	x	x	x	x				
2.4	**h**	**n**		**Sonstige Laufende Kosten und Einsparungen**		x	x	x	x	x	x	x	x		
2.4.1	h	n	1	Datenschutz-/ Datensicherungskosten	Personal intern, - extern, Externe Leistungen, Hardware, Software, Raum und Gebäude, Kommunikation, Sonstige Gemeinkosten	x	x	x	x	x	x	x	x		
2.4.2	h	n	1	Kosten begleitender Externer Beratung	Personal extern		x								
2.4.3	h	n	1	Versicherungen u.ä.	Sonstige Gemeinkosten								x		
2.4.4	h	n	1	Sonstige laufende Kosten und Nutzen	Sonstige Gemeinkosten								x		

7.1.2 Matrix zur Soft- und Hardware-Kostenermittlung

Tab. 66: Matrix zur Soft- und Hardware-Kostenermittlung

Migrationsobjekt	Systemtyp	Produkt ... Beispiele ...	Komponenten	Kosten			
				Investitions-Kosten	lfd. Kosten Jahr 1	lfd. Kosten Jahr 2	lfd. Koste Jahr 3
Server							
Software							
Infrastrukturdienste	Directory	NDS					
	File	Netware 4.11					
	Druck	Jet Direct					
	DNS/ DHCP/ BOOTP	BIND					
Systemmanagement	Softwareverteilung						
	Inventarisierung						
	HelpDesk						
	Systemüberwachung	MRTG/ Nagios/ SNMPWatchNetview					
	Netzwerküberwachung						
Groupware & Messaging	Groupware	eGroupware					
	Mail	Suse Email 2					
Terminalserver							
Hardware							
Arbeitsplatzcomputer							
Software							
Betriebssystem	Betriebssystem	Windows NT 4.0					
Standardsoftware	Dokumentenaustausch, PDF-Betrachter	Acrobat Reader					
	Webbrowser und Mailclient	Mozilla					
	Büro	Open Office					
	Komprimierung	WinZip					
	Datenbank	Access					
	Tabellenkalkulation	Excel					
	Präsentation	Powerpoint					
	Textverarbeitung	Word					
Terminalserver (Client Zugriff)							
Hardware							

Tab. 67: Ausschnitt Summenübersicht für Projekte eines Beipiel-Migrationsvorhabens

Projekt			Kat	Personalaufwand						
Migrationsvorhaben 123	**Summe Gesamt**	**Projekt-Stufe**		Summe Pers.kosten	Personentage		Personalkosten		Externe Dienstleistungen	Software Wartung
					Intern	Extern	Intern	Extern		
S u m m e n - Ü b e r s i c h t - G e s a m t -										
Saldo Gesamt	**-331.012**	**Gesamt**		**3.177.744**	**16.094,0**	**681,5**	**4.205.446**	**-1.027.702**	**-458.392**	**-1.900.665**
Saldo Var. 2	**696.690**	**Var. 2**		**3.177.744**	**16.094,0**	**681,5**	**4.205.446**	**-1.027.702**	**569.310**	**-1.900.665**
Summe -K- Var. 2	-1.234.523	**Var. 2**	**K**	**-1.234.523**	**700,0**	**681,5**	**-206.821**	**-1.027.702**	**0**	**0**
Summe -B- Var. 2	-3.099.855	**Var. 2**	**B**	**0**	**0,0**	**0,0**	**0**	**0**	**0**	**-1.938.465**
Summe -E- Var. 2	5.031.067	**Var. 2**	**E**	**4.412.267**	**15.394,0**	**0,0**	**4.412.267**	**0**	**569.310**	**37.800**
S u m m e n - Ü b e r s i c h t - haushaltswirksam -										
Saldo Gesamt	**-3.508.757**	**Gesamt**		**-1.027.702**	**0,0**	**681,5**	**0**	**-1.027.702**	**569.310**	**-1.900.665**
Saldo Var. 2	**-3.508.757**	**Var. 2**		**-1.027.702**	**0,0**	**681,5**	**0**	**-1.027.702**	**569.310**	**-1.900.665**
Summe -K- Var. 2	-1.027.702	**Var. 2**	**K**	**-1.027.702**	**0,0**	**681,5**	**0**	**-1.027.702**	**0**	**0**
Summe -B- Var. 2	-3.099.855	**Var. 2**	**B**	**0**	**0,0**	**0,0**	**0**	**0**	**0**	**-1.938.465**
Summe -E- Var. 2	618.800	**Var. 2**	**E**	**0**	**0,0**	**0,0**	**0**	**0**	**569.310**	**37.800**
S u m m e n - Ü b e r s i c h t - nicht haushaltswirksam -										
Saldo Gesamt	**3.177.744**	**Gesamt**		**4.205.446**	**16.094,0**	**0,0**	**4.205.446**	**0**	**-1.027.702**	**0**
Saldo Var. 2	**4.205.446**	**Var. 2**		**4.205.446**	**16.094,0**	**0,0**	**4.205.446**	**0**	**0**	**0**
Summe -K- Var. 2	-206.821	**Var. 2**	**K**	**-206.821**	**700,0**	**0,0**	**-206.821**	**0**	**0**	**0**
Summe -B- Var. 2	0	**Var. 2**	**B**	**0**	**0,0**	**0,0**	**0**	**0**	**0**	**0**
Summe -E- Var. 2	4.412.267	**Var. 2**	**E**	**4.412.267**	**15.394,0**	**0,0**	**4.412.267**	**0**	**0**	**0**

Tab. 68: Ausschnitt Projektübersicht für Beipiel-Migrationsvorhaben

Projekt			Kat	Personalaufwand							
Migrationsvorhaben 123	**Summe Gesamt**	**Projekt-Stufe**		Summe Pers.kosten	Personentage		Personalkosten		Externe Dienstleistungen	Software Wartung	S In
					Intern	Extern	Intern	Extern			
Projekte:		Standard									
Software	**-1.161.390**	Var. 2		0	0,0	0,0	0	0	0	0	
Wartung	**-1.938.465**	Var. 2		0	0,0	0,0	0	0	0	-1.938.465	
Feinkonzept	**-249.837**	Var. 2		-249.837	80,0	150,0	-23.637	-226.200	0	0	
Customizing	**-592.824**	Var. 2		-592.824	118,0	370,0	-34.864	-557.960	0	0	
Schulung	**-50.842**	Var. 2		-50.842	70,0	20,0	-20.682	-30.160	0	0	
Projektmanagement	**-164.406**	Var. 2		-164.406	240,0	62,0	-70.910	-93.496	0	0	
Qualitätssicherung	**-111.304**	Var. 2		-111.304	96,0	55,0	-28.364	-82.940	0	0	
Dokumentation	**-65.310**	Var. 2		-65.310	96,0	24,5	-28.364	-36.946	0	0	
AfA externe Personalkosten	**-1.027.702**	Stufe 2		0	0,0	0,0	0	0	-1.027.702	0	
Ersparnis Prozess 1 (in allen Szenarien gleich)	**279.507**	Var. 2		279.507	1.406,4	0,0	279.507	0	0	0	
Ersparnis Prozess 2 (in allen Szenarien gleich)	**4.132.760**	Var. 2		4.132.760	13.987,6	0,0	4.132.760	0	0	0	
Ersparnisse aus Ist-Betriebskosten	**618.800**	Var. 2		0	0,0	0,0	0	0	569.310	37.800	

Tab. 69: Ausschnitt Projektbeispiel "Software" für Beipiel-Migrationsvorhaben

Projekt			Kat	Personalaufwand							
Migrationsvorhaben 123	**Summe Gesamt**	**Projekt-Stufe**		Summe Pers.kosten	Personentage		Personalkosten		Externe Dienstleistungen	Software Wartung	S In
					Intern	Extern	Intern	Extern			
Projekte:		Standard									
Software	**-1.161.390**	Var. 2		0	0,0	0,0	0	0	0	0	
Software	0	Var. 2	**K**	0	0,0	0,0	0	0	0	0	
Software	**-1.161.390**	Var. 2	**B**	0	0,0	0,0	0	0	0	0	
Software	0	Var. 2	**E**	0	0,0	0,0	0	0	0	0	
Software	**232.278**	Var. 2	B	0			0	0			
Software	**232.278**	Var. 2	B	0			0	0			
Software	**232.278**	Var. 2	B	0			0	0			
Software	**232.278**	Var. 2	B	0			0	0			
Software	**232.278**	Var. 2	B	0			0	0			

Tab. 70: Ausschnitt Projektbeispiel "Customizing" für Beipiel-Migrationsvorhaben

Projekt			Kat	Personalaufwand							
Migrationsvorhaben 123	**Summe Gesamt**	**Projekt-Stufe**		Summe Pers.kosten	Personentage		Personalkosten		Externe Dienstleistungen	Software Wartung	S In
					Intern	Extern	Intern	Extern			
Projekte:		Standard									
Software	**-1.161.390**	Var. 2		0	0,0	0,0	0	0	0	0	
Wartung	**-1.938.465**	Var. 2		0	0,0	0,0	0	0	0	-1.938.465	
Feinkonzept	**-249.837**	Var. 2		-249.837	80,0	150,0	-23.637	-226.200	0	0	
Customizing	**-592.824**	Var. 2		-592.824	118,0	370,0	-34.864	-557.960	0	0	
Customizing	**-592.824**	Var. 2	**K**	-592.824	118,0	370,0	-34.864	-557.960	0	0	
Customizing	0	Var. 2	**B**	0	0,0	0,0	0	0	0	0	
Customizing	0	Var. 2	**E**	0	0,0	0,0	0	0	0	0	
Customizing	**557.960**	Var. 2	K	557.960		370,0	0	557.960			
Customizing	**34.864**	Var. 2	K	34.864	118,0		34.864	0			

7.2 Rechtsgrundlagen

BHO[1], § 7 Wirtschaftlichkeit und Sparsamkeit, Kosten- und Leistungsrechnung

(1) Bei Aufstellung und Ausführung des Haushaltsplans sind die Grundsätze der Wirtschaftlichkeit und Sparsamkeit zu beachten. Diese Grundsätze verpflichten zur Prüfung, inwieweit staatliche Aufgaben oder öffentlichen Zwecken dienende wirtschaftliche Tätigkeiten durch Ausgliederung und Entstaatlichung oder Privatisierung erfüllt werden können.

(2) Für alle finanzwirksamen Maßnahmen sind angemessene Wirtschaftlichkeitsuntersuchungen durchzuführen. In geeigneten Fällen ist privaten Anbietern die Möglichkeit zu geben darzulegen, ob und inwieweit sie staatliche Aufgaben oder öffentlichen Zwecken dienende wirtschaftliche Tätigkeiten nicht ebenso gut oder besser erbringen können (Interessenbekundungsverfahren).

(3) In geeigneten Bereichen ist eine Kosten- und Leistungsrechnung einzuführen.

VV[2] zu § 7 BHO:

1 Grundsatz der Wirtschaftlichkeit[3]

Die Ausrichtung jeglichen Verwaltungshandelns nach dem Grundsatz der Wirtschaftlichkeit soll die bestmögliche Nutzung von Ressourcen bewirken. Damit gehört zur Beachtung des Grundsatzes der Wirtschaftlichkeit auch die Prüfung, ob eine Aufgabe durchgeführt werden muss und ob sie durch die staatliche Stelle durchgeführt werden muss.

Nach dem Grundsatz der Wirtschaftlichkeit ist die günstigste Relation zwischen dem verfolgten Zweck und den einzusetzenden Mitteln (Ressourcen) anzustreben. Der Grundsatz der Wirtschaftlichkeit umfasst das Sparsamkeits- und das Ergiebigkeitsprinzip. Das Sparsamkeitsprinzip (Minimalprinzip) verlangt, ein bestimmtes Ergebnis mit möglichst geringem Mitteleinsatz zu erzielen. Das Ergiebigkeitsprinzip (Maximalprinzip) verlangt, mit einem bestimmten Mitteleinsatz das bestmögliche Ergebnis zu erzielen. Bei der Ausführung des Haushaltsplans, der in aller Regel die Aufgaben (Ergebnis, Ziele) bereits formuliert, steht der Grundsatz der Wirtschaftlichkeit in seiner Ausprägung als Sparsamkeitsprinzip im Vordergrund.

---

1 Vgl. Bundeshaushaltsordnung, i.d.F.v. 19.8.1969, zuletzt geändert durch Gesetz zur Änderung von Vorschriften über parlamentarische Gremien vom 17.6.1999

2 Vgl. Vorschriftensammlung der Bundesfinanzverwaltung, Verwaltungsvorschrift zur Bundeshaushaltsordnung, i.d.F.v. 16.05.2001, S. 16 ff

3 Mit dem Grundsatz der Wirtschaftlichkeit sind - in Übereinstimmung mit der herrschenden Meinung in den Verwaltungswissenschaften - die Grundsätze der Wirtschaftlichkeit und Sparsamkeit im Sinne des § 7 BHO gemeint.

Der Grundsatz der Wirtschaftlichkeit ist bei allen Maßnahmen des Bundes, die die Einnahmen und Ausgaben des Bundeshaushaltes unmittelbar oder mittelbar beeinflussen, zu beachten. Dies betrifft sowohl Maßnahmen, die nach einzelwirtschaftlichen Kriterien (z.B. Beschaffungen für den eigenen Verwaltungsbereich und Organisationsänderungen in der eigenen Verwaltung) als auch Maßnahmen, die nach gesamtwirtschaftlichen Kriterien (z.B. Investitionsvorhaben im Verkehrsbereich, Subventionen und Maßnahmen der Sozial- und Steuerpolitik) zu beurteilen sind. Unter die Maßnahmen fallen auch Gesetzgebungsvorhaben.

2 Wirtschaftlichkeitsuntersuchungen

Wirtschaftlichkeitsuntersuchungen sind Instrumente zur Umsetzung des Grundsatzes der Wirtschaftlichkeit. Es ist zwischen einzel- und gesamtwirtschaftlichen Wirtschaftlichkeitsuntersuchungen zu unterscheiden.

Wirtschaftlichkeitsuntersuchungen sind bei allen Maßnahmen durchzuführen. Sie sind daher bei der Planung neuer Maßnahmen einschließlich der Änderung bereits laufender Maßnahmen (Planungsphase) sowie während der Durchführung (im Rahmen einer begleitenden Erfolgskontrolle) und nach Abschluss von Maßnahmen (im Rahmen einer abschließenden Erfolgskontrolle) vorzunehmen.

2.1 Wirtschaftlichkeitsuntersuchungen als Planungsinstrument

Wirtschaftlichkeitsuntersuchungen in der Planungsphase bilden die Grundlage für die begleitenden und abschließenden Erfolgskontrollen. Wirtschaftlichkeitsuntersuchungen müssen mindestens Aussagen zu folgenden Teilaspekten enthalten:

- Analyse der Ausgangslage und des Handlungsbedarfs,
- Ziele, Prioritätsvorstellungen und mögliche Zielkonflikte,
- relevante Lösungsmöglichkeiten und deren Nutzen und Kosten (einschl. Folgekosten), auch soweit sie nicht in Geld auszudrücken sind,
- finanzielle Auswirkungen auf den Haushalt,
- Eignung der einzelnen Lösungsmöglichkeiten zur Erreichung der Ziele unter Einbeziehung der rechtlichen, organisatorischen und personellen Rahmenbedingungen,
- Zeitplan für die Durchführung der Maßnahme,
- Kriterien und Verfahren für Erfolgskontrollen (vgl. Nr. 2.2).

Ist das angestrebte Ziel nach dem Ergebnis der Ermittlungen oder aus finanziellen Gründen nicht in vollem Umfang zu verwirklichen, so ist zu prüfen, ob das erreichbare Teilziel den Einsatz von Mitteln überhaupt rechtfertigt und ob die geplante Maßnahme besser zu einem späteren Zeitpunkt durchgeführt werden sollte.

Besteht für den Erwerb oder die Nutzung von Vermögensgegenständen eine Wahlmöglichkeit zwischen Kauf-, Miet-, Leasing-, Mietkauf- und ähnlichen Verträgen, so ist vor dem Vertragsabschluss zu prüfen, welche Vertragsart für die

Verwaltung am wirtschaftlichsten ist; ein Mangel an Haushaltsmitteln für den Erwerb durch Kauf reicht als Rechtfertigungsgrund für die Begründung von Dauerschuldverhältnissen nicht aus. Bei der Ausübung der Wahlmöglichkeit ist zu berücksichtigen, dass Leasingverträge hinsichtlich ihrer Wirtschaftlichkeit im Einzelfall einer besonders eingehenden Prüfung bedürfen.

2.2 Wirtschaftlichkeitsuntersuchungen als Instrument der Erfolgskontrolle

Die Erfolgskontrolle ist ein systematisches Prüfungsverfahren. Sie dient dazu, während der Durchführung (begleitende Erfolgskontrolle) und nach Abschluss (abschließende Erfolgskontrolle) einer Maßnahme ausgehend von der Planung festzustellen, ob und in welchem Ausmaß die angestrebten Ziele erreicht wurden, ob die Maßnahme ursächlich für die Zielerreichung war und ob die Maßnahme wirtschaftlich war.

Bei Maßnahmen, die sich über mehr als zwei Jahre erstrecken, und in sonstigen geeigneten Fällen sind nach individuell festzulegenden Laufzeiten oder zu Zeitpunkten, an denen abgrenzbare Ergebnisse oder Teilrealisierungen einer Maßnahme zu erwarten sind, begleitende Erfolgskontrollen durchzuführen. Sie liefern vor dem Hintergrund zwischenzeitlich eingetretener ökonomischer, gesellschaftlicher und technischer Veränderungen die notwendigen Informationen für die Entscheidung, ob und wie die Maßnahme fortgeführt werden soll.

Von der begleitenden Erfolgskontrolle ist die laufende Beobachtung zu unterscheiden. Im Gegensatz zum systematisch angelegten umfassenden Prüfungsverfahren der Erfolgskontrolle ist sie eine fortlaufende gezielte Sammlung und Auswertung von Hinweisen und Daten zur ergänzenden Beurteilung der Entwicklung einer Maßnahme. Alle Maßnahmen sind nach ihrer Beendigung einer abschließenden Erfolgskontrolle zur Überprüfung des erreichten Ergebnisses zu unterziehen.

Methodisch besteht zwischen begleitender und abschließender Erfolgskontrolle kein Unterschied.

Die Erfolgskontrolle umfasst grundsätzlich folgende Untersuchungen:

- Zielerreichungskontrolle
  Mit der Zielerreichungskontrolle wird durch einen Vergleich der geplanten Ziele mit der tatsächlich erreichten Zielrealisierung (Soll-Ist-Vergleich) festgestellt, welcher Zielerreichungsgrad zum Zeitpunkt der Erfolgskontrolle gegeben ist. Sie bildet gleichzeitig den Ausgangspunkt von Überlegungen, ob die vorgegebenen Ziele nach wie vor Bestand haben.

- Wirkungskontrolle
  Im Wege der Wirkungskontrolle wird ermittelt, ob die Maßnahme für die Zielerreichung geeignet und ursächlich war. Hierbei sind alle beabsichtigten und unbeabsichtigten Auswirkungen der durchgeführten Maßnahme zu ermitteln.

- Wirtschaftlichkeitskontrolle
  Mit der Wirtschaftlichkeitskontrolle wird untersucht, ob der Vollzug der Maß-

nahme im Hinblick auf den Ressourcenverbrauch wirtschaftlich war (Vollzugswirtschaftlichkeit) und ob die Maßnahme im Hinblick auf übergeordnete Zielsetzungen insgesamt wirtschaftlich war (Maßnahmenwirtschaftlichkeit).

Erfolgskontrollen sind auch durchzuführen, wenn die Dokumentation in der Planungsphase unzureichend war. In diesem Fall sind die benötigten Informationen nachträglich zu beschaffen.

Die Zielerreichungskontrolle und die Wirkungskontrolle sind die Grundlagen für die Wirtschaftlichkeitskontrolle. Im Gegensatz zur Wirtschaftlichkeitskontrolle lassen sie aber den Mitteleinsatz unberücksichtigt.

2.3 Methoden (Verfahren) der Wirtschaftlichkeitsuntersuchungen[1]

2.3.1 Allgemeines

Bei der Durchführung von Wirtschaftlichkeitsuntersuchungen ist die nach den Erfordernissen des Einzelfalls einfachste und wirtschaftlichste Methode anzuwenden. Zur Verfügung stehen einzelwirtschaftlich und gesamtwirtschaftlich orientierte Verfahren. Welches Verfahren anzuwenden ist, bestimmt sich nach der Art der Maßnahme, dem mit ihr verfolgten Zweck und den mit der Maßnahme verbundenen Auswirkungen.

Gesamtwirtschaftlich orientierte Verfahren sind für alle Maßnahmen mit rheblichen gesamtwirtschaftlichen Auswirkungen geeignet. Einzelwirtschaftlich orientierte Verfahren sind geeignet für Maßnahmen, die sich in erster Linie auf den betrachteten Verwaltungsbereich (z.B. Ministerium, Behörde) beziehen.

2.3.2 Einzelwirtschaftliche Verfahren

Für Maßnahmen mit nur geringen und damit zu vernachlässigenden gesamtwirtschaftlichen Nutzen und Kosten sind grundsätzlich die finanzmathematischen Methoden der Investitionsrechnung (z.B. Kapitalwertmethode) zu verwenden. Für Maßnahmen mit nur geringer finanzieller Bedeutung können auch Hilfsverfahren der Praxis (z.B. Kostenvergleichsrechnungen, Angebotsvergleiche) durchgeführt werden.

2.3.3 Gesamtwirtschaftliche Verfahren

Für Maßnahmen, die nicht zu vernachlässigende gesamtwirtschaftliche Auswirkungen haben, sind gesamtwirtschaftliche Wirtschaftlichkeitsuntersuchungen (z.B. Kosten-Nutzen-Analyse) durchzuführen.

2.4 Verfahrensvorschriften

2.4.1 Die Wirtschaftlichkeitsuntersuchungen sind grundsätzlich von der Organisationseinheit durchzuführen, die mit der Maßnahme befasst ist.

[1] Vgl. Arbeitsanleitung Einführung in Wirtschaftlichkeitsuntersu-chungen, Anlage zum Rundschreiben des BMF vom 31. August 1995 - II A 3 - H 1005 - 23/95 - (GMBl 1995, S. 764).

2.4.2 Das Ergebnis der Untersuchung ist zu vermerken und zu den Akten zu nehmen. Bei Maßnahmen mit nur geringer finanzieller Bedeutung kann hiervon abgesehen werden.

2.4.3 Zu den Unterlagen nach § 24 gehören auch Wirtschaftlichkeitsuntersuchungen.

2.4.4 Die Beauftragten für den Haushalt entscheiden, über welche Wirtschaftlichkeitsuntersuchungen sie zu unterrichten sind. Sie können sich an den Wirtschaftlichkeitsuntersuchungen beteiligen und die Berücksichtigung einer Maßnahme bei der Aufstellung der Voranschläge und bei der Ausführung des Haushaltsplans von der Vorlage von Wirtschaftlichkeitsuntersuchungen abhängig machen.

3 Interessenbekundungsverfahren[1]

In geeigneten Fällen ist privaten Anbietern die Möglichkeit zu geben darzulegen, ob und inwieweit sie staatliche Aufgaben oder öffentlichen Zwecken dienende wirtschaftliche Tätigkeiten nicht ebenso gut oder besser erbringen können (Interessenbekundungsverfahren).

Ein Interessenbekundungsverfahren kommt bei der Planung neuer und der Überprüfung bestehender Maßnahmen oder Einrichtungen in Betracht. Es erfordert eine Erkundung des Marktes nach wettbewerblichen Grundsätzen. Das Ergebnis der Markterkundung ist mit den sich bietenden staatlichen Lösungsmöglichkeiten zu vergleichen, um eine wirtschaftliche Bewertung zu gewährleisten.

Das Interessenbekundungsverfahren ersetzt nicht das Verfahren zur Vergabe öffentlicher Aufträge. Wenn das Interessenbekundungsverfahren ergibt, dass eine private Lösung voraussichtlich wirtschaftlich ist, ist ein Verfahren zur Vergabe öffentlicher Aufträge durchzuführen.

4 Kosten- und Leistungsrechnung

Dauerhafte Aufgabe der öffentlichen Verwaltung ist es, das Verhältnis von Kosten und Leistungen bei der Aufgabenwahrnehmung zu verbessern. Grundlage dafür ist die Einführung einer Kosten- und Leistungsrechnung gemäß der Standard-KLR[2].

Die mit der Kosten- und Leistungsrechnung erzielten Ergebnisse machen entstandene Kosten und erbrachte Leistungen transparent. Ebenso wird eine wirksame Planung, Steuerung und Kontrolle ermöglicht. Auch die Haushaltsplanung und -ausführung kann durch die Kosten- und Leistungsrechnung unterstützt werden. Ebenso ist durch Informationen der Kosten- und Leistungsrechnung eine Ermittlung von kostendeckenden Gebühren und Entgelten realisierbar.

… Ende VV zu § 7 BHO

---

1 Zur Durchführung des Interessenbekundungsverfahrens vgl. Rundschreiben des BMF vom 31. August 1995 - II A 3 - H 1005 - 22/95 - (GMBl 1995, S. 764).

2 VSF H 90 01

8 Mitwirkende Autoren und Experten

8.1 Autoren

Die Darstellung erfolgt in alphabetischer Reihenfolge.

Bernd Dersch, Spezialist für IT-Strategien, Betriebskonzepte und Datenbank- und Webanwendungen. Herr Dersch hatte die Projektleitung bei der Erstellung des Leitfadens und er hat als Autor u.a. an den technischen Betrachtungen der Desktopmigration mitgewirkt. <bernd.dersch@eds.com>

Peter Ganten hat sich auf die Themen Verzeichnisdienste, Migration von Windows NT-basierten Domänen nach Samba und OpenLDAP unter Linux sowie für die Bereiche Thin Clients und Integration von Windows-Anwendungen auf dem Linux-Desktop spezialisiert. Er hat an den entsprechenden Abschnitten im Leitfaden mitgewirkt. <ganten@univention.de>

Roberto Herrmann ist auf die Wirtschaftlichkeitsbetrachtungen und Controlling großer IT-Projekte spezialisiert. Herr Herrmann hat diesbezüglich auch am Abschnitt zu den Wirtschaftlichkeitsbetrachtungen als Autor mitgewirkt. <roberto.herrmann@eds.com>

Sebastian Hetze hat an den Abschnitten Datenbanken, Dateiablage, Netzwerk- und Systemmanagementdiensten des Leitfadens als Autor mitgewirkt. Seine Spezialgebiete sind Datenbanken und Dateiablage unter Linux sowie Datenaustauschformate. <s.hetze@linux-ag.de>

Gregor Lietz setzt seine Schwerpunkte im Bereich der Enterprise Architekturen und beschäftigt sich insbesondere mit auf Effizienz ausgerichteten IT-Strategien für Organisationen und Unternehmen. Er ist Mitglied in der SAGA-Expertenkommission des BMI und verantwortet die Gesamtredaktion des Migrationsleitfadens. Als Autor wirkte Herr Lietz an mehreren Abschnitten mit, u.a. an der Wirtschaftlichkeitsbetrachtung sowie den Migrationspfaden und -empfehlungen. <gregor.lietz@eds.com>

Dr. Axel Metzger ist u.a Experte für Urheber-, Patent- und Computerrecht. Er beschäftigt sich schon seit längerem mit den rechtlichen Rahmenbedingungen des Einsatzes von Freier Software. Herr Metzger hat in diesem Zusammenhang die Ausführungen zu den „Rechtlichen Aspekten“, die mit der zweiten Auflage des Migrationsleitfadens aufgenommen wurden, verfasst. <metzger@mpipriv-hh.mpg.de>

Kurt Pfeifle hat sich auf die Integration von netzwerkweiten Druckdiensten in heterogenen Umgebungen spezialisiert und hat diesbezüglich an den technischen Betrachtungen zu den Druckdiensten als Autor mitgewirkt.
<kpfeifle@danka.de>

Dr. Klaus Schmidt ist Experte für IT-Infrastruktur und Produkt-Entwicklung. In dieser Funktion ist er insbesondere Spezialist für Hochverfügbarkeitslösungen. Er hat an den entsprechenden Abschnitten des Leitfadens mitgewirkt

Holger Stautmeister ist Spezialist für Webtechnologien, Content- und Wissensmanagement-Systeme. In diesem Zusammenhang hat er u. a. als Autor an den Abschnitten Webserver- und Groupwaremigration mitgewirkt.
<holger.stautmeister@eds.com>

Sebastian Stöcker ist auf Microsoft Infrastrukturen und Systemarchitekturen spezialisiert und hat wesentliche Teile der technischen Betrachtungen bezüglich der Microsoft-Komponenten verfasst.

Thomas Uhl beschäftigt sich mit der Integration offener Systeme und insbesondere im Open Source Bereich. Er hat als Autor Textbeiträge zu den technischen Betrachtungen von Groupware und Terminalservices beigetragen.
<thomas.uhl@to.com>

Marc Werner sieht unter anderem die Themen Softwarearchitekturen, Systemintegration auf Basis von Webservices und als Kernpunkte seiner Arbeit. Als Autor der Betrachtungen zur Interoperabilität von Office-Anwendungen und der Backend-Integration hat er maßgeblich an der ersten Fortschreibung des Leitfadens mitgewirkt.<marc.werner-eds@eds.com>

8.2 Experten

Die Darstellung erfolgt in alphabetischer Reihenfolge.

Frank Gamerdinger als Spezialist für Open- und StarOffice hat er an den technischen Betrachtungen zur Office-Migration mitgewirkt.
<frank.gamerdinger@sun.com>

Volker Lendecke ist Mitglied des Samba Core Entwicklerteams. Diesbezüglich hat er wichtige Erkenntnisse zu den technischen Betrachtungen der Infrastruktudienste Dateiablage, Authentifizierung, und Druckdienste beigetragen.
<vl@sernet.de>

Dieter Löschky setzt einen wichtigen Schwerpunkt seiner Arbeit in die Weiterentwicklung der Interoperabilität zw. MS Office und StarOffice / OpenOffice.org sowie der in StarOffice / OpenOffice.org verankerten XML-Strategie.
<Dieter.Loeschky@sun.com>

Michael Meskes ist auf DBMS und insbesondere auf PostgreSQL spezialisiert und hat diesbezüglich Beiträge zu den technischen Betrachtungen beigetragen.
<Michael.Meskes@credativ.de>

Dr. Carsten Schulz ist als Rechtsanwalt schwerpunktmäßig in den Bereichen gewerblicher Rechtsschutz, Urheberrecht und Wettbewerbsrecht im IT-Sektor tätig. Er hat als beteiligter Experte am Abschnitt über die rechtlichen Aspekte einer Migration mitgewirkt. <carsten.schulz@ifross.de>

9 Abkürzungsverzeichnis

a.a.O	am angegebenden Ort
Abs.	Absatz
ACE	Access Control Entries
ACL	Access Control List
AD	Active Directory
ADAM	Active Directory Application Mode
ADC	Active Directory Connector
ADO	ActiveX Data Objects
ADS	Active Directory Service
ADSI	Active Directory Service Interface
AFS	Andrew File System
API	Application Programming Interface
APOC	"A Point Of Control"
APOP	Authenticated Post Office Protocol
APT	Advanced Package Tool
ASCII	American Standard Code for Information Interchange
ASF	Apache Software Foundation
ASP	Active Server Pages
Aufl.	Auflage
AZ	Aktenzeichen
BB	Bulletin Boards
BDC	Backup Domain Controller
BfD	Bundesbeauftragter für den Datenschutz
BGB	Bürgerliches Gesetzbuch
BHO	Bundes-Haushalts-Ordnung
BIND	Berkeley Internet Name Domain
BMI	Bundesministerium des Innern
BSD	Berkeley Software Distribution
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVA	Bundesverwaltungsamt
BVB	Besondere Vertragsbedingungen

CA	Certification Authority
CAS	Code Access Security
CDO	Collaboration Data Objects
CGI	Common Gateway Interface
CIFS	Common Internet File System
CIM	Common Information Model
CIS	COM Internet Service
CLI	Common Language Infrastructur
CLR	Common Language Runtime
cn	common Name
CO	Crossover Office
COM	Component Object Models
COM+	Component Object Models
CORBA	Common Objects Request Broker Architecture
COLS	Commercial Linux Software
CPU	Central Processing Unit
CSS	Cascading Style Sheets
CUPS	Common UNIX Printing System
DACL	Discretionary Access Control List
DAV	Distributed Authoring and Versioning
DBMS	Datenbankmanagementsystem
dc	domainComponent
DCOM	Distributed Component Object Models
DDE	Dynamic Data Exchange
DDNS	Dynamic DNS
DFS	Distributed File System
d.h.	das heißt
DHCP	Dynamic Host Configuration Protocol
DLC	Data Link Control
DLL	Dynamic Link Libraries
DMS	Dokumentenmanagementsystem
DNS	Domain Name Server

DNSSEC	Domain Name System Security
DRBD	Distributed Replicated Block Device
DS	Directory Service
DSO	Dynamic Shared Objects
DTD	Document Type Definition
DTS	Data Transformation Services
E2K	Exchange 2000
EFS	Encrypting File System
EJB	Enterprise Java Beans
EMF	Enhanced Meta Format
ESC/P	Epson Printer Language
EULA	End User License Agreement
EVB-IT	Ergänzende Vertragsbedingungen für die Beschaffung von IT-Leistungen
EXT2	Extendend Filesysten Version 2
EXT3	Extended Filesystem Version 3
FAT	File Allocation Table
f., ff.	folgende
Fn.	Fußnote
FQDN	Full Qualified Domain Name
FRS	File Replication Service
FSG	Free Standard Group
FSMO	Flexible Single Master Operation
FTP	File Transfer Protocol
GC	Global Catalog
GDI	Graphics Device Interface
GNOME	GNU Network Object Model Environment
GNU	GNU's Not UNIX
GPL	General/Gnu Public License
GPOs	Group Policy Objects
GPS	Global Positioning System
GUID	Global Unique Identifier
GWB	Gesetz gegen Wettbewerbsbeschränkungen

HACMP	High Availability Cluster Management Protocol
HD	Harddisk
HIS	Host Integration Server
HP	Hewlett-Packard
Hrsg.	Herausgeber
HSM	Hierarchical Storage Management
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hyper-Text Transfer Protocol Secure
ICA	Independent Computing Architecture
IDE	Integrated Development Enviroment
IEAK	Internet Explorer Administration Kit
IETF	Internet Engineering Task Force
IIOP	Internet Inter-ORB Protocol
IIS	Internet Information Server
IL	Intermediate Language
IMAP4	Internet Mail Access Protocol 4
IMAPS	Internet Mail Access Protocol Secure
IPC	Interprocess Communication
IPP	Internet Printing Protocol
Ipsec	Internet Protocol Security Protocol
IPv6	IP Version 6
IPX	Internet Packet Exchange
IRC	Internet Relay Chats
IRM	Information Rights Management
IS	Information Store
ISA	Internet Security and Acceleration
ISAPI	Internet Service Application Programming Interface
ISC	Internet Software Consortium
IT-WiBe	Empfehlung zur Durchführung von Wirtschaftlichkeitsbetrachtungen beim Einsatz der IT in der Bundesverwaltung
J2EE	Java 2 Enterprise Edition

J2SE	Java 2 Standard Edition
JAXP	Java API for XML
JDBC	Java Database Connection
JDS	Sun Java Desktop System
JFS	Journaled File System
JIT	Just In Time
JMC	Java Message Service
JNDI	Java Naming and Directory Interface
JRE	Java Runtime Environment
JRMI	Java Remote Methode Invocation
JSP	Java Server Pages
JTA	Java Transaction API
JVM	Java Virtual Machine
KBSt	Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung
KDC	Key Distribution Center
KDE	K Desktop Environment
KMS	Key Management Server
LAMP	Linux, Apache, MySQL, PHP
LAN	Local Area Network
LANANA	Linux Assigned Names and Numbers Authority
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Data Interchange Format
LGPL	Lesser General Public License
Li18nux	Linux Internationalization Initiative
LM	LAN Manager
LMRepl	Verzeichnisreplikationsdienst
LPD	Line Printing Daemon
LPI	Linux Professional Institute
LPR	Line Printing Redirector
LSB	Linux Standard Base
LTSP	Linux Terminal Server Project
LVM	Logical Volume Manager

LVS	Linux Virtual Server
MAC	Media Access Control
MAPI	Messaging Application Programming Interface
MDX	Message Digest X
MLP	Message/Multilayer Link Protocol
MMC	Microsoft Management Console
MMQS	Microsoft Message Queue Server
MOM	Microsoft Operation Manager
MPL	Mozilla Public License
MRTG/RRD	Multi Router Traffic Grapher/Round Robin Database
MS	Microsoft
MSMQ	Microsoft Message Queuing
MSPS	Microsoft Proprietary Standards
MTA	Message Transfer Agent
MTBF	mean time between failure
MTS	Microsoft Transaction Server
MTTR	Mean Time To Repair
NAS	Network Attached Storage
NAT	Network Address Translation
NCSA	National Center for Supercomputing Application
NetBEUI	NetBIOS Extended User Interface
NetBIOS	Network Basic Input and Output System
NetBT	NetBIOS over TCP/IP
NFS	Network File System
NIS	Network Information Service
NLD	Novell Linux Desktop
NNTP	Network News Transport Protocol
NPL	Netscape Public License
NTDS	NT Directory Service
NTFS	NT File System
NTFS4	NT File System 4
NTFS5	New Technology File System 5

NTLM	Windows NT LAN Manager
NTLMv2	Windows NT LAN Manager Version 2
NTP	Network Time Protocol
o.ä.	oder ähnliches
ODBC	Open Database Connectivity
OLAP	Online Analytical Processing
OLE	Object Linking and Embedding
OGo	OpenGroupware.org
OMG	Object Management Group
OOo	OpenOffice.org
OOo/SO	Open Office.org/StarOffice
OSI	Open Systems Interconnection
OSOS	Open Standards mit Open Source
OSS	Open Source Software
OU	Organizational Unit
OWA	Outlook Web Access
PAM	Pluggable Authentication Module
PatG	Patentgesetz
PBS	Portable Batch System
PCL	Printer Control Language
PDA	Personal Digital Assistant
PDC	Primary Domain Controller
PDF	Portable Document Format
Perl	Practical Extraction and Report Language
PHP	PHP Hypertext Pre-processor
PIM	Personal Information Manager
PKI	Public Key Infrastructure
POP3	Post Office Protocol Version 3
POSIX	Portable Operating System Interface for UNIX
PPD	PostScript Printer Descriptions
ProdHaftG	Produkthaftungsgesetz
PT	Personentage

PXE	Pre-Boot Execution Environment
RAC	Real Application Cluster
RAID	Redundant Array of Inexpensive/Independent Discs
RAM	Random Access Machine/Memory
RAS	Remote Access Service
RAW	Read After Write
RDBMS	Relationales Datenbank Management System
RDP	Remote Desktop Protocol
ReiserFS	Reiser File System
RFCs	Request for Comments
RHCE	Red Hat Certified Engineer
RHD	Red Hat Desktop
RHN	Red Hat Network
RID	Relative Identifier
RISC	Reduced Instruction Set Computer
RMS	Rights Management Services
RPC	Remote Procedure Calls
RPM	Red Hat Packet Management
Rz.	Randziffer
S.	Seite
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SA	System Attendant
SACL	System Access Control List
SAGA	Standards und Architekturen für E-Government-Anwendungen
SAM	Security Accounts Manager
SAN	Storage Area Network
SASL	Simple Authentication and Security Layer
SC	Samsung Contact
SCM	Security Configuration Manager
SCS	Sun Control Station
SCSI	Small Computer System Interface
SFU	Service for UNIX

SID	Security Identifier
SISL	Sun Industry Source License
SLAs	Service Level Agreements
SLOX	Suse Linux Openexchange
SMB	Server Message Block
SMS	Short Message Service
SMS	System Management Server
SMTP	Simple Mail Transfer Protocol
SNA	Storage Network Attached
SNMP	Simple Network Management Protocol
SO	StarOffice
SOAP	Simple Object Access Protocol
SPM	Standard TCP/IP Port Monitor
SPX	Sequenced Packet Exchange
SQL	Structured Query Language
SQL-DMO	SQL Distributed Management Objects
SRS	Standard Replication Service
SSH	Secure Shell
SSL	Secure Sockets Layer
SSL/TLS	Secure Sockets Layer / Transport Layer Security
SUS	Java System Update Service
SVG	Scalable Vector Graphic
SW	Software
SWA	Scalix Web Access
SWAP	Simple Workgroup Access Protocol
TB	Terabyte
TCL	Tool Command Language
TCO	Total Costs of Ownership
TCP/IP	Transmission Control Protocol / Internet Protocol
TDS	Tabular Data Stream
TGS	Ticket Granting Service
TGT	Ticket Granting Ticket

TTS	Trouble Ticket System
UDDI	Universal Description, Discovery and Integration
UDP	User Datagram Protocol
UHD	User Help Desks
UNC	Uniform Naming Convention
UNO	Universal Network Objects
UrhG	Urheberrechtsgesetz
URL	Uniform Resource Locator
USB	Universal Serial Bus
USN	Unique Sequence Number
VBA	Visual Basic for Applications
VBS	Visual Basic Scripting Edition
VBScript	Visual Basic Script
VFS	Virtual File System
Vgl.	Vergleiche
VLDB	Very Large Database
VOL	Verdingungsordnung für Leistungen
VOL/A	Verdingungsordnung für Leistungen/ Teil A Allgemeine Bestimmungen für die Vergabe von Leistungen
VPN	Virtual Private Network
W2K	Windows 2000
W3C	World Wide Web Consortiums
WAP	Wireless Application Protocol
WBEM	Web Based Enterprise Management
WebDAVS	Web Document Authoring And Versioning
WINS	Windows Internet Name Service
WSDL	Web-Services Description Language
WSH	Windows Sripting Host
WWW	World Wide Web
XFS	Extended File System
XHTML	eXtensible HyperText Markup Language
XML	Extensible Markup Language

XSL	Extensible Style Sheet Language
XSLT	Extensible Stylesheet Language for Transformations
YaST	Yet another Setup Tool
z.B.	zum Beispiel

10 Glossar

ADO — ADO steht für Active Data Objects und ist eine High-Level Schnittstelle (z.B. aus Visual Basic) für den allgemeinen Datenzugriff von Microsoft über einen OLE DB Provider (z.B. für SQL Server, ODBC, Oracle, Active Directory Service, u.a.). ADO enthält Objekte für das Erstellen einer Verbindung zu einer Datenquelle, für Lese-, Update-, Schreib- und Löschoperationen.

ACL — Eine Access Control List ist eine Liste mit Zugriffsrechten. Anhand dieser Listen erfolgt die Zugriffsteuerung auf die Ressourcen des IT-Systems. Anhand der ACLs entscheidet das System, welchen Zugriff ein Benutzer auf eine Ressource, z.B. ein Verzeichnis, hat.

ActiveX — Sammelbegriff für eine von Microsoft eingeführte Technologie, die (inter)aktive Inhalte auf Webseiten ermöglicht. Der Browser lädt ActiveX-Programmteile vom Server herunter und führt sie auf dem PC des Benutzers aus. ActiveX wurde von Microsoft als Alternative zu Java-Applets entwickelt.

API — Application Programming Interface (Definierte Programmierschnittstelle, die für die Integration und Erweiterung genutzt werden kann)

ASP — Steht für "Active Server Pages"; ist das Microsoft-Konzept für die serverseitige Generierung (z.B. mit JavaScript, Visual Basic Script) dynamischer Web-Seiten (s.a. JSP).

C# — Von Microsoft auf Basis von C und C++ entwickelte objektorientierte Programmiersprache.

CGI — Das Common Gateway Interface ist die Urvariante der Web-Server-Schnittstellen. Praktisch jeder aktuelle Web-Server unterstützt dieses Interface. Anwendungen, die über CGI arbeiten, können mit verschiedenen Programmiersprachen entwickelt werden. Neben Interpretiersprachen wie beispielsweise PERL können auch kompilierte Anwendungen, die in C oder C++ geschrieben sind, verwendet werden.

COM — Das Component Object Model ist ein Software-Standard von Microsoft, mit dessen Hilfe die Kommunikation zwischen Prozessen und Programmen realisiert werden kann. COM definiert dazu eine objektorientierte Schnittstelle, mit der ein Programm oder eine Software-Komponente Dienste zur Verfügung stellt.

CORBA — CORBA steht für Common Object Request Broker Architecture und wurde mit dem Ziel geschaffen, eine orts-, plattform- und implementationsunabhängige Kommunikation zwischen Applikati-

onen zu ermöglichen. CORBA ist ein offener Standard, der durch die Object Management Group (OMG) definiert wird.

DCOM — Das Distributed Component Object Model ist eine Variante des Microsoft-Standards COM. Über das Netzwerk können mit DCOM Dienste einer Software verteilt zur Verfügung gestellt werden. DCOM verwendet zur Realisierung RPC (Remote Procedure Calls), um mittels Nachrichtenaustausch Funktionen auf einem anderen Computer aufzurufen.

DDE — Dynamic Data Exchange ist eine Technik unter Windows, welche es Anwenderprogrammen ermöglicht, Daten miteinander auszutauschen. Der Datenaustausch selbst erfolgt dabei dynamisch. Wird eine der mittels DDE verbundenen Dateien geändert, erfolgt die Übernahme der Änderung in alle mit der betreffenden Datei kommunizierenden Dateien automatisch.

DHCP — Das Dynamic Host Configuration Protocol schafft die Grundlage zur dynamischen Vergabe von IP-Adressen. Der DHCP-Client erhält von zentralen DHCP-Servern dynamisch eine IP-Adresse. Neben den IP-Adressen können dem Client noch weitere Konfigurationsparameter übergeben werden.

DNS — Das Domain Name System ist ein hierarchisch aufgebautes System für die Vergabe von Namen für an das Internet/Intranet angeschlossene Rechner.

DTD — Dokument-Typ-Definitionen definieren formal die Struktur eines XML-Dokuments. Sie geben die Syntax vor, die für einen bestimmten Dokument-Typ (und somit auch für ein bestimmtes Datenformat) gelten sollen.

Emulation — Fähigkeit eines Systems beziehungsweise eines Programms, die Arbeitsweise eines anderen Computersystems mit Hardware- oder Softwaremitteln nachzuahmen.

Failover — Ist die spezifische Betriebsweise von Hard- oder Software, z. B. einer Datenbank, eines Servers oder eines Netzwerks, die so konfiguriert sind, dass ihre Dienste bei einem vorübergehenden Systemausfall automatisch von einem System mit ähnlicher oder gleicher Funktionsweise übernommen werden.

HTML — Hypertext Markup Language – der offene Standard bzw. das Dateiformat für die Darstellung von Inhalten im Internet bzw. Intranet.

HTTP — Standard für die elektronische Interaktion bei der Übertragung von Web-Dokumenten ins Internet.

IMAP — Mit dem Internet Mail Access Protocol lassen sich E-Mail-Postfächer verwalten. Im Gegensatz zu POP3 verwaltet IMAP die Mail auf dem Server. Beim Start des Mail-Programms werden

standardmäßig nur die Kopfdaten (Absender, Betreff und Eingangszeit) geladen. Jetzt können Mails vom Adressaten gezielt ausgewählt und komplett heruntergeladen werden. Eine Mail, die auf dem Server verbleiben soll, kann dort in besonderen Ordnern abgelegt werden.

IPsec — Ein Standard für Netzwerksicherheitslösungen, der sich vor allem für die Implementierung von VPNs sowie den Fernzugriff auf private Netzwerke über Wählverbindungen eignet.

IPv6 — Ist die neue Version 6 des Internet-Protokolls (IP), bei der die IP-Adressen aus 128 statt 32 Bit wie beim IPv4 bestehen sollen. U. a. werden dadurch mehr Adressierungsmöglichkeiten für Websites geschaffen.

IPX — Ein von der Firma Novell definierter Standard für die Datenübertragung.

Java — Von SUN Microsystems entwickelte objektorientierte Programmiersprache, die vor allem im Bereich der Internettechnologie genutzt wird. Aus den Quelltexten wird durch einen so genannten Compiler ein plattformunabhängiger Zwischencode übersetzt. Dieser kann von einem geeigneten Interpreter auf beliebigen Rechnern ausgeführt werden. Dadurch können Java-Programme auf allen Rechnerplattformen laufen, für die ein passendes Interpreter-Programm existiert.

Java Beans — Java Beans sind wieder verwendbare Softwarekomponenten, die in Java realisiert wurden.

Java Script — Eine ursprünglich von der Firma Netscape definierte Skriptsprache zur Verknüpfung von Programmcode mit statischen HTML-Seiten. In der Regel erfolgt die Ausführung des Codes im Browser des Benutzers.

JDBC — Die Java Database Connectivity bietet einen Mechanismus zur Kommunikation mit bestehenden Datenbanken. Dabei bilden Treiber die Schnittstelle zwischen dem Java-Programm und der Datenbank.

JSP — JavaServer-Pages sind HTML-Dateien mit eingebettetem Java-Programmcode, die mit Hilfe einer JSP-Engine einmalig in Servlets umgewandelt und anschließend im Webserver ausgeführt werden. Das Ergebnis wird dann im normalen HTML-Format an den Client gesendet (s. a. ASP).

LAMP — Eine auf Linux, Apache, MySQL und PHP bzw. PERL oder Python basierende Open Source Plattform für Web-Entwickler und Webanwendungen.

LDAP — Das Lightweight Directory Access Protocol (X.509) ist eine vereinfachte Version des DAP (X.500). Mit LDAP werden Zugriffe auf Verzeichnisdienste realisiert, mit denen z. B. Benutzermerkmale abgefragt werden können.

Makro — Eine Kombination einzelner Anweisungen bzw. eine Folge von Befehlen und Vorgängen, die festgehalten und gespeichert werden kann. Wird ein Makro aufgerufen, werden die Vorgänge und Aktionen in der entsprechenden Reihenfolge automatisch wieder abgearbeitet.

MP3 — Standardformat für komprimierte Audiodateien, das im Rahmen der MPEG vom Fraunhofer-Institut entwickelt wurde und sich vor allem im Internet verbreitet hat.

MTA — Softwarekomponente, die für die Verteilung von E-Mails zwischen verschiedenen Computersystemen zuständig ist. Ein MTA nimmt Nachrichten sowohl von anderen MTAs als auch von MUAs entgegen und leitet diese an die entsprechenden Empfänger weiter.

MUA — Der Mail User Agent ist das E-Mail-Programm, das es dem Benutzer ermöglicht, auf elektronische Nachrichten zuzugreifen, sie anzuzeigen, zu lesen, zu bearbeiten und zu verwalten.

.NET — Plattform für XML basierte Web Services von Microsoft. Die Plattform soll die Informationen, Geräte und Anwender in einer einheitlichen und personalisierten Weise miteinander verbinden.

NTP — Das Network Time Protocol dient dazu die Uhrzeiten verschiedener Computer über ein Netzwerk zu synchronisieren. Das NTP ermöglicht eine millisekundengenaue Einstellung der Rechnerzeiten; ist insbesondere sehr wichtig für Vorgänge, an denen gleichzeitig mehrere Rechner beteiligt sind.

ODBC — Standardisiertes Verfahren, das den Zugriff auf Datenbanken gewährleistet. Beispielsweise können Anwendungsprogramme auf Datenbanken unterschiedlichsten Art mittels ODBC zugreifen.

OLE — OLE steht für "Objekt Linking and Embedding" und ist eine Methode zur gemeinsamen Nutzung von Informationen. Dabei können die Informationen in unterschiedlichen Formaten vorliegen und mit unterschiedlichen Anwendungen erstellt worden sein. Es werden Daten aus einem Quelldokument mit einem Zieldokument verknüpft bzw. in dieses eingebettet. Wenn die eingebetteten Daten im Zieldokument markiert werden, wird wieder die Quell-Anwendung geöffnet, damit die Daten in gewohnter Umgebung mit den notwendigen Funktionen bearbeitet werden können. Man spricht auch von "OLE Compound Documents".

OSI — Internationaler Standard für den Datenaustausch in Netzwerken. OSI wird in sieben Schichten dargestellt, die jeweils die einzelnen Kommunikationsprozesse beschreiben.

PDF — Plattformübergreifendes Dokumentenformat der Firma Adobe Systems, mit welchem sich aus Texten, Bildern und Grafiken bestehende Dokumente erzeugen und darstellen lassen.

Perl — Die Practical Extraction and Report Language ist eine frei verfügbare Programmiersprache, die besonders häufig zum Schreiben von CGI-Skripten verwendet wird. Durch die vielfältigen Möglichkeiten, insbesondere auch in der Verarbeitung von Strings, werden Perl-Programme auch häufig für administrative Routineaufgaben verwendet.

PHP — Serverseitige Skriptsprache zur Erstellung datenbankgestützter und dynamischer Webinhalte.

POP3 — Beim Arbeiten mit Post Office Protocol in der Version 3 lädt das lokale Mail-Programm (Client) grundsätzlich nach dem Start alle neue Post vom Mail-Server auf den lokalen Computer. Normalerweise ist der Client so konfiguriert, dass die Mail nach dem Download auf dem Server gelöscht wird.

POSIX — Auf UNIX basierender Schnittstellen-Standard gemäß IEEE, der von allen UNIX-Derivaten unterstützt wird.

PostScript — Von der Firma Adobe entwickelte Seitenbeschreibungssprache für die Steuerung von Druckern. postscriptfähige Drucker erhalten ihre Druckbefehle von dem jeweiligen Anwendungsprogramm in Form einer standardisierten Anweisungsfolge; diese interpretiert der entsprechende Drucker und setzt sie in einen Druckvorgang um.

RAS — Ist die Microsoft-Bezeichnung für Bereitstellung von Dial-Up-Diensten innerhalb des Microsoft-Betriebssystems.

RDBMS — In einem relationalen Datenbank-Managementsystem liegen die Informationen der Datenbank in Tabellen vor, die zueinander in Relation stehen. Organisiert nach dem relationalen Modell.

Server — Ein Prozess, ein Programm oder ein Computer zur Bearbeitung der Anforderungen eines Clients bzw. zur Bereitstellung von Diensten, die von einem Client genutzt werden können.

SQL — Stellt die Standard-Abfragesprache für relationale Datenbanken dar.

SSH — Ein Protokoll bzw. eine entsprechende Implementierung (Unix/Linux-Systemen) dieses Protokolls, das den sicheren Zugriff auf an ein Netzwerk angeschlossene Rechner gewährleistet. Die

Implementierung bietet eine gesicherte Datenübertragung auf ungesicherten Verbindungen an.

SSL — Eine von der Firma Netscape entwickelte Verschlüsselungstechnologie und ein Protokoll für die sichere Kommunikation bzw. Dokumentenübermittlung zwischen Webbrowsern und Webservern.

TCP/IP — Ein Satz von Netzwerkprotokollen, die innerhalb eines Netzwerkes verwendet werden, um dem Benutzer eine Reihe von Diensten zur Verfügung zu stellen. TCP (Transmission Control Protocol) und IP (Internet Protocol) bieten die Grundlagen über die Formulierung der einzelnen Datenpakete, deren Versendung und Zustellung.

UNO — UNO ist ein Komponentenmodell, welches Interoperabilität zwischen unterschiedlichen Programmiersprachen, unterschiedlichen Objektmodellen, unterschiedlicher Maschinenarchitekturen und unterschiedlichen Prozessen schafft. Diese kann in einem LAN oder über das Internet hergestellt werden. UNO wird von der OpenOffice Community zusammen mit den Entwicklungslabors von Sun Microsystems entwickelt. Die Basis-Bibliotheken von UNO sind unabhängig von OpenOffice und StarOffice und können als Framework für andere Anwendungen eingesetzt werden. UNO ist frei verfügbar und steht unter der LGPL-Lizenz. Derzeit werden Java, C und C++ auf Windows, Linux und Solaris unterstützt. (siehe auch http://udk.openoffice.org/common-/man/uno.html)

URL — Der Uniform Resource Locator beschreibt eine eindeutige Adresse im World Wide Web, z. B. "http://www.csar-ag.com".

VBA — Visual Basic for Applications

W3C — Das World Wide Web Consortium koordiniert die Entwicklung des WWW und die Standardisierung von HTML, XML und deren Derivate.

WebDAV — Das Web-based Distributed Authoring and Versioning ist eine Erweiterung des Hypertext Transfer Protocol (HTTP) und bietet eine standardisierte Unterstützung für asynchrones, kollaboratives Erstellen von Inhalten über das Internet bzw. Intranet.

WINS — Mircosoft-System zur Namensauflösung innerhalb eines Netzwerkes (Netzwerknamen <-> IP-Adressen).

XML — Eine Spezifikation für die Definition von Sprachen zur Formatierung von Dokumenten. XML bietet eine strenge Trennung von Inhalten und Design.

XSLT — Vom W3C empfohlene Sprache zur Erstellung von Stilvorlagen, die XML-Strukturen regelbasiert in andere XML-Strukturen umwandeln, z. B. in eine Seitenbeschreibungssprache wie HTML.

11 Tabellenverzeichnis

Tab. 1: Suse Linux ... 34
Tab. 2: Red Hat ... 35
Tab. 3: Sun Java Desktop ... 36
Tab. 4: Red Hat Desktop ... 38
Tab. 5: Managementkomponenten ... 40
Tab. 6: Systemmanagementfunktionalitäten des Red Hat Networks ... 41
Tab. 7: Novell Linux Desktop ... 42
Tab. 8: Systemmanagementfunktionalitäten des ZENworks Linux Managements ... 43
Tab. 9: Eigenschaften der Windows Sammelberechtigungen ... 56
Tab. 10: Windows Attribute ... 57
Tab. 11: Vergleich der Dateiserver ... 63
Tab. 12: Vergleich der Dateisysteme ... 67
Tab. 13: POSIX-Berechtigungen und Windows-Aggregationen ... 70
Tab. 14: POSIX- und Windowsberechtigungen ... 71
Tab. 15: Gruppentypen ... 75
Tab. 16: Client-Anbindung an CUPS ... 93
Tab. 17: Eindeutige Kennzeichnungen NetBIOS-Namen ... 113
Tab. 18: Mehrwertige Kennzeichnungen NetBIOS-Namen ... 114
Tab. 19: Übersicht der unterstützten DNS Resource Record Typen ... 115
Tab. 20: DHCP-Optionen ... 116
Tab. 21 Vergleich Verzeichnisdienste ... 156
Tab. 22: Gegenüberstellung J2EE und .NET ... 196
Tab. 23: Apache-Module ... 202
Tab. 24: Erweiterte Funktionalitäten der Internet Information Server 5.0 ... 208
Tab. 25: Als Objekte vorhandene Komponenten im MS SQL-Server ... 213
Tab. 26: unter Open Source Lizenz verfügbare Datenbanksysteme ... 218
Tab. 27: Zusammenstellung SQL Datenbanksysteme ... 223
Tab. 28: Erweiterte Internet- und Intranetlösungen MS SQL Server 2000 ... 224
Tab. 29: Verwaltungs- und Entwicklungsfunktionalitäten ... 225

Tab. 30: Basiskomponenten Exchange 5.5 228
Tab. 31: Auswahl an phpGroupware-Modulen 233
Tab. 32: Zentrale Kolab-Server-Komponenten 234
Tab. 33: Optionale Kolab Server-Komponenten 235
Tab. 34: exchange4linux Komponenten 243
Tab 35: Mögliche Komponenten der Open-Xchange-Lösung 247
Tab. 36: Samsung Contact Komponenten 254
Tab. 37: Alternative Groupware-Lösungen 259
Tab. 38: Kompatibilitätsmatrix – Exchange 265
Tab. 39: Outlook Web Access 267
Tab. 40: VBA-Versionen 281
Tab.: 41: Problematische MS Office Eigenschaften hinsichtlich der Konvertierung nach OOo/SO 291
Tab. 42: Gegenüberstellung der verfügbaren Vorlagen- und Format-Typen 292
Tab. 43: Unterschiede in den Schlüsselfunktionalitäten 292
Tab. 44: OSS Webbrowser Übersicht 336
Tab. 45: Vorteile von Terminal-Servern und Thin Clients 353
Tab. 46: Ausgewählte Nachteile von Terminal-Servern und Thin Clients 354
Tab. 47: Anforderungen an ein HA-System 363
Tab. 48: Zusammenstellung Abstraktionsebenen 364
Tab. 49: Übersicht 367
Tab. 50: Vertragsverhältnisse Nutzer-Zwischenhändler 376
Tab. 51: Anwendbares Recht 378
Tab. 52: Urheberrechtliche Fragen 385
Tab. 53: Vertragliche Ansprüche auf Haftung und Gewährleistung gegen den Zwischenhändler 391
Tab. 54: Beispiele für Annahmen einer Wirtschaftlichkeitsbetrachtung 406
Tab. 55: Prozentuelle Anteile der Personalaufwendungen in den Migrationsphasen 409
Tab. 56: Prozentueller Gesamtpersonalaufwand 410
Tab. 57: Erhebungsstruktur Preisinformationen Hard-/ Software "Server" 411

Tab. 58: Erhebungsstruktur Preisinformationen Hard-/ Software "Arbeitsplatzcomputer" ... 412

Tab. 59: Portierungsgruppen ... 416

Tab. 60: Klassifizierung von Dokumentvorlagen und Makros ... 421

Tab. 61: Informationscluster für die Erhebung der IT-Fachverfahren ... 422

Tab. 62: Vergleichende Übersicht thematischer Eigenschaften von WiBe 4.0 und MiKoMa 2.0 ... 440

Tab. 63: Vorschlag Zusammenstellung Projekt-Organisationsformen ... 489

Tab. 64: Überleitungstabelle Kriterien WiBe 4.0 zu Kostenartengruppen MiKoMa 2.0, " Entwicklungskosten/ Einführungskosten und Entwicklungsnutzen" ... 495

Tab. 65: Überleitungstabelle Kriterien WiBe 4.0 zu Kostenartengruppen MiKoMa 2.0, " Betriebskosten und Betriebsnutzen" ... 496

Tab. 66: Matrix zur Soft- und Hardware-Kostenermittlung ... 497

Tab. 67: Ausschnitt Summenübersicht für Projekte eines Beipiel-Migrationsvorhabens ... 498

Tab. 68: Ausschnitt Projektübersicht für Beipiel-Migrationsvorhaben ... 499

Tab. 69: Ausschnitt Projektbeispiel "Software" für Beipiel-Migrationsvorhaben ... 500

Tab. 70: Ausschnitt Projektbeispiel "Customizing" für Beipiel-Migrationsvorhaben ... 500

12 Abbildungsverzeichnis

Bild 1: Systemlandschaft – Ausgangssituation 23
Bild 2: Systemlandschaft – Ablösende Migration 26
Bild 3: Systemlandschaft – Fortführende Migration 27
Bild 4: Red Hat Network 39
Bild 5: B-G-L-R Methode 59
Bild 6: B-G-R Methode 59
Bild 7: Druckumgebung 82
Bild 8: Prozessabfolge bei der „Point & Print“-Methode 86
Bild 9: Drucken unter CUPS 92
Bild 10: Anmeldeszenario 106
Bild 11: Beispiel NT-Domänenstruktur 142
Bild 12: Beispiel Windows 2000 142
Bild 13: Beispiel Standort- und Domänenstruktur 144
Bild 14: Ausgangssituation 145
Bild 15: Stammdomäne: W2K.BEHOERDE.DE 146
Bild 16: Stammdomäne: BEHOERDE.DE 147
Bild 17: Stammdomäne: NEU.DE 147
Bild 18: Stamm- und Strukturdomäne: NEU.DE/ INTRA.NEU.DE 149
Bild 19: Stammdomäne: INTRA.BEHOERDE-ONLINE.DE 150
Bild 20: Stammdomäne: AMT.LOCAL 151
Bild 21: Migration durch Upgrade oder Restrukturierung 160
Bild 22: Migration ADS – Aktualisierung plus Restrukturierung 161
Bild 23: Migration ADS – Neue Domäne plus Restrukturierung 161
Bild 24: Migration ADS – Klonen von Benutzern und Gruppen 162
Bild 25: Migration ADS – Parallelwelt und Migration der Ressourcen 163
Bild 26: Migration ADS – Füllen der parallelen Welt mit Benutzerkonten und Gruppen 163
Bild 27: Behälter-orientierte Struktur-Interpretation 168
Bild 28: Hierarchische Strukturinterpretation 169
Bild 29: Eingabeunterstützung und Konsistenzprüfung anhand des Schemas: typischer XML-Editor 171

Bild 30: Komponenten des .NET-Frameworks 190
Bild 31: Microsoft .NET Framework 192
Bild 32: Schichtenmodell J2EE 194
Bild 33: Serverarchitektur des MS SQL Servers 212
Bild 34: OpenGroupware-Architektur 239
Bild 35: Scalix-Plattform 250
Bild 36: Scalix-Clientsysteme 251
Bild 37: Scalix- Integration 252
Bild 38: Architektur Samsung Contact 254
Bild 39: Gemischte Umgebungen – Exchange 266
Bild 40: VBA in der Office Anwendung 282
Bild 41: Erweiterungsmöglichkeiten von Office 283
Bild 42: Fontmapping MS Office OOo/SO 285
Bild 43: Konfiguration der "XML Filter" (XSLT-Filter) in OOo 1.9.69 (Beta) 289
Bild 44: "XML Filter" präsentieren sich dem Anwender als weiterer Dateityp. 290
Bild 45: Schatten-Objekte PowerPoint und Impress 298
Bild 46: Dokumentenkonverter: Auswahl des Quellformats 299
Bild 47: Dokumentenkonverter: Auswahl des Quell- und Zielverzeichnisses 299
Bild 48: Architektur des Dokumentgenerators 303
Bild 49: Typische Architektur einer Visual Studio Tools für Office Lösung 307
Bild 50: Verwendung benutzerdefinierter Schemata in Word 2003 311
Bild 51: Schema-Verwaltung von Word 2003: nicht immer selbsterklärend 312
Bild 52: Einbindung von Transformations-Stylesheets in Word 2003 beim Laden (oben) und Speichern (unten) 312
Bild 53: Nicht unterstützte Schema-Konstrukte in Excel 313
Bild 54: Verwendung benutzerdefinierter Schemata in Excel 2003 314
Bild 55: Ausschnitt der Web-Site von Microsoft zur Unterstützung im Umgang mit IRM-geschützten Dokumenten 317
Bild 56: KDE-Desktop – Beispiel 1 332
Bild 57: KDE-Desktop – Beispiel 2 333

Abbildungsverzeichnis

Bild 58: Beispiel - GNOME-Desktop 334

Bild 59: Windows-Desktop unter Linux mittels VMware 342

Bild 60: Windows-Desktop auf Linux mittels Win4Lin 345

Bild 61: Windows-Anwendungen auf dem Linux-Desktop mittels WINE 348

Bild 62: Ausführen von X-Anwendungen auf einem Fat Client 355

Bild 63: Ausführen von X- und Windows-Anwendungen auf einem Thin Client 356

Bild 64: Booten eines Linux-Systems übers Netzwerk 356

Bild 65: Serverfarm unter Metaframe XP 361

Bild 66: HA-Lösungen 366

Bild 67: Lösung mit Heartbeat und DRBD 369

Bild 68: Vertragsverhältnisse 373

Bild 69: Regelkreis der Wirtschaftlichkeitsbetrachtung 405

Bild 70: Migrationsphasen 409

Bild 71: Bandbreite des Personaltagebedarfs in Prozent der Nutzer 411

Bild 72: Beispiel Erhebungsbogen "Infrastruktur der Server" 417

Bild 73: Beispiel Erhebungsbogen "Infrastruktur der Arbeitsplatz-Computer" 418

Bild 74: Beispiel Erhebungsbogen "Infrastruktur des Netzwerks" 419

Bild 75: Beispiel Erhebungsbogen "Drucker-Infrastruktur" 419

Bild 76: Beispiel Erhebungsbogen "Erhebungsbogen für Serverinfrastrukturdienste" 420

Bild 77: Beispiel Erhebungsbogen "Standardsoftware" 421

Bild 78: Beispiel Erhebungsbogen "Office" 422

Bild 79: Beispiel Erhebungsbogen "IT-Fachverfahren – Architektur und Nutzer" 423

Bild 80: Beispiel Erhebungsbogen "IT-Fachverfahren – Client-/ Serverbetriebssysteme, Datenbanksysteme und Applikationsserver" 424

Bild 81: Beispiel Erhebungsbogen "IT-Fachverfahren – Benutzer-/ Rechteverwaltung und Schnittstellen" 424

Bild 82: Beispiel Erhebungsbogen "IT-Fachverfahren – Hosting, Verfahrensentwicklung und Ausprägung" 425

Bild 83: Beispiel Erhebungsbogen "IT-Fachverfahren – Ausblick, Kosten und Anmerkungen" 425

Bild 84: Methodik WiBe 4.0 ... 427
Bild 85: WiBe - Beispielhafte WiBe Kalkulation 1, Einführungskosten/ -nutzen ... 436
Bild 86: WiBe - Beispielhafte WiBe Kalkulation 2, Betriebskosten/ -nutzen ... 437
Bild 87: WiBe – Entwicklung externer Kosten (haushaltswirksam) ... 438
Bild 88: WiBe - Break even Übersicht ... 438
Bild 89: Modell der Wirtschaftlichkeitsbetrachtung nach MiKoMa ... 442
Bild 90: MiKoMa - Beispielhafte Übersicht dreier Alternativen ... 449
Bild 91: MiKoMa - Kosten Externer Anbieter ... 450
Bild 92: MiKoMa - Vergleich der nominalen Projektnutzen ... 450
Bild 93: MiKoMa - Rentabilitätsvergleich ... 451
Bild 94: MiKoMa - Break even Übersicht ... 451
Bild 95: Entscheidungsprozess zur Einführung von OSS ... 455
Bild 96: Systemarchitektur mit einem linuxbasierten Fat Client ... 459
Bild 97: Empfohlene IT-Architektur einer großen Behörde bei vollständiger „Ablösender Migration“ ... 463
Bild 98: Anwendungsfelder der Directory-Services am Beispiel der SunOne Plattform ... 464
Bild 99: Empfohlene IT-Architektur einer spezialisierten Behörde bei vollständiger „Ablösender Migration“ ... 466
Bild 100: Empfohlene IT-Architektur einer kleinen Behörde bei vollständiger „Ablösender Migration“ ... 468
Bild 101: Ausgangssituation für eine Fortführende Migration ... 470
Bild 102: Unterschiedliche Varianten einer Exchange-Ablösung bei Teilmigration ... 475
Bild 103: Sanfte Migration ... 480
Bild 104: Phasen der Umstellung bei einer sanften Migration ... 481
Bild 105: Modell: stufenförmiger Migrationsprozess ... 482
Bild 106: Stufen der Qualitätskontrolle ... 493