



# **Open Source Software (OSS)**

in der Landesverwaltung Baden–Württemberg

## **Studie der SuSE Linux Solutions AG**

im Auftrag  
des

Innenministeriums Baden–Württemberg  
Stabsstelle für Verwaltungsreform

**Erste Fassung  
28.08.2000**

Autoren:

Achim Frank (Achim.Frank@suse.de)  
SuSE Linux Solutions AG

Andreas Nemeth (Andreas.Nemeth@suse.de)  
SuSE Linux Solutions AG

Gerhard Strauß (gerhard.strauss@im.bwl.de)  
Innenministerium Baden-Württemberg

Diese Studie wurde mit StarOffice Version 5.1 erstellt.

## Inhaltsverzeichnis

<b>1. Auftrag und Zielsetzung</b> .....	<b>4</b>
<b>2. Grundlagen</b> .....	<b>6</b>
2.1. Inhalte, Grundsätze und Ziele der Open Source Bewegung.....	6
2.2. Organisation.....	8
2.3. Hard- und Software .....	8
2.4. Entwicklung, Standardisierung.....	9
2.5. Rechtliche Einordnung, insbesondere Urheberrecht, Gewährleistung.....	9
2.6. Unternehmen, SuSE und andere Distributoren.....	10
2.7. Weitere Entwicklung, Ausblick.....	11
2.8. Service, Support.....	12
<b>3. Linux, die Alternative</b> .....	<b>13</b>
3.1. Unterschiede zu eingeführten Systemen.....	13
3.2. Hardware.....	15
3.3. Software.....	15
3.4. Installation.....	16
3.5. System- und Benutzerverwaltung.....	16
3.6. Linux als Server-Plattform.....	16
3.7. Linux als Client-Plattform.....	19
3.8. Router.....	20
3.9. Koexistenz mit eingeführten Systemen.....	20
3.10. Interoperabilität.....	20
3.11. Vorteile.....	21
3.12. Einschränkungen.....	23
3.13. Absehbare Entwicklungen.....	23
<b>4. Sicherheit</b> .....	<b>25</b>
4.1. Unterschiede zu eingeführten Systemen.....	25
4.2. Computerviren.....	25
4.3. Überwachung der Systemintegrität.....	25
4.4. Entdeckung von Angriffen.....	26
4.5. Verschlüsselung.....	26
<b>5. Wirtschaftlichkeit</b> .....	<b>27</b>
<b>6. OSS-Einsatz in der Landesverwaltung Baden-Württemberg</b> .....	<b>28</b>
6.1. Stand.....	28
6.2. Weitere Einsatzmöglichkeiten, Szenarien.....	30
6.3. Verschlüsselung: Mail-V., Platten-V. und Digitale Signaturen.....	40
6.4. Web- und Intranet-Server.....	43
<b>7. Empfehlungen</b> .....	<b>46</b>
<b>8. Index</b> .....	<b>47</b>
<b>9. Anlagen</b> .....	<b>49</b>
9.1. Anlage I: Historische Meilensteine der Open Source Bewegung.....	49
9.2. Anlage II: OSS-Installationen in der Landesverwaltung Baden-Württemberg.....	51
9.3. Anlage III: Standards des Landessystemkonzepts Baden-Württemberg .....	53
9.4. Anlage IV: Quellenverzeichnis.....	57

## 1. Auftrag und Zielsetzung

Open Source Software findet insbesondere durch das freie Betriebssystem Linux zunehmendes Interesse in Wirtschaft und Verwaltung. Alle namhaften Hersteller bieten inzwischen ihre Software auf der Basis von Linux an oder haben dies angekündigt. Für einzelne Anwendungsbereiche sind Software-Pakete vorhanden, die an die Funktionsvielfalt und Leistungsfähigkeit bekannter, lizenzierter und entgeltlicher Software heranreichen oder diese gar übertreffen. Einen aktuellen Überblick vermittelte die Ende Juni / Anfang Juli 2000 erstmals in Stuttgart stattfindende Linux-Messe (Linux-Tag e.V.).

Auch die öffentliche Verwaltung beschäftigt sich in der letzten Zeit verstärkt mit Open Source Software. Insbesondere die Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik<sup>1</sup> hat durch ihre Empfehlung zu Gunsten des Open Source Software-Einsatzes für Schlagzeilen gesorgt. Das BMWi fördert ebenfalls Open Source Software. Im Juni dieses Jahres führte die Bundesverwaltung eine Auftaktveranstaltung durch, die der Vorbereitung von dreitägigen Open Source Software-Workshops im September 2000 diente. Dabei wurde auch über erste Linux-Installationen in der Bundesverwaltung berichtet. Ziel der Workshops soll es u.a. sein, Migrationskonzepte und ein Fortbildungskonzept für Open Source Software in der Bundesverwaltung erarbeiten zu können. Auch die EU hat die Förderung von Open Source Software bei Ausschreibungen empfohlen und eine Arbeitsgruppe eingerichtet.<sup>2</sup> In den anderen Bundesländern werden Überlegungen zum Einsatz von OSS angestellt.

Open Source Software führt weit über Linux hinaus. Eine nicht überschaubare Anzahl von Programmen ist inzwischen vorhanden. Die bekanntesten sind Apache im Webbereich, Samba als Workgroup-Server sowie KDE und GNOME als grafische Client-Oberfläche

Wichtigster Aspekt für den Einsatz von Linux ist, dass es frei erhältlich ist, ebenso wie ein Großteil der Anwendungssoftware, die es für Linux gibt. Laut Erhebungen von IDC ist Linux ein System mit hoher Verfügbarkeit und das am stärksten wachsende Betriebssystem im Serverbereich.

Angesichts dieser Entwicklung beauftragte die Stabsstelle für Verwaltungsreform beim Innenministerium Baden-Württemberg die SuSE Linux Solutions AG mit der

- Unterstützung bei der Einrichtung eines Testsystems auf der Basis von Linux/Staroffice
- Erstellung der vorliegenden Studie über die Möglichkeiten des Einsatzes von Open Source Software in der Landesverwaltung Baden-Württemberg.

Mit dem Aufbau des Testsystems und dieser Studie verfolgt die Stabsstelle folgende Ziele:

- Sammlung von Erfahrungen, Beobachtung der weiteren technischen Entwicklung und der Entwicklung von Open Source Software am Markt, insbesondere auch im Bürokommunikationsbereich (Office), bei Servern und im Bereich der Netzwerksicherheit,

---

<sup>1</sup> KBSt-Brief Nr. 2/2000, Open Source Software in der Bundesverwaltung, Stand: Februar 2000

<sup>2</sup> <http://linux.kbst.bund.de/>

## OSS IN DER LANDESVERWALTUNG BADEN-WÜRTTEMBERG

- Prüfung, ob es in absehbarer Zeit kostengünstige und ebenso funktionstüchtige Alternativen zu den heute installierten Produkten gibt und
- Prüfung der Qualität und der Wirtschaftlichkeit der heute in der Landesverwaltung eingesetzten kostenpflichtigen Software.

## 2. Grundlagen

### 2.1. Inhalte, Grundsätze und Ziele der Open Source Bewegung

Der Open Source Gedanke geht davon aus, dass die Möglichkeiten, den Quellcode eines Programms zu lesen, zu verändern und neu zu verteilen, zwangsläufig zu einer Verbesserung der Funktion und Qualität des Programms führen. Jeder interessierte Benutzer eines Programms hat dadurch die Möglichkeit, ein Programm an seine Anforderungen anzupassen, es zu verbessern und Fehler zu beheben. Je mehr Benutzer und Ko-Entwickler ein Programm hat, um so effektiver ist dieser Prozess. Dies steht im Gegensatz zu dem traditionellen Entwicklungsmodell, in dem nur eine begrenzte Anzahl von Programmierern Zugang zum Quellcode hat und an der Entwicklung und der Fehlerbehebung arbeiten kann. In seinem Buch »The Cathedral and the Bazaar« [1] prägte Eric S. Raymond für die beiden unterschiedlichen Entwicklungsmodelle die Begriffe »Cathedral« für das geschlossene, konventionelle Entwicklungsmodell und »Bazaar« für das offene Modell.

Die Gartner Group hat sich damit auseinander gesetzt und empfiehlt in einer neueren Studie Unternehmen, die den Einsatz von Open Source Software bisher ausgeschlossen haben, ihre Strategie zu überdenken. Diese Studie mit dem Titel »Debunking Open-Source Myths: Development and Support« [3] enthält die folgenden Kernaussagen:

- Open Source Software Produkte werden stets von einzelnen Personen oder kleinen Entwicklungsgruppen strikt kontrolliert.
- Die Abhängigkeit von einzelnen Entwicklern ist durch die Verfügbarkeit der Programm-Quellen stark verringert.
- Für viele Open Source Projekte gibt es kommerzielle Unterstützung.
- Die Verfügbarkeit der Programm-Quellen verringert das Risiko der Abspaltung, wie sie bei UNIX geschehen ist.

Jeder, der sich mit dem Open Source Modell auseinandersetzt, kommt früher oder später zu dem Punkt, an dem er sich fragt, was die Entwickler von Open Source Software dazu motiviert, qualitativ hochwertige Software zu entwickeln, ohne dafür einen ersichtlichen materiellen Gegenwert zu erhalten. Das fehlende Verständnis für die Hintergründe und Gesetzmäßigkeiten, denen die Open Source Softwareentwicklung folgt, führt zu Misstrauen und Ablehnung. Daher sei an dieser Stelle ein kurzer Hinweis auf den Artikel »Homesteading the Noosphere« [1] und [1a] von Eric S. Raymond erlaubt, der diese Fragen beantwortet, in dem er erläutert, wie das Internet die Bildung einer neuen sozio-ökonomischen Gemeinschaft ermöglicht hat, die aufgrund der nahezu uneingeschränkten Verfügbarkeit von Ressourcen (Rechner, Netzzugänge, Kommunikationsmittel) Mechanismen zur gegenseitigen Belohnung entwickelt hat, die denen gleichen, die Kulturen entwickeln, in denen ein Überfluss an Wirtschaftsgütern herrscht. Eine Diskussion dieser Analyse würde den Rahmen dieser Studie sprengen. Man sollte sich jedoch mit dem Gedanken auseinandersetzen, dass die Open Source Bewegung nicht nur ein temporäres technisches Phänomen ist, sondern eine neue gesellschaftliche und

wirtschaftliche Kraft darstellt, die erst mit der Verbreitung des Internet entstehen konnte und dessen Möglichkeiten optimal nutzen kann.

In der Open Source Definition (OSD) [2] der Open Source Initiative (OSI) wurden die Regeln festgelegt, nach denen sich Softwarelizenzen für Open Source Software (OSS) richten müssen:

1. Freie Weitergabe  
Die Weitergabe oder der Verkauf der Software im Rahmen einer Software Distribution darf nicht eingeschränkt werden. Es dürfen keine Lizenzgebühren für die Software verlangt werden.
2. Verfügbarkeit des Quell Codes  
Das Programm muss zusammen mit dem Sourcecode verteilt werden. Falls der Sourcecode nicht enthalten ist, muss ein Verweis auf eine Möglichkeit zum Erhalt der Quellen vorhanden sein (z. B. eine URL).
3. Veränderbarkeit  
Die Lizenz muss die Modifikation und die Verteilung der modifizierten Software zu den Bedingungen der Originalsoftware ermöglichen.
4. Integrität des original Source Codes  
Eine Lizenz darf die Verbreitung modifizierten Sourcecodes nur einschränken, wenn gleichzeitig die Verteilung zusätzlicher Modifikationen erlaubt ist. Dadurch wird die Integrität des Originals erhalten, und der Autor der Originalsoftware bleibt erkennbar.
5. Keine Diskriminierung von Personen oder Gruppen  
Die Lizenz darf keine Personen oder Gruppen von der Verteilung ausschließen. Damit darf eine Lizenz auch keine nationalen Exportbeschränkungen enthalten – sie darf aber auf die Existenz solcher Beschränkungen hinweisen.
6. Keine Diskriminierung des Einsatzgebietes  
Die Lizenz darf das Einsatzgebiet des Programms nicht einschränken. Somit darf auch die Nutzung im kommerziellen Umfeld nicht verboten werden.
7. Freie Weitergabe der Lizenz  
Die mit dem Programm verbundenen Rechte gelten für jeden, an den das Programm weitergegeben wurde, ohne dass weitere Lizenzen erteilt werden müssen. Diese Klausel verhindert den Abschluss von Non Disclosure Agreements (NDA).
8. Unabhängigkeit der Lizenz vom Produkt  
Die mit dem Programm verbundenen Rechte gelten auch, wenn das Programm losgelöst von einer Distribution weitergegeben wird.
9. Kein Einschluss fremder Software  
Die Lizenz darf keine Einschränkungen für andere Software, die gemeinsam mit dem Programm weitergegeben wird, enthalten. Es darf z. B. nicht verlangt werden, dass das Programm nur zusammen mit Open Source Software weitergegeben wird.

Die Open Source Initiative hat inzwischen eine Zertifizierung ins Leben gerufen, um die Möglichkeit des Nachweises der Konformität von Software zur OSD belegen zu können.

## 2.2. Organisation

Der Open Source Bewegung liegt keine fest definierte Organisationsform zugrunde, die mit etablierten herstellerunabhängigen Organisationen wie z. B. The Open Group vergleichbar wäre. Die Open Source Bewegung wird durch Projektgruppen gebildet, die ihre Softwareprodukte auf der Basis von freier Software entwickeln und unter Open Source Lizenzen veröffentlichen. Die Projektgruppen sind in der Regel entgegen oft geäußerten Vorbehalten straff organisiert [3].

Auch wenn sich die Open Source Bewegung nicht an einer konkreten Organisationsform festmachen lässt, gibt es inzwischen einige Organisationen oder Konsortien, die aus der Open Source Bewegung heraus entstanden sind wie z. B.

- Open Source Initiative(OSI) <http://www.opensource.org>  
Verantwortlich für die Open Source Definition und Zertifizierung von Open Source Software.
- Linux Professional Institute(LPI) <http://www.lpi.org>  
Definitionen von distributionsunabhängigen Prüfungen für die Zertifizierung als Linux Systemadministrator.
- Linux Standard Base (LSB) <http://www.linuxbase.org>  
Das Ziel der LSB ist die Schaffung und Förderung von Standards, die die Kompatibilität von Linux Distributionen so verbessern sollen, dass Anwendungen ohne Anpassungen auf allen LSB kompatiblen Distributionen ablauffähig sind. Zusätzlich koordiniert die LSB Projekte mit dem Ziel, Produkte für Linux zu portieren oder zu entwickeln.
- Free Standards Group (<http://www.freestandards.org/>)  
Die Free Standards Group ist eine nicht kommerzielle Dachorganisation für eine Reihe von Projekten wie z. B. LSB oder die Linux Internationalisation Initiative, die sich der Förderung der Nutzung und Akzeptanz von Open Source Technologien verschrieben hat.

## 2.3. Hard- und Software

Open Source Entwicklungen sind nicht auf eine bestimmte Hardware festgelegt. Linux ist als Beispiel nicht nur für Intel sondern auch für Compaq Alpha, für SUN Sparc und PowerPC Architekturen und mittlerweile auch für IBM S/390 Mainframes verfügbar. IBM arbeitet an einer Portierung für die AS/400.

Der Apache Webserver ist ein Beispiel für eine Open Source Entwicklung, die auf fast allen aktuellen Betriebssystemen verfügbar ist.

## 2.4. Entwicklung, Standardisierung

Ein Effekt der Softwareentwicklung nach dem »Bazaar« Modell ist eine starke Beschleunigung des Entwicklungsprozesses. Dadurch können neue Versionen früher und schneller herausgegeben werden. Ein kritischer Faktor für den Release-Zyklus ist die Geschwindigkeit, mit der Fehler gefunden und beseitigt werden. Im Gegensatz zur klassischen Softwareentwicklung, in der ein Team von Programmierern abgeschlossen an der Entwicklung neuer Produkte arbeitet, und jeder Programmierer aus Gründen der Effizienz spezielle Aufgaben lösen muss, werden in der Open Source Entwicklung die Aufgaben an eine Vielzahl von Ko-Entwicklern delegiert. Für das Testen und die Fehlerbeseitigung stehen in der Open Source Entwicklung also eine wesentlich größere Anzahl von Personen zur Verfügung. Die Aufgabe der Fehlerbeseitigung stellt damit in diesem Entwicklungsmodell kein so großes Problem dar, wie bei der herkömmlichen Methode.

Die Open Source Entwicklung ist sehr stark an die Entwicklung des Internets gekoppelt, was sich u.a. auch daran zeigt, dass ein sehr großer Anteil der Internet-Server auf der Basis von Open Source Software arbeitet. So basieren nach aktuellen Schätzungen ca. 80% aller Internet Mailserver auf dem Open Source Programm Sendmail und 60 % aller Webserver auf Apache. Ein Grund für diese Verbreitung ist, dass das Standardisierungsverfahren, das allen im Internet eingesetzten Protokollen zugrunde liegt, der Open Source Entwicklung sehr entgegenkommt. Diese Standardisierung basiert auf den Request for Comments (RFC), die ein Verfahren beschreiben und – wie der Name sagt – öffentlich zur Diskussion stellen. Erst wenn für ein solches Verfahren zwei unabhängige Implementierungen existieren, die die Machbarkeit bewiesen haben, erhält der RFC den Status eines Standards. Dabei spielt die IETF (Internet Engineering Task Force) (<http://www.ietf.org/>) die Rolle eines Kontrollorgans.

Oftmals sind es Open Source Entwicklungen, die die ersten Implementierungen eines RFCs bilden und in folgenden auch die Basis für kommerzielle Entwicklungen bilden. Der Standardisierungsprozess selbst ist in RFC 2026 definiert (<http://www.ietf.org/rfc/rfc2026.txt>).

## 2.5. Rechtliche Einordnung, insbesondere Urheberrecht, Gewährleistung

Open Source Software unterscheidet sich von anderen Softwareprodukten durch die Lizenzbedingungen. Open Source Lizenzen haben den Zweck, die Veröffentlichung und freie Nutzung von Software zu ermöglichen, während herkömmliche Softwarelizenzen das Ziel haben, sicherzustellen, dass für die Benutzung der Software bezahlt werden muss.

Auch Open Source Software unterliegt wie andere Computerprogramme dem Urheberrecht. Nach §2(1) lit 1 UrhG sind Computerprogramme den Sprachwerken gleichgestellt. Das Urheberrecht schützt das Programm als eine konkrete Umsetzung eines Algorithmus in jeder Ausprägung (Entwurfsmaterial, Quellcode, Binärdaten). Nicht geschützt ist der Algorithmus selbst. Eine Implementierung kann nicht durch das Urheberrecht sondern nur durch Patente geschützt werden.

Auch wenn Programme als solche nach gegenwärtiger deutscher Rechtsprechung nicht patentierbar sind, so wird doch in der gängigen Erteilungspraxis die technische

Anwendung eines auf einem Rechner ausgeführten Verfahrens unter den für die Patenterteilung notwendigen Voraussetzungen (Anwendbarkeit, Neuheit, erfinderischer Schritt) als patentfähig angesehen. Die Europäische Kommission plant derzeit die Klarstellung der Patentierbarkeit von Software in Europa und damit eine Vereinheitlichung der europäischen Rechtsprechung. Die Open Source Gemeinde befürchtet, dass dabei eine Anlehnung an die US-Regelungen erfolgt und hat ihren Widerspruch gegen eine Änderung der gängigen Praxis deutlich gemacht. Ein Beispiel für die Argumentation der deutschen Open Source Gemeinde ist ein Interview vom 7. Juli 2000 mit Daniel Riek, Vorstandsmitglied des LIVE Linux Verband e.V., das hier in Auszügen zitiert wird [11]:

**Keine Entwarnung bei Software-Patenten  
Linux Verband kritisiert Haltung der EU-Kommission**

[http://www.linux-verband.de/aktuell/News\\_60.de.shtml](http://www.linux-verband.de/aktuell/News_60.de.shtml)

*"Die Innovationsgeschwindigkeit in der Informationsgesellschaft bedarf nicht mehr der Unterstützung durch das Patentrecht des 19. Jahrhunderts, das ja ursprünglich als Belohnung für die Offenlegung von Forschungsergebnissen gedacht war. – Hier geht es nicht mehr um Dampfmaschinen, sondern um digitale Information!" Ohnehin sei, so der LIVE-Mann, Open-Source-Software dem Fortschritt deutlich dienlicher als eine offengelegte, jedoch mit Patenten blockierte Technologie.*

*"Die politische Forderung des LINUX Verbandes bleibt daher, auf die Patentierbarkeit von so genannten Software-bezogenen Erfindungen zu verzichten oder zumindest Open-Source-Software grundsätzlich von der Wirkung des Patentrechts auszunehmen" fasst das LIVE-Vorstandsmitglied zusammen. Nur so könne Europa langfristig von den Vorteilen freier Software profitieren und eine international wettbewerbsfähige Software-Industrie aufbauen.*

Weitere Hinweise zu Fragen der Einordnung von Open Source Software hinsichtlich des Urheber- und des Patentrechts findet man unter [9].

Eine Gewährleistung auf Open Source Software gibt es im allgemeinen nicht, da für die Bereitstellung der Software keine Lizenzgebühren erhoben werden. Insofern sind Gewährleistungsansprüche bei Open Source Software noch stärker eingeschränkt als bei normalen Softwareprodukten.

## **2.6. Unternehmen, SuSE und andere Distributoren**

Es gibt mittlerweile eine Vielzahl von Unternehmen, die sich kommerziell mit Linux beschäftigen. Diese Unternehmen können nach der Art ihres Geschäftsmodells unterschieden werden.

**Distributoren** sind Unternehmen oder Organisationen, die Linux zusammen mit weiterer freier Software und Dokumentation zusammenstellen und verkaufen. Der Mehrwert entsteht hierbei durch die Erstellung des Pakets, die Bereitstellung von

Installationsverfahren, die es auch ungeübten Anwendern ermöglichen, Linux zu installieren sowie durch einen befristeten kostenlosen Installationssupport.

Beispiele: Caldera, Corel, Debian, Mandrake, Red Hat, SuSE, Turbo Linux

**Hardwarehersteller** haben mit der zunehmenden Verbreitung von Linux ein wachsendes Interesse an der Verfügbarkeit von Linux auf ihren Hardwareplattformen. Sie schließen meist Kooperationen mit einem oder mehreren Distributoren ab, die ihre Linux Distribution für diese Hardware zertifizieren.

Beispiele: IBM, Fujitsu Siemens Computers, SGI, Compaq.

**Anbieter von Standardsoftware** unterstützen Linux ebenfalls wegen der zunehmenden Verbreitung aber auch, weil sich Linux zunehmend zum UNIX-Standard entwickelt hat, der auf allen Plattformen verfügbar ist. Auch hier werden meist Kooperationen mit einigen Distributoren abgeschlossen.

Beispiele: SAP, Oracle, Software AG, SUN, Informix, IBM

Es gibt aber auch mittlerweile Anbieter von Standardsoftware, die eigene Distributionen herausgeben.

Beispiele: Corel

**Dienstleister** bieten für Linux Support, Beratungen und Schulungen an.

Beispiele: ID-Pro, Innominate, Red Hat, SuSE

**Verlage** profitieren von der großen Nachfrage an Literatur zum Thema Linux und Open Source Software generell.

Beispiele: O'Reilly, SuSE Press

## 2.7. Weitere Entwicklung, Ausblick

Derzeit scheint sich das Open Source Entwicklungsmodell neben dem herkömmlichen Modell als anerkannte Alternative zu etablieren. Obwohl beide Systeme gegeneinander konkurrieren, ist nicht zu erwarten, dass eines verschwinden wird. Es ist nicht zu verleugnen, dass das Bazaar Model auch seine Schwächen hat, obgleich es seine außerordentliche Funktionstüchtigkeit hinreichend bewiesen hat. Da sich Projekte um Persönlichkeiten bilden, die versuchen müssen, möglichst viele Mitglieder der Open Source Gemeinde für ihr Projekt zu gewinnen, wird es auch immer Themengebiete geben, in denen das nicht ohne weiteres gelingt. Vermutlich ist es erfolgversprechender, Entwicklungen für betriebswirtschaftliche Standardsoftware in einer »Kathedrale« zu betreiben als in einem »Basar«.

Es zeichnet sich ab, dass vor allem große kommerzielle Unternehmen wie z. B. Siemens SUN oder IBM künftig ihre Entwicklungen wenigstens teilweise als Open Source veröffentlichen werden. Den ersten Schritt hat Netscape mit der Freigabe seiner Browser-Software unter dem Open Source Projektnamen Mozilla bereits vollzogen. IBM hat bereits ein Linux Technology Center eingerichtet, das eng mit OSS Entwicklern zusammenarbeitet (<http://oss.software.ibm.com/developerworks/opensource/linux/>)

Die Schwerpunkte der Open Source Software Entwicklung haben sich von der Toolentwicklung (z. B. GNU) zunächst auf die Betriebssystem Entwicklung (z. B. Linux) ausgedehnt. Aktuell erschließt sich die Open Source Gemeinde den Bereich der Desktop- und Anwendungsentwicklung (z. B. KDE und KOffice). Es ist wahrscheinlich, dass zukünftig verstärkt in den Bereichen der Embedded Systems und Spiele gearbeitet wird.

## **2.8. Service, Support**

Das weitgehend fehlende Supportangebot für Linux-Systeme stellte bis vor einem Jahr noch ein wesentliches Hindernis für den kommerziellen Einsatz von Linux dar. Inzwischen hat sich dies grundlegend geändert. Alle Hardwarehersteller, die auch Linux als Betriebssystem unterstützen, bieten für Linux den gleichen Support an, wie für vergleichbare kommerzielle Betriebssysteme. Der 3<sup>rd</sup> Level Support wird dabei meist durch Linux-Dienstleister wie z. B. die SuSE GmbH erbracht, mit denen die Hardwarelieferanten Supportverträge abgeschlossen haben.

Darüberhinaus bieten die Linux-Unternehmen ein breites Spektrum an Dienstleistungen um das Betriebssystem Linux herum an, die bei weitem nicht auf das Betriebssystem beschränkt sind.

Das Supportkonzept der SuSE reicht vom kostenlosen Installationssupport, über Callpacks bis hin zum 24x7 Support rund um die Uhr durch Callcenter. Anspruchsvolle Anwender können sich mit Supportpaketen, die bis hin zur Fehlerbeseitigung auf Quellcode-Ebene reichen, ein Maximum an Sicherheit einkaufen (siehe <http://support.suse.de/>)

### 3. Linux, die Alternative

#### 3.1. Unterschiede zu eingeführten Systemen

##### 3.1.1. Kernel-Architektur

Linux ist eines der wenigen Betriebssysteme, das auf allen Plattformen vom Embedded System über Midrange-Server bis hin zum Mainframe und massiv parallelen Supercomputern eingesetzt wird. Ein Grund hierfür ist die spezifische Architektur des Linux-Kernels. Im Gegensatz zu anderen Betriebssystemen wie z. B. Microsoft Windows NT/2000, MacOS oder OS/2 hat Linux keinen Microkernel sondern einen monolithischen Kernel. Das bedeutet, dass alle Kernfunktionen des Betriebssystems im residenten Hauptspeicher gehalten werden. Die Idee des Microkernels ist, alle Hardwareabhängigkeiten in einem sogenannten Hardware Abstraction Layer abzuhandeln, so dass der eigentliche Betriebssystemkern sehr klein gehalten werden kann. Dies sollte die Portierung auf andere Hardwareplattformen erleichtern. Linus Torvalds, der Schöpfer von Linux, war jedoch der Meinung, dass Microkernel-Architekturen zu Komplexität und Performance-Engpässen neigen. Er ging beim Design von Linux davon aus, dass die heute und in absehbarer Zukunft existierenden Hardware-Architekturen auf gemeinsamen Grundlagen beruhen, die auch zu gemeinsamen Grundfunktionen führen. Diese gemeinsamen Funktionen werden im monolithischen Kernel von Linux behandelt. Der Vergleich der unterstützten Hardwareplattformen zwischen Linux und z. B. Windows NT/2000, macht deutlich, dass Linus Torvalds die richtige Entscheidung getroffen hat.

Die Kombination des monolithischen Kernels mit der allgemeinen Verfügbarkeit der Quellen ermöglicht zudem jedem Linux-Nutzer eine Neukompilierung des Kernels und damit eine individuelle Anpassung an seine Anforderungen. Dies bringt die folgenden Vorteile:

- Das Betriebssystem enthält nur noch die notwendigen Komponenten; alles Überflüssige kann entfernt werden.
- Das Betriebssystem benötigt weniger Ressourcen. Es gibt Linux-Systeme, die auf eine Diskette mit 1,4 MB passen.
- Der Verzicht auf alle überflüssigen Komponenten ist eine wesentliche Voraussetzung für den Aufbau sicherer Systeme. Jeder unnötige Dienst kann Sicherheitslöcher öffnen.

##### 3.1.2. Multiuser-Fähigkeit

Linux ist wie UNIX multiuser-fähig, das heißt, dass auf einem Linux-System gleichzeitig mehrere Benutzer arbeiten können, z. B. indem sie über direktangeschlossene Terminals arbeiten oder, was heute fast immer der Fall ist, indem sie sich über das Netz anmelden. Für Windows-Benutzer ist es oft schwer zu verstehen, was Multiuser-Fähigkeit bedeutet, denn auch an einem Windows-NT Server können mehrere Benutzer gleichzeitig Dienste in Anspruch nehmen. Dazu ist jedoch immer ein Client-Programm auf einem Client-Rechner erforderlich, das mit dem Server kommuniziert. Linux stellt dagegen jedem

angemeldeten Benutzer auf dem Server eine vollständige Benutzerumgebung mit allen Diensten zur Verfügung.

Selbst für ein System, an dem normalerweise nur eine Person arbeiten wird, wie z. B. ein Notebook, bringt die Multiuser-Fähigkeit entscheidende Vorteile. Linux stellt dem Benutzer neben dem grafischen Desktop nämlich noch virtuelle Konsolen zur Verfügung, an denen man sich auf der Betriebssystemebene der Shell anmelden kann. Falls also die grafische Benutzeroberfläche des Betriebssystems nicht mehr reagiert, kann man sich immer noch auf einer virtuellen Konsole anmelden und den Desktop neu starten. Ein Neustart des ganzen Betriebssystems, wie unter Windows üblich, ist unter Linux daher so gut wie nie erforderlich.

### 3.1.3. Multitasking

Linux ist ein Multitasking-System, d.h. es kann mehrere Prozesse gleichzeitig abarbeiten. Das Betriebssystem hat die Kontrolle über die Prozesse und entscheidet, wann ein Prozess suspendiert wird. Selbst wenn der Rechner, auf dem man arbeitet nur über einen Prozessor verfügt und somit eine parallele Abarbeitung mehrerer Prozesse nicht möglich ist, wird dadurch die Performance des Systems erheblich beschleunigt.

### 3.1.4. Windows-System

Unter Microsoft Windows ist, wie der Name schon andeutet, das Windowssystem vom Betriebssystem nicht zu trennen. Bei Linux ist das anders. Man benötigt kein Windows-System, um Linux zu administrieren. Das Windowssystem von Linux ist X. Dabei handelt es sich um eine Entwicklung des MIT, die seit 1996 von »The Open Group« übernommen wurde.

Das X-Window-System zeichnet sich durch seine integrierte Netzwerkfähigkeit aus. Es besteht immer aus einem X-Client und einem X-Server, die über ein Netzwerk verteilt oder auf der selben Maschine ablaufen können. Durch diese Eigenschaft ist jede X-Anwendung sofort netzwerkfähig. Der unter Linux eingesetzte X-Server wird durch das Open Source Software Projekt XFree86 entwickelt.

Auf dem X Windows System wird meist ein Windowmanager betrieben, der erweiterte Funktionen für die Verwaltung der Fenster zur Verfügung stellt. Für Linux gibt es eine Vielzahl von Windowmanagern und Desktops, von denen hier nur die wichtigsten aufgeführt werden sollen:

- |               |                                                                                                                                                                                                       |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MWM           | Der Motif Windowmanager. Da Motif bis vor kurzem lizenzpflichtig war, ist dieser ältere UNIX Window Manager unter Linux kaum anzutreffen.                                                             |
| FVWM2, FVWM95 | Eine Familie von Windowmanagern, die mehrere virtuelle Desktops zur Verfügung stellen, zwischen denen der Benutzer hin- und herschalten kann. FVWM95 imitiert dabei das Look-and-feel von Windows 95. |

CDE	Das Common Desktop Environment ist der erste erfolgreiche Ansatz, unter den verschiedenen UNIX–Derivaten einen gemeinsamen Desktop anzubieten. CDE ist lizenzpflichtig.
KDE	Das schon erwähnte K Desktop Environment, der derzeit erfolgreichste Desktop unter Linux.
GNOME	Eine Alternative zu KDE, die entstand, weil in einer alten Version von KDE Komponenten eingesetzt wurden, die nicht Open Source zertifiziert waren.

### 3.1.5. Entwicklungswerkzeuge

Linux wird nicht nur mit den Quellcodes ausgeliefert, sondern auch mit allen für die Übersetzung der Quellen notwendigen Werkzeugen. Diese Werkzeuge sind ebenfalls Open Source Software und wurden zu einem großen Teil im GNU Projekt entwickelt. (GNU ist die rekursive Abkürzung für Gnu is not UNIX).

### 3.2. Hardware

Linux ist auf eine Vielzahl von Hardware–Architekturen portiert worden. Die wichtigsten sind:

- Intel IA32
- Alpha AXP
- SUN Sparc
- PowerPC
  - Macintosh
  - IBM RS/6000
  - Motorola PreP
- IBM S/390

IBM arbeitet derzeit an der Portierung von Linux auf die AS/400.

Die Anforderungen von Linux an die Hardware hängen von den Funktionen ab, für die das System eingesetzt wird.

### 3.3. Software

Es gibt für Linux eine nicht mehr überschaubare Menge an Softwarepaketen. Alle großen Anbieter von Standardsoftware unterstützen Linux bereits heute oder planen, ihre Software zukünftig auch unter Linux anzubieten. Diese Feststellung bezieht sich selbstverständlich nicht auf Produkte von Microsoft oder Produkte von mit Microsoft verbundenen Unternehmen. Allerdings gibt es mit dem Produkt VMware eine virtuelle Maschine für Linux in der Windows Betriebssysteme als Gastssysteme unter Linux

ablaufen. Dadurch ist die Nutzung von Microsoft Windows Anwendungen auch unter Linux möglich.

Die SuSE Linux Distribution enthält neben dem Betriebssystem noch 1500 weitere Softwarepakete (<http://www.suse.de/de/produkte/susesoft/linux/Pakete/gesamt.html>).

Einen Überblick über die für Linux verfügbare kommerzielle Software gibt der Linux Isis Report [12].

### **3.4. Installation**

Die Installation ist bei den meisten Linux-Distributionen heute auch für unerfahrene Anwender kein Problem mehr. Sie wird durch grafische Installationsprogramme wie SuSE Yast II unterstützt, so dass keine spezifischen Linux Kenntnisse erforderlich sind.

Dem Linux Experten stehen darüber hinaus mit der SuSE Distribution automatische Installationsverfahren zur Verfügung, die für den Aufbau größerer Umgebungen notwendig sind.

### **3.5. System- und Benutzerverwaltung**

Linux ist ein UNIX-System und bietet die unter UNIX-Systemen üblichen Mechanismen der Systemverwaltung, d.h. mächtige kombinierbare Tools, die meist über Kommando-schnittstellen bedient werden müssen. Für den unerfahrenen Benutzer ist dies oft eine unüberwindbar scheinende Hemmschwelle. Erfahrenen Benutzern gibt die Beherrschung dieser Werkzeuge dagegen die direkte Kontrolle über das System. Aus diesem Grund ist Linux bei Systemadministratoren, die es einmal kennengelernt haben, so beliebt.

Linux verfügt mit dem K-Desktop-Environment KDE (<http://www.kde.org/>) über einen Desktop, der dem Benutzer die erforderlichen Verwaltungswerkzeuge auch mit grafischen Benutzeroberflächen zur Verfügung stellt.

Für die Benutzerverwaltung von Linux gibt es eine Vielzahl unterschiedlicher Möglichkeiten, auf die teilweise in den folgenden Abschnitten detaillierter eingegangen wird. Als Stichworte seien an dieser Stelle genannt:

- Lokale Benutzerverwaltung
- Network Information Service (NIS)
- Kerberos
- Distributed Computing Environment (DCE)
- LDAP/X.500

### **3.6. Linux als Server-Plattform**

Als Server Betriebssystem hat sich Linux in den Unternehmen inzwischen durchgesetzt. Dies wird eindrucksvoll durch den ständig wachsenden Marktanteil von 6% in 1997, 17% in 1998 und 25 % in 1999 verdeutlicht. IDC prognostiziert Linux in diesem Sektor auch

weiterhin ein jährliches Wachstum um 25–30% –ungefähr doppelt so hoch wie die übrigen Betriebssysteme zusammen. [4]

### 3.6.1. Intranet

#### Fileserver

Linux unterstützt eine ganze Reihe von Fileserver-Protokollen sowohl als Client wie auch als Server. Die wichtigsten sollen an dieser Stelle kurz beschrieben werden:

SMB, das Server Message Block Protokoll, ist das Protokoll, das Windows for Workgroups (WfW), Windows 95, Windows NT, Windows 2000 und OS/2 Lan Manager benutzen, um gemeinsam Dateien und Drucker in einem lokalen Netz zu nutzen. SMB ermöglicht das einhängen (mounten) von Dateisystemen (oftmals in diesem Zusammenhang "Shares" genannt) und den Zugriff, wie auf jedes andere Unix-Verzeichnis. Durch das Open Source Produkt Samba wird ein Linux-System zu einem vollwertigen File- und Printserver in einem Windowsnetz. Mehr dazu finden Sie im Abschnitt 6.2.3 Samba als File/Printserver.

NFS, das Network Filesystem, ist das in UNIX-Netzwerken am häufigsten eingesetzte Netzwerk Filesystem. Es basiert auf SUN RPC, der Remote Procedure Call Definition von SUN. NFS ermöglicht den Zugriff auf Dateien, die auf remote Systemen liegen, in derselben Weise wie auf Dateien, die auf einem lokalen Rechner vorhanden sind. Die Konfiguration von NFS ist sehr einfach: Der NFS Server exportiert anhand einer Liste Verzeichnisse, die die NFS Clients dann in den lokalen Dateibaum einhängen können. NFS basiert normalerweise auf UDP/IP, dem IP-Datagramm-Dienst und ist daher nur für den Einsatz in LANs geeignet.

Coda ist ein noch in Entwicklung befindliches Netzwerk-Dateisystem. Es ermöglicht, ähnlich wie NFS, Dateisysteme eines entfernten Servers einzuhängen (zu mounten) und auf diese mit regulären Unix-Befehlen zuzugreifen, als lägen sie auf einer lokalen Festplatte. Coda hat einige Vorteile gegenüber NFS:

- Unterstützung für unterbrochene Operationen,
- Replikation des Servers (read/write),
- Sicherheitsmodelle für Authentisierung und Verschlüsselung,
- persistente Caches bei Klienten und Zurückschreiben von Caches.

AFS, das Andrew Filesystem, wurde an der Carnegie Mellon's University entwickelt. Es handelt sich um ein verteiltes Dateisystem, das auch über Wide Area Networks (WAN) benutzt werden kann. Im Unterschied zu SMB oder NFS müssen Dateisysteme bei AFS nicht gemountet werden, sondern sie stehen ständig unter dem Verzeichnis /afs zur Verfügung. AFS ermöglicht die Replikation von Servern, so dass Server-Ausfälle vom Client nicht bemerkt werden. AFS Clients verfügen über einen lokalen Cache, um die Netzlast zu verringern.

### **Applicationserver**

Ein Application-Server erlaubt das gleichzeitige Benutzen von Anwendungen durch mehrere User. Dazu benötigt der Application-Server genügend Kapazität an Hauptspeicher und Rechenleistung. Im Gegenzug können – meist in weit größerem Ausmaß – Kapazitäten auf der Client-Seite eingespart werden, was zu einem sogenannten Thin-Client Konzept führt. In Verbindung mit Kosteneinsparungen durch die zentralisierte Anwendungsadministration sind Application-Server ein hervorragendes Mittel zur Serverkonsolidierung. Linux bringt alle notwendigen Eigenschaften, die ein Application-Server benötigt, wie Multi-Tasking und Multi-User-Fähigkeit, hohe Stabilität und ausgefeilte Speicherverwaltung von Hause aus mit sich. In Abschnitt 6.2.1 wird an einem Einsatzbeispiel gezeigt, wie Linux als Application-Server für Office-Lösungen eingesetzt werden kann.

### **Printserver**

Unter Linux werden am besten PostScript-Drucker eingesetzt, da viele unter Linux verfügbare Werkzeuge zur Erstellung von Texten und Grafiken PostScript erzeugen. Linux enthält einen freien PostScript Interpreter namens Ghostscript, der mehr als 100 Druckertypen unterstützt. Über den Linux Druckerspooler können sowohl lokale als auch Netzwerkdrucker angesprochen werden.

Mit Samba (siehe Abschnitt 6.2.3) kann Linux auch in einem Windows-Netz als Printserver eingesetzt werden.

### **Mailserver**

Der am häufigsten eingesetzte Mail Transfer Agent (MTA) unter Linux ist sicherlich Sendmail (<http://www.sendmail.org>). Sendmail wurde um 1980 von Eric Allman in Berkeley entwickelt und bildet das Rückgrat der Internet E-Mail.

Das von Wietse Venema mit IBM Unterstützung entwickelte Programm Postfix (<http://www.postfix.org>) ist eine Alternative zu Sendmail, die einige Probleme von Sendmail durch ihre modulare Struktur zu beseitigen sucht.

Sendmail und Postfix sind Mail Router für das Simple Message Transfer Protocol (SMTP), die Mail an lokale Postfächer ausliefern. Heute werden dafür meist Arbeitsgruppen-Server benutzt, von denen die Benutzer ihre Mail über die Protokolle POP und IMAP abholen. Auch diese POP- bzw. IMAP-Server sind als Open Source Software unter Linux verfügbar<sup>3</sup>.

---

3 Suse bietet einen vorkonfigurierten IMAP-Server für Arbeitsgruppen an.  
<http://www.suse.de/de/produkte/susesoft/imas/index.html>.

### 3.6.2. Internetserver

#### Webserver

Nach Angaben des Internet Operating System Counter (<http://www.leb.net/hzo/ioscount>) liefen im April '99 42,7% der Webserver der .de Domain unter Linux, was einer Anzahl von 197.670 entsprach.

Der unter Linux am häufigsten eingesetzte Webserver ist das Open Source Produkt Apache. Der Name rührt daher, dass Apache aus einer Reihe von Modifikationen (patches) am frei verfügbaren Sourcecode des NCSA httpd Webserver entstanden ist: »a patchy server«.

Eine Analyse der Ausfallzeiten realer Webserver der Zeitschrift c't im April 2000 hat gezeigt, dass die Stabilität der Kombination Linux/Apache etwa fünfmal höher liegt als die von Windows NT/IIS. [13]

Nach den Zahlen, die NetCraft Survey of Web Sites unter <http://www.netcraft.net/survey/> veröffentlicht, ist der Apache Webserver der am häufigsten eingesetzte Webserver im Internet (Abbildung 1)

#### Firewalls

Das Thema Linux-Firewalls wird in Abschnitt 6.2.2 ausführlich behandelt.

#### Mailserver

Für Internet Mailserver kommen üblicherweise die gleichen Produkte zum Einsatz wie im Intranet.

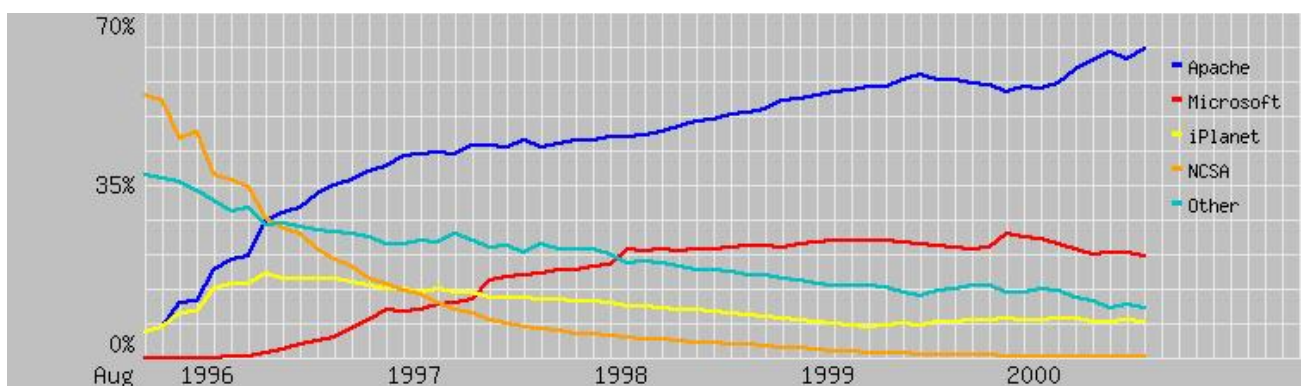


Abbildung 1: Market Share for Top Servers Across All Domains August 1995 - June 2000

### 3.7. Linux als Client-Plattform

Die Bedeutung von Linux als Desktop-System wurde von Analysten bisher nur als gering eingestuft. Es wird meist davon ausgegangen, dass der Linux-Anteil in diesem Sektor bei 4-5% liegen wird. Man erwartet nicht, dass Linux Microsoft Windows NT/2000 ersetzen wird, da Linux im Office- und Desktop-Bereich erst noch in den Anfängen steckt. Eine

tiefere Durchdringung des Desktop-Marktes wird allenfalls in der langfristigen Perspektive als realistisch angesehen. [4]

Der Grund dafür ist die Marktdurchdringung, die Microsoft heute in diesem Bereich hat. Allerdings gibt es inzwischen eine Reihe von Initiativen bei Behörden und Unternehmen, die prüfen, inwieweit Linux Desktop-Systeme bereits heute die Anforderungen erfüllen. Für Linux spricht die hervorragende Stabilität und das Wegfallen von Lizenzgebühren.

In Abschnitt 6.2.1 werden konkurrenzfähige Office-Produkte für Linux vorgestellt.

### **3.8. Router**

Für Arbeitsgruppen, mit begrenztem Netzwerkaufkommen stellen Router auf Linux-Basis eine leistungsfähige und kostengünstige Alternative dar, die oftmals die Weiterverwendung von Hardware ermöglicht, die anderenfalls ausgemustert werden müsste. Ein Linux-Router kann durchaus auf einem Intel 486 PC mit 16 MB Hauptspeicher realisiert werden. In größeren Netzen mit hoher Last sollten jedoch spezialisierte Router eingesetzt werden, bei denen Software und Hardware von vornherein für diese spezielle Aufgabe entwickelt wurden.

### **3.9. Koexistenz mit eingeführten Systemen**

Da Linux eine Vielzahl von Protokollen, Schnittstellen und Server-Anwendungen unterstützt, lassen sich Linux-Systeme besonders leicht in vorhandene Umgebungen integrieren. Die leichte Administrierbarkeit und die Stabilität eines Linux-Servers wirkt sich dabei positiv auf die Verfügbarkeit der Dienste aus.

### **3.10. Interoperabilität**

Aufgrund der Dominanz von Microsoft im Desktop-Bereich wurden die proprietären Formate von Microsoft Office zum Quasi-Standard. Alle konkurrierenden Produkte werden an der Kompatibilität zu diesen Formaten gemessen. Da es sich meist um nicht veröffentlichte Formate handelt, die in der Vergangenheit auch auf Kosten der Kompatibilität immer wieder verändert wurden, haben die Konkurrenzprodukte meist das Nachsehen<sup>4</sup>. Der Anwender wird nur dann die Wahlfreiheit beim Betriebssystem und der Anwendung haben, wenn herstellerunabhängige Dokumentenformate sich durchsetzen können. Obwohl alle unabhängigen Standardisierungsbemühungen für Dokumentenformate wie z. B. der ISO Standard 8613 ODA (Office Document Architecture) an der mangelnden Unterstützung durch die Hersteller von Office-Produkten gescheitert sind, gibt es heute etablierte und offengelegte Dokumenten-Standards. Beispiele dafür sind die weite Verbreitung des Portable Document Formats (PDF) von Adobe sowie die Extended Markup Language (XML). Insbesondere in Behörden ist PDF heute ein anerkanntes Austauschformat [6].

---

<sup>4</sup> Die Filterfunktionen von StarOffice wurden allerdings vom BSI nach Tests als »praxistauglich« bezeichnet [6].

### 3.11. Vorteile

#### **Leichte Administrierbarkeit**

Warum ist Linux leicht administrierbar? Es steht doch im Ruf im Vergleich mit Microsoft Windows für den Endanwender schwieriger bedienbar zu sein?

Leicht administrierbar bedeutet, dass die Funktionen eines Betriebssystems auf einfache Weise für den Benutzer bzw. bei Servern für den Administrator konfigurierbar und kontrollierbar sein müssen.

Der Verdienst von Microsoft Windows liegt darin, dem Anwender kryptische Kommandos zu ersparen und statt dessen komfortable grafische Benutzeroberflächen für die Systembedienung anzubieten. Der Anwender muß sich zunächst nicht mehr intensiv mit dem System auseinandersetzen, weil er durch die grafische Benutzeroberfläche geführt wird, so wie es sich der Programmierer vorgestellt hat. Das ist solange hilfreich, bis Situationen eintreten, die bei der Entwicklung nicht vorgesehen waren. In diesem Fall ist der Anwender in der Regel hilflos. Vielleicht kann er noch mit Hilfe des Registryeditors das Problem beseitigen. Dazu ist aber einiges Expertenwissen erforderlich.

Im Unterschied zu Windows stellt Linux neben der grafische Benutzeroberfläche verschiedene Kommandozeileninterprete – im Fachjargon Shells genannt – zur Verfügung. Wer sich die Mühe macht, sich mit einer dieser Kommandosprachen auseinanderzusetzen, wird mit der nahezu vollständigen Kontrolle über das System belohnt. Ein meist übersehener Vorteil von Kommandosprachen ist, dass ein Systembefehl viel besser zu beschreiben ist, als eine grafische Benutzeroberfläche. Das Problem, Befehle mit Optionen und Parametern auswendig lernen zu müssen wird durch die umfangreichen online Manuals erheblich entschärft.

Dass alle wichtigen Konfigurationsparameter in ASCII-Dateien gespeichert werden, die mit einem Texteditor bearbeitet werden können, erleichtert die Administration von Linux erheblich. Es gibt keine mehr oder weniger vollständig dokumentierte Systemkonfigurationsdatenbank, die mit eigens dafür vorgesehenen Werkzeugen bearbeitet werden muss.

#### **Sparsamer Ressourcen-Verbrauch**

Linux ist im Verhältnis zu anderen Betriebssystemen relativ schlank. Es besteht allerdings immerhin noch aus ca 20 Mio. Zeilen Quellcode. Ein Grund für den sparsamen Ressourcenverbrauch ist die Anpassbarkeit an die wirklichen Gegebenheiten. Nicht benutzte Funktionen können aus dem Betriebssystem entfernt werden. Ein anderer Grund ist das Open Source Entwicklungsmodell. Jeder Programmierer möchte seinen Code so effizient wie möglich schreiben, um die Anerkennung seiner Kollegen zu erhalten. Der Quellcode ist schließlich für die Öffentlichkeit sichtbar und ist das Aushängeschild eines Programmierers.

### **Hohe Stabilität**

Auch die hohe Stabilität von Open Source Software ist auf das Open Source Entwicklungsmodell zurückzuführen. Durch die Veröffentlichung des Quellcodes werden viele Fehler durch Codeinspektionen von Entwicklern gefunden und nicht erst bei der Anwendung durch den Benutzer. Zudem ist der Prozess der Fehlerbeseitigung effizienter. Man führe sich vor Augen, was geschieht, wenn man als Anwender eines nicht Open Source Programms auf einen Fehler stößt. Man kann den Fehler melden und darauf hoffen, dass er im nächsten Release, für das man möglicherweise Upgradelizenzen bezahlen muss, beseitigt sein wird. Bei Open Source Software kann man selbst versuchen, den Fehler im Quellcode aufzuspüren, zu beseitigen und die Fehlerbehebung zu testen. Anschließend wird der »Fix« an den Autor geschickt, der ihn nochmals prüft und in die neue Version aufnimmt. Die neue Version steht in der Regel kurze Zeit später im Internet zum herunterladen bereit. Natürlich wird ein normaler Endbenutzer nicht dazu in der Lage sein, Fehler im Quellcode zu beseitigen. Stellt man sich jedoch vor, wieviele interne IT-Experten oder externe Berater heute damit beschäftigt sind, Fehler zu umgehen, weil sie keinen Zugriff auf den Quellcode haben, wird deutlich, welche Vorteile Open Source Software beim Einsatz in Unternehmen mit sich bringt. Open Source Software lässt sich sehr viel schneller und stabiler in Ihre IT-Infrastruktur integrieren.

### **Transparenz der Funktionalität aufgrund des Open Source Ansatzes**

Es ist offensichtlich, dass es so gut wie unmöglich ist, trojanische Pferde oder andere Hintertüren in Open Source Software einzubauen. Man müsste darauf hoffen, dass niemand bei Codeinspektionen darauf stößt. Das ist bei der Vielzahl von Entwicklern, die sich heute mit Open Source Software beschäftigen äußerst unwahrscheinlich.

Vorfälle, wie die Entdeckung eines NSAKEY<sup>5</sup> in Microsoft Windows CryptoAPI System, die das Vertrauen in die Sicherheit von Microsoft Betriebssystemen<sup>6</sup> im August 1999 erschütterte, sind bei Open Source Software undenkbar. Unabhängig davon, ob Microsofts Aussage, es handele sich um einen Backupschlüssel richtig ist, oder ob der Verdacht stimmt, dass Microsoft Betriebssysteme eine Hintertür enthalten, die der NSA (U.S. National Security Agency) Zutritt zum System ermöglichen soll, ist das Fehlen einer unabhängigen Überprüfung ein Sicherheitsrisiko an sich, das in vielen Bereichen nicht tragbar ist.

### **Herstellerunabhängigkeit**

Open Source Software wird, wie bereits dargestellt, stets mit dem Quellcode ausgeliefert. Dadurch können Anpassungen und Fehlerbehebungen, die bei konventioneller Software dem Hersteller als alleinigem Inhaber des Quellcodes möglich sind, im Prinzip von jedem Programmierer vorgenommen werden. Der Anwender ist dadurch unabhängiger vom Hersteller der Software.

---

5 Andrew Fernandes: Microsoft Installs US Spy Agency with Windows, <http://www.cryptonym.com/hottopics/msft-nsa/msft-nsa.html>

6 Der zweite Schlüssel mit der Bezeichnung \_NSAKEY wurde in NT4, Windows 95, Windows 98 und Windows 2000 gefunden.

Diese Unabhängigkeit bezieht sich auch auf die Releasezyklen. Mit Open Source Software ist es möglich bei einem Release stehenzubleiben, ohne zukünftige Releasewechsel nachvollziehen zu müssen. Trotzdem können aufgrund der Verfügbarkeit des Quellcodes auftretende Fehler noch beseitigt werden.

### **Günstige Anschaffungs- und Betriebskosten (TCO)**

Seit dem Erfolg von Linux ist eines der häufig geäußerten Argumente von Herstellern konventioneller Betriebssysteme, dass die Kosten des Betriebssystems laut Gartner nur einen Anteil von ca 5% an den Gesamtkosten nach TCO ausmachen, die ein System während seiner Lebensdauer verursacht.

Damit können Linux und andere Open Source Betriebssysteme schon einmal ein Einsparpotenzial von 5% für sich verbuchen.

Weitere Einsparungen ergeben sich durch die hohe Stabilität und die gute Adminstrierbarkeit, die weniger Betriebsaufwand erfordern. Die gute Ressourcenauslastung sorgt darüber hinaus für ein längeres Nutzungspotenzial und eine längere Lebensdauer der Systeme.

### **3.12. Einschränkungen**

Obwohl Linux in den Bereichen Hardwareunterstützung und Anwendungssoftware gegenüber MS Windows Betriebssystemen aufgeholt hat, gibt es immer noch Defizite. Die USB Unterstützung ist derzeit noch auf relativ wenige Geräte beschränkt. Linux hat derzeit in der Ausnutzung der möglichen Hardware auf Intel noch weitere Einschränkungen, an deren Beseitigung gearbeitet wird:

- Maximal ausgenutzter Hauptspeicher 4 GB
- Maximale SMP Unterstützung bei linearer Performance 4 CPUs
- Maximale File-Größe 2 GB

Linux verfügt nicht wie die meisten anderen UNIX Derivate über eine Sicherheitsklassifizierung nach Orange Book C2. Diese formale Klassifizierung ist in sicherheitskritischen Bereichen oft die Voraussetzung für die Auswahl des Betriebssystems.

Die im Vergleich zu MS Windows eingeschränkte Verfügbarkeit von Anwendungssoftware ist immer noch zu spüren, auch wenn viele Hersteller Linux als unterstützte, wenn nicht sogar als strategische Plattform ansehen.

### **3.13. Absehbare Entwicklungen**

Im technischen Bereich wird derzeit an Hochverfügbarkeitslösungen für Linux gearbeitet, die den Betrieb von Linux-Systemen auch für Mission Critical Server ermöglichen sollen. Hier ist SuSE mit SGI eine Kooperation eingegangen, um die Hochverfügbarkeitslösung von SGI »Fail-safe« unter Open Source Software Lizenzen frei verfügbar zu machen.

Darüber hinaus wird an vielen weiteren aktuellen Themen gearbeitet wie z. B.

- Linux MPP Supercomputer
- Embedded Systems
- Large File Support
- KOffice – Linuxdesktop

## 4. Sicherheit

Da Linux als Open Source Software zusammen mit dem Quellcode verbreitet wird, besteht immer Transparenz über die Struktur und die Verhaltensweise des Systems. Das unbemerkte Einschleusen von Hintertüren in Programme ist durch die Offenlegung nicht vorstellbar. Dies ist insbesondere für sicherheitskritische Bereiche relevant, in denen man sich nicht auf Aussagen eines Herstellers verlassen kann oder will.

Die Verfügbarkeit des Quellcodes führt dazu, dass Sicherheitsprobleme proaktiv erkannt werden können, bevor sie in der Realität auftreten. Auf der anderen Seite steht der Quellcode natürlich auch Computerkriminellen offen, die durch Studium des Quellcodes potenzielle Sicherheitslücken leichter entdecken können.

### 4.1. Unterschiede zu eingeführten Systemen

Als Multi-User System hat Linux ein Sicherheitskonzept, das den Zugriff der Benutzer auf Systemressourcen regelt. Jede Ressource, sei es eine Datei, ein Verzeichnis, ein Prozess oder ein Programm gehört einem Benutzer und zu einer Gruppe. Der Besitzer der Systemressourcen ist der Superuser *root*, den es auf jedem Linux-System gibt. Für Verzeichnisse und Dateien werden die Zugriffsberechtigungen jeweils für den Besitzer, die Gruppe oder andere (weder Benutzer noch Gruppe) definiert. Die Systemdateien gehören dem Superuser und haben sehr restriktive Zugriffsrechte, die verhindern, dass normale Benutzer die Systemkonfiguration verändern können.

### 4.2. Computerviren

Obwohl auch unter Linux Computerviren vorstellbar sind, gibt es kaum Fälle, die in der Öffentlichkeit bekannt geworden sind. Dies liegt nicht zuletzt am Sicherheitskonzept von Linux, das den Zugriff eines Virus, der meist von einem Benutzer über E-Mails oder Downloads eingeschleppt wurde, auf Systemressourcen verhindert.

Ein E-Mail Virus wie Melissa oder ILOVEYOU richtet unter Linux keinen Schaden an:

1. Weil der Benutzer, der die E-Mail empfängt und das Attachment ausführt normalerweise nicht über die notwendigen Privilegien verfügt, die der Virus bräuchte, um Änderungen am System vorzunehmen.
2. Um Änderungen am System vorzunehmen, muss ein Virus Superuser Privilegien erlangen, indem er entweder direkt vom Superuser – dem Systemadministrator – gestartet wird oder indem er eine Sicherheitslücke ausnutzt, die es ihm ermöglicht die Privilegien zu bekommen.
3. Aufgrund der Vielzahl von einsetzbaren Mailprodukten gibt es unter Linux i.d.R. nicht die Produktmonotonie, die die Ausbreitung der Viren erst ermöglicht hat.

### 4.3. Überwachung der Systemintegrität

Wenn es einem Eindringling gelingt, Systemdateien zu verändern, ergeben sich die folgenden Fragen:

1. Wie werden die Systemveränderungen bemerkt?
2. Was wurde am System verändert?
3. Welcher Schaden wurde angerichtet?

Dieses Thema wird unter Linux von Open Source Software Tools wie »Tripwire« oder »AIDE« behandelt. Diese Tools nehmen den Systemzustand auf, indem sie für jede relevante Datei einen MD5-Hash (vergleichbar einer Checksumme) berechnen und abspeichern. Später wird zyklisch überprüft, ob eine erneute Berechnung Unterschiede aufweist, die auf eine Veränderung hindeuten. Es ist dann die Aufgabe des Systemadministrators nachzuvollziehen, ob es sich um geplante Änderungen oder um Manipulationen handelt.

#### **4.4. Entdeckung von Angriffen**

Einem konkreten Einbruchversuch gehen fast immer Analysen potenzieller Sicherheitslücken voraus, die auf einen späteren Einbruchversuch hindeuten. Bei diesen Portscans werden bekannte Dienstadressen (Ports) angesprochen, in der Hoffnung eine Hintertür in das System zu finden. Für Linux gibt es eine ganze Reihe von Programmen, die solche Portscan Angriffe erkennen und warnen. Unter anderem enthält auch der Linux-Kernel einen solchen Detektor.

#### **4.5. Verschlüsselung**

Unter Linux gibt es eine einfache, leistungsfähige und kostenfreie Lösung, verschlüsselte Verbindungen zwischen Systemen herzustellen: Secure Shell (SSH).

Secure Shell ermöglicht die Ausführung von Kommandos auf entfernten Rechnern, das Kopieren von Dateien zwischen Rechnern und den Aufbau von Tunnel-Verbindungen, über die dann andere Protokolle gefahren werden können (wie z. B. POP zum Abholen von Mails und X11). Die ersten beiden Anwendungsfälle sind sicher auf Systemadministratoren beschränkt.

SSH kann auf unterschiedliche Verschlüsselungsalgorithmen (Blowfish, Triple DES, IDEA) und Authentisierungsverfahren (RSA) zurückgreifen, um einen Session-Key zu ermitteln, der für die Verschlüsselung der Verbindung benutzt wird.

Secure Shell gibt es sowohl in einer freien Version (OpenSSH <http://www.openssh.com/>) als auch in einer kommerziellen Entwicklung (<http://www.datafellows.com/products/ssh/>).

Mit den Open Source Software Produkten FreeSWan und PPTP können unter Linux auch VPNs (Virtual Private Networks) realisiert werden, mit denen mehrere Intranets über das Internet miteinander verbunden werden können. Mehr dazu in Abschnitt 6.3.

## 5. Wirtschaftlichkeit

Die Behörden und Dienststellen der Landesverwaltung sind nach den Vorschriften des Haushaltsrechts verpflichtet, sparsam zu wirtschaften. Für Wirtschaftlichkeitsberechnungen sind der Wirtschaftlichkeits-Leitfaden des FM und die Empfehlungen zur Durchführung von Wirtschaftlichkeitsberechnungen beim IT-Einsatz in der Bundesverwaltung zu Grunde zu legen<sup>7</sup>.

Da beim Einsatz von OSS keine Lizenzkosten anfallen, können im Einzelfall erhebliche Kosteneinsparungen erzielt werden. Durch den ressourcenschonenden Umgang der OSS mit der Hardware ist es nach Auffassung von Prof. Dr. Detlef Leipelt, KBSt<sup>8</sup> oft möglich, eingesetzte Hardware länger zu nutzen. Deshalb sei für die Wirtschaftlichkeitsanalyse ein Betrachtungszeitraum von 5 Jahren oder sogar länger sicher als angemessen zu betrachten.

Eine generelle Annahme der Wirtschaftlichkeit bei Einsatz von OSS ist wegen unterschiedlicher Rahmenbedingungen im Einzelfall nicht sachgerecht. Zur Bewertung schlägt Leipelt vor, einen WiBe-Kriterienkatalog zu entwickeln, der alle für eine Wirtschaftlichkeitsbetrachtung relevanten Punkte berücksichtigt und für den Einsatz von OSS die entsprechende Hilfestellung leistet.

Bis auf weiteres müssen daher im Falle des Einsatzes von OSS mit den bekannten Methoden dem zu erwartenden Nutzen die einmaligen und laufenden Kosten gegenübergestellt werden. Bei den einmaligen Kosten können dabei erfahrungsgemäß die Umstellungskosten, d.h. die Kosten der Datenübernahme, die Aus- und Fortbildungskosten für das Systempersonal sowie etwaige Schulungskosten für Anwender von erheblicher Bedeutung sein. Ferner kann ergänzend mittels einer Nutzwertanalyse eine Wirtschaftlichkeitsbetrachtung im weiteren Sinne durchgeführt werden, wenn nichtmonetäre Werte, z. B. Dringlichkeit, Strategie usw. zu berücksichtigen sind.

---

<sup>7</sup> Vgl. Nr. 10 der Standards des Landessystemkonzepts vom 15.05.00, GABI. S. 150, <http://www.verwaltungsreform-bw.de>

<sup>8</sup> Grundgedanken zu Wirtschaftlichkeitsbetrachtungen für den Einsatz von OSS, <http://linux.kbst.bund.de/ws-oss/vortraege/leipelt>

## 6. OSS–Einsatz in der Landesverwaltung Baden–Württemberg

### 6.1. Stand

Beim Einsatz von OSS in der Landesverwaltung Baden–Württemberg sind insbesondere die Standards des Landessystemkonzepts<sup>9</sup> und die Networking–Konzeption für die Landesverwaltung Baden–Württemberg i. d. Fassung vom 22.02.99 zu Grunde zu legen.

Danach ist Linux derzeit nicht als Betriebssystem für Großrechner zugelassen. Für Behörden– und Arbeitsplatzrechner in der Bürokommunikation (Office) kann Linux und andere OSS nur außerhalb des sog. Kernbereichs der Landesverwaltung eingesetzt werden. Dabei handelt es sich im Wesentlichen um die Finanzämter, verschiedene Behörden und Dienststellen des Ministeriums Ländlicher Raum und des Wirtschaftsministeriums. Im Kernbereich, d.h. bei allen anderen Behörden und Dienststellen sind für diese Aufgaben ausschließlich die Produkte und Techniken der Fa. Microsoft, insbesondere Windows, die Office–Programme, Arial als Schrifttyp, einheitliche mit Visual Basic Application (VBA) programmierte Vorlagen, Schnittstellen wie ODBC, OLE, DDE und MAPI sowie das NT–Filesystem (NTFS) als Landesstandard vorgeschrieben.

Für den Betrieb von Firewalls<sup>10</sup>, die Benutzerauthentifizierung zentral über existierendes X.500 mittels LDAP, die Verschlüsselung<sup>11</sup> mit PGP oder SSL V.3, den Betrieb von Anwendungs– oder von Web– und Intranet–Servern bestehen keine Festlegungen, die den Einsatz von Linux einschränken oder gar verhindern.

Eine formlose Umfrage bei den Mitgliedern des Arbeitskreises Informationstechnik (AK–IT) hat zum Einsatz von OSS folgenden aktuellen Stand ergeben:

Staats–, Innen–, Justiz–, Finanz–, Wirtschafts– und Wissenschaftsministerium sind mit einem Informationsangebot im Internet vertreten. Zum Einsatz kommt dafür ein externer Linux–Server mit Apache–Software. Die Informationsinhalte wurden unter der technischen Leitung der Medien– und Filmgesellschaft (MFG) in den Ministerien aufgebaut.

Im Bereich des Staatsministeriums, des Innenministeriums und des Sozialministeriums werden Firewalls mit Linux betrieben.

In der Innenverwaltung setzt das Zentrum für Kommunikationstechnik Linux für ein Firewall–Log–Host– und ein Firewall–e–Mail–Backup–System für Administratoren ein. Linux wird ferner für den Internet–DNS verwendet. Eine beachtliche Anzahl von Linux–Installationen gibt es im Bereich der Polizei für folgende Aufgaben: Host–Emulation mit Siemens Großrechnern (70), Router auf ausgedienten PC (200), DNS– und Sendmail–Mail–Server (55), teilweise auch Workgroup–Server (Samba), Timeservice für eine große Anzahl dezentraler Rechner, Internet–PC (150) und Firewalls (6). Ferner sind ein Web–Server mit Apache und Adabas D in Betrieb. Verschiedene Endgeräte werden unter Verwendung von VMware sowohl mit NT als auch mit Linux genutzt.

---

9 Vgl. Nr. 10 der LSK–Standards (a.a.O.), <http://www.verwaltungsreform–bw.de>

10 vgl. Nr. 7.8 der LSK–Standards (a.a.O.)

11 vgl. Nr. 7.7 der LSK–Standards (a.a.O.)

Bei den Finanzämtern ist im Rahmen der bundesweiten Fiscus-Programmierung die Einführung der Bürokommunikationssoftware StarOffice geplant.

Im Geschäftsbereich des Wirtschaftsministeriums setzt das Landesamt für Geologie, Rohstoffe und Bergbau Linux mit Apache für einen Internet-Web-Server ein. Ferner ist Linux Betriebssystem für einen Intranet-Name-Server, einen internen und externen Mail-Server sowie für File- und Print-Server in 5 Dienstgebäuden. Verwendet werden SuSE-Distributionen. Mehrere Arbeitsplätze des Erdbebendienstes sind unter Verwendung von Linux mit BK-Funktionen, Internetzugang und E-Mail-Funktion ausgestattet. An drei weiteren Arbeitsplätzen ist ebenfalls Linux im Einsatz, wobei in einem Fall durch das Programm VMware MS-Windows als Gastbetriebssystem genutzt werden kann. Ein Arbeitsplatzrechner wird mit FreeBSD betrieben. Linux-Systeme werden ferner für Netzwerkdienste eingesetzt. Die Erfahrungen mit Linux sind ausnahmslos sehr gut. Insbesondere die Stabilität und Effektivität sowie der äußerst geringe Wartungsaufwand des Betriebssystems überzeugen. Die Linux-Systeme arbeiten darüber hinaus ausgezeichnet mit den Sun-Systemen zusammen.

Es gibt Überlegungen, Software für Bürokommunikation auf der Basis von Linux zu testen. Geplante Fachanwendungen werden künftig verstärkt mit Internettechnologie unter Verwendung von OSS entstehen. Bei der Vermessungsverwaltung ist im Gegensatz dazu vorgesehen, die heute im Auskunft- und im Entwicklungsbereich vorhandenen Linux-PC (2 je Vermessungsamt/Dienststelle) im Rahmen der Vereinheitlichung der Betriebssystem-Landschaft zu Gunsten von Windows-NT abzulösen.

Beim Landesamt für Flurneuordnung und Landentwicklung im Geschäftsbereich des Ministeriums Ländlicher Raum werden Web-Server mit Linux und Apache, Firewalls und Name-Server auf der Basis von Linux eingesetzt.

Die Landesanstalt für Umweltschutz plant die Einrichtung von zwei Linux-Systemen mit Apache als Web-Server und für DNS noch in diesem Jahr. Zwei Testrechner mit SuSE Linux 6.4 und Red Hat Linux 6.2 sind in Betrieb. Beim Landesamt für Straßenwesen werden 47 Server mit Samba als File- und Print-Server, 1 Apache Web-Server, 1 Internet-Proxy-Server und 8 Server als Router jeweils mit Linux oder HP-Unix betrieben. Ferner befinden sich OSS-Tools im Einsatz, z. B. tcpdump, tkined zur Netzwerkanalyse. Geplant ist die Ausstattung von zwei weiteren Dienststellen mit Linux als File- und Print-Server, evtl. auch als Mail-Server sowie die Ausstattung von 120 Dienststellen mit Linux-Routern. Eine wichtige Rolle spielt Linux im Rahmen der Überlegungen für eine neue Serverkonzeption.

Im kommunalen Bereich wird mit Linux für Web-Server, Firewalls und Name-Server getestet.

Einen Überblick gibt Anlage II auf Seite 51.

## 6.2. Weitere Einsatzmöglichkeiten, Szenarien

### 6.2.1. Office-Lösungen für OSS Umgebungen

Derzeit gibt es mehrere vielversprechende Office-Lösungen für Linux, die einen Großteil der Anforderungen an ein Office-Paket erfüllen.

#### StarOffice™ von SUN Microsystems

<http://www.sun.com/staroffice>

StarOffice ist ein umfangreiches Office Paket, das für die wichtigsten Betriebssysteme zur Verfügung steht. Mittlerweile ist auch die kommerzielle Nutzung von StarOffice kostenlos, allerdings handelt es sich dabei nicht um eine Open Source Software, da der Quellcode in der aktuellen Version noch nicht frei verfügbar ist<sup>12</sup>. Ursprünglich wurde StarOffice von dem deutschen Unternehmen StarDivision entwickelt, das 1998 von SUN aufgekauft wurde. SUN bietet StarOffice für die Plattformen Windows, Unix und Linux an. Der Einsatz von StarOffice ist also nicht auf die Linux Plattform beschränkt.

Das StarOffice Paket enthält Komponenten zur Tabellenkalkulation, Textverarbeitung, zur Erstellung von Präsentation, Vektor- und Bitmap-Grafiken, Datenbanken und eine Terminverwaltung. Es gibt umfangreiche Filter für den Import und Export von Microsoft Office Dateiformaten, sowie zu den Produkten von Lotus und Corel. StarOffice verfügt über einen eigenen Desktop, der zusätzlich oder als alternativer Desktop eingesetzt werden kann. Weiterhin gibt es integrierte E-Mail, News- und Web-Funktionen. Vom Reifegrad und dem Funktionsumfang ist die aktuelle Version StarOffice 5.2 eine kostenfreie Alternative zu Microsoft Office.

#### Corel WordPerfect® 8 für Linux

<http://194.106.141.198/de/products/wp8.html>

Bei WordPerfect handelt es sich um ein kommerzielles Office Paket, das eine umfangreiche integrierte Funktionspalette enthält u.a.:

- Internet-Publisher
- Tabellenkalkulation
- Zeichen- und Diagrammfunktionen
- Versionsverwaltung

WordPerfect kann entweder aus dem Internet geladen oder als CD-ROM Version gekauft werden.

---

<sup>12</sup> Sun Microsystems hat inzwischen angekündigt, die StarOffice Spezifikation offenzulegen und den Quellcode unter der GNU Public License verfügbar zu machen.

## Office



<http://koffice.kde.org>

KOffice ist ein integriertes Office-Paket für KDE, das K Desktop Environment. KOffice wird unter Open Source Lizenzen herausgegeben. Derzeit befindet sich KOffice noch im Beta-Stadium, was bedeutet, dass noch nicht alle Funktionalitäten fehlerfrei sind. Die Fertigstellung der Version Koffice 1.0 wird für Herbst 2000 erwartet.

Das besondere an KOffice ist seine Komponenten basierte Architektur auf der Basis eines KParts genannten Komponenten-Modells. Diese Architektur ermöglicht es alle KOffice Komponenten untereinander zu kombinieren. Die Dateiformate basieren auf XML und sind vollständig dokumentiert. Alle KOffice Funktionalitäten sind über Skripte steuerbar.

KOffice 1.0 enthält die folgenden Komponenten:

*Kword* ist eine Rahmen-orientierte Textverarbeitung.

*KSpread* ist eine Tabellenkalkulation

*KPresenter* ist ein Präsentationsprogramm

*KIllustrator* ist ein Vektor-orientiertes Zeichenprogramm

*KImageShop* ist ein Bildverarbeitungsprogramm

*Katabase* ist die KOffice Datenbank.

*KFormula* ist ein Formel-Editor

*KChart* ist eine Anwendung für Diagramme

*KImage* ist ein Bildbetrachter

*KFilter* stellt Import- und Export-Filter zur Verfügung

KOffice verfügt derzeit noch nicht über einen Funktionsumfang, um in einer Bürokommunikationsumgebung eingesetzt werden zu können. Insbesondere die Verfügbarkeit von Import/Export-Filtern ist noch zu stark eingeschränkt. Aufgrund des vielversprechenden Ansatzes von KOffice und der Bedeutung die dieses Projekt in der Open Source Gemeinde hat, ist jedoch mittelfristig mit professionell einsetzbaren Lösungen zu rechnen.

## Einsatzbeispiel

Linux Systeme verfügen mit dem X11-Protokoll von vornherein über ein netzwerkfähiges Grafikprotokoll. Dabei läuft der X-Server<sup>13</sup> auf dem Arbeitsplatz-Rechner und nimmt Grafikrequests der auf dem Server laufenden Anwendungen entgegen. Die Benutzer müssen sich dafür auf dem Server anmelden, das X-Display durch Setzen eines Parameters auf ihren Arbeitsplatz umlenken und die Anwendung starten. Dieser Vorgang kann durch Systemeinstellungen und Login-Skripts vollständig automatisiert werden. Aufgrund dieser Eigenschaft ist Linux bestens als Thin-Client in Verbindung mit

---

<sup>13</sup> Ein freier X-Server wird im Open Source Projekt XFree86 entwickelt.

Applicationservern geeignet (Abbildung 2). Die Anzahl der Clients, die an einen – Applicationserver angeschlossen werden können, ist durch den Ressourcenbedarf der Anwendungen, die Kapazität des Servers und des Netzwerks begrenzt. An ein Intel Pentium III 800 SMP System mit zwei Prozessoren und 512 MB Hauptspeicher können über Switched Ethernet ca. 50 StarOffice Benutzer angeschlossen werden. Da es sich bei X11 um ein offenes Protokoll handelt, kann als Server übrigens auch ein beliebiges UNIX-System zum Einsatz kommen.

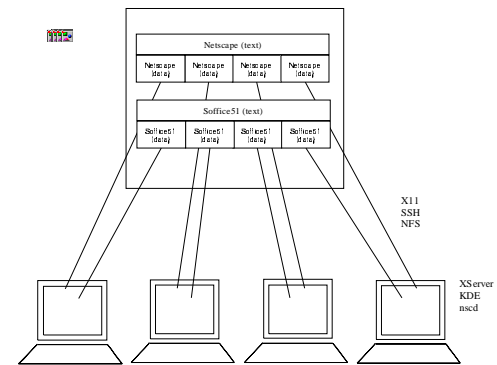


Abbildung 2: Thin-Clients

Der Vorteil dieser Architektur liegt im geringeren Administrationsaufwand und den niedrigen Anschaffungs- und Betriebskosten. Im Gegensatz zu den üblichen Thin-Client Konzepten, ist diese Linux-basierte Architektur sehr flexibel. Man kann sich durchaus dafür entscheiden, bestimmte Anwendungen lokal zu installieren – z. B. den Linux-Desktop KDE, der selbst eine X-Anwendung ist, und den Linux-Druckdienst, um auf lokal angeschlossenen Druckern auszudrucken.

In Kombination mit Secure Shell z. B. auf der Basis von OpenSSH lässt sich die Verbindung zwischen Client und Server transparent verschlüsseln, so dass auch eine hohe Abhörsicherheit gewährleistet werden kann.

## 6.2.2. Linux als Firewall

Quelle: [Firewalling unter Linux von Samuel Stähle \[7\]](http://www.pro-linux.de/work/server/andere/firewall.html)  
<http://www.pro-linux.de/work/server/andere/firewall.html>

Aufgrund seiner Leistungsfähigkeit und der Tatsache, dass Firewall Funktionalitäten bereits im Betriebssystemkern – dem Kernel – enthalten sind, bietet sich Linux als kostengünstige und sichere Alternative zu spezialisierten Firewall-Lösungen an. Solche Lösungen werden heute zunehmend sowohl von mittelständischen Unternehmen als auch von Abteilungen großer Konzerne eingesetzt.

Eine Firewall sollte die einzige Schnittstelle zwischen einem internen Netz (hinter dem Firewall) und einem externen Netz (oftmals dem Internet) bilden.

Die folgenden Aufgaben sollte eine Firewall erfüllen:

- Angriffsversuche aus anderen Netzen (andere LANs oder dem Internet) abwehren und dem Administrator des angegriffenen Netzes melden
- die übertragenen Daten auf Viren und andere unerwünschte Inhalte prüfen, und diese herausfiltern
- Die Netzwerkadressen der internen Netze nach außen verbergen
- sich für die Benutzer der angeschlossenen Netze transparent verhalten
- beliebig viele Netzwerksegmente unterstützen

- fernadministrierbar sein
- ausfallsicher sein

### **Linux-Firewall als Paketfilter oder Screening-Router**

Die Linux-Firewall ist ein leistungsfähiger Filter für IP-Pakete. Anhand von Regeln, die die Quell- und Zieladresse, die Portnummern, den Pakettyp, das Netzwerkinterface und die Richtung auswerten, wird entschieden, ob ein Paket die Firewall passieren darf, oder nicht.

#### Masquerading und Network Address Translation (NAT)

Eine wichtige Funktion einer Firewall ist das Verbergen der internen Netzwerkstruktur nach außen. Bei einer an das Internet angeschlossenen Firewall muss das äußere Netzwerk-Interface der Firewall über eine offizielle, registrierte Internetadresse angesprochen werden können. In allen Paketen, die aus dem internen Netz in das äußere Netz verschickt werden, ersetzt die Firewall die interne Quelladresse durch die eigene offizielle IP-Adresse. Bei aus dem Internet kommenden Paketen übersetzt sie die Zieladresse durch die IP-Adresse des Hosts im eigenen Netz, der die Verbindung aufgebaut hat. Dieser Vorgang, bei dem die Firewall als einziger IP-Knoten des internen Netzes nach außen sichtbar ist, wird als IP-Masquerading bezeichnet. Es ermöglicht die Anbindung vieler Rechner an das Internet mit nur einer einzigen offiziellen IP-Adresse.

Bei IP-Masquerading, das eine n:1-Abbildung von IP-Adressen darstellt, handelt es sich um eine Sonderform der Network Address Translation (NAT), bei der eine n:m-Abbildung erfolgt.

#### Dienst-Weiterleitung – Port Forwarding

Eine Linux-Firewall ist in der Lage, alle Anfragen an einen bestimmten Dienst auf einen anderen Rechner umzuleiten, der sich im internen Netz hinter der Firewall befindet. Die Rechner im Internet bemerken dabei nicht, wie deren IP-Pakete hinter der Firewall behandelt werden. Da Dienste unter Unix über sogenannte Ports angesprochen werden, spricht man in diesem Zusammenhang von »Port Forwarding«.

### **Application-Level-Gateways**

Paketfilter, wie die Firewall im Linux-Kern, haben immer dann potenzielle Sicherheitsprobleme, wenn eine Sitzung mehrere Verbindungen benötigt und dafür temporäre, nicht deterministische Ports verwendet werden. Bekannt sind solche Probleme z. B. bei FTP, IRC und pcAnywhere. Um diese Verbindungen zuzulassen, müssten die Regeln weiter gefasst werden als aus sicherheitstechnischen Überlegungen heraus wünschenswert ist. Man müsste eigentlich vor jedem solchen Verbindungsaufbau den Paketfilter umkonfigurieren. Das ist von Hand nicht praktikabel. Ein sogenanntes Application-Level-Gateway auch Application-Proxy genannt, kann Regeln jedoch dynamisch einfügen und entfernen, indem das zugrunde liegende Protokoll (z. B. FTP) interpretiert wird und die nötigen Änderungen an den Filterregeln automatisch durchgeführt werden.

Application-Level-Gateways sind oftmals die beste Möglichkeit, das interne Netz vor Angriffen zu schützen, die ein Paketfilter nicht erkennen kann. Ein allgemein bekanntes Beispiel ist der E-Mail Dienst, bei dem Nachrichten über das SMTP Protokoll vom Internet an einen Mailserver im internen Netz durch den Firewall durchgelassen werden müssen. Ein Paketfilter, der nur die Header-Information der IP-Pakete auswerten kann, ist nicht in der Lage zu erkennen, ob der Inhalt eines Pakets Teil eines E-Mail Virus ist. Das kann nur ein Proxy, der das Application-Protokoll kennt und im Fall von E-Mail feststellen kann, welcher Teil der Mail ein Anhang ist, der durch einen Virenschanner überprüft werden muss.

Unter Linux stehen Application-Level-Gateways für die gebräuchlichsten Protokolle als nachladbare Kernel-Module zur Verfügung.

### **Warum eine Linux-Firewall?**

#### Preis/Leistungs-Verhältnis

Ein bedeutendes Argument für den Einsatz von Linux als Firewall ist das ausgezeichnete Preis/Leistungs-Verhältnis. Verstärkt wird die Kostenersparnis noch dadurch, dass aufgrund des sparsamen Umgangs mit den Systemressourcen oftmals ausgediente Altsysteme einer Verwendung als Komponente einer Firewall zugeführt werden können.

#### Anpassbarkeit

Jede Firewall ist ein sicherheitskritisches System, auf dem ein Höchstmaß an Sicherheit nur erreicht werden kann, wenn nur die absolut erforderlichen Dienste auf dem System zur Verfügung gestellt werden. Jeder unnötige Dienst stellt eine potenzielle Sicherheitslücke dar.

Da Linux auf einem monolithischen Kernel basiert, der mit allen Programmquellen ausgeliefert wird, ist es ohne großen Aufwand möglich, einen speziell auf die eigenen Anforderungen zugeschnittenen Kernel zu bauen. Damit ist von vornherein ausgeschlossen, dass der Betriebssystemkern mit für diesen Einsatzzweck überflüssigen Funktionalitäten belastet ist, die im Fall einer Firewall sogar ein Sicherheitsrisiko bilden können.

#### Monolithischer Kernel

Im Gegensatz zu Betriebssystemen, die auf einer modularen Microkernel Architektur basieren, ist Linux durch seinen monolithischen Kernel nicht darauf angewiesen, Funktionen von Subsystemen dynamisch nachladen zu müssen – obwohl auch dies möglich ist. Damit kann ausgeschlossen werden, dass ein Einbrecher auf dem System durch Austausch von nachladbaren Modulen dem Kernel trojanische Pferde unterschiebt. Ein Hacker müsste in diesem Fall den kompletten Kernel austauschen.

#### Verifizierbarkeit

Da die Linux-Quellen öffentlich verfügbar sind, besteht prinzipiell die Möglichkeit, das Programmverhalten anhand des Quellcodes zu verifizieren. Natürlich ist kein Einzelner in der Lage, 20 Millionen Zeilen Quellcode auf Ihre Korrektheit zu überprüfen. Da der Linux

Quellcode jedoch der Allgemeinheit zur Verfügung steht, gibt es mehrere tausende von Entwicklern, denen es möglich ist, den Code zu überprüfen.

#### Einsatzbeispiel

In einer typischen Firewallkonfiguration eines kleinen Unternehmens oder einer Abteilung, wird die Verbindung nach außen (meist dem Internet) über einen Router mit Paketfilter-Funktion hergestellt. Das Firewall-Gateway befindet sich in der DMZ – der demilitarisierten Zone – einem internen Subnetz, das nur für bestimmte Dienste direkt von außen erreichbar ist. Der Router sorgt durch seine Filterregeln dafür, dass das interne Netz nicht von außen erreichbar ist. Die Aufgabe des Linux Firewall-Gateways ist die Vermittlung von Diensten von außen in das interne Netz. Typischerweise handelt es sich um einen Mail-Relay, also einem Mailserver, der als sogenannter Mail Transfer Agent (MTA) Mails entgegennimmt und an die internen Empfänger weiterleitet. Die gleiche Aufgabe übernimmt das Gateway auch für ausgehende Post. Es fungiert also im besten Sinne als Application-Proxy für den E-Mail Service. Da das Gateway von außen direkt erreichbar ist, müssen auf diesem System alle Vorkehrungen getroffen werden, um Einbruchversuche zu entdecken und zu verhindern. Für Linux existieren eine Vielzahl von Sicherheits-Werkzeugen, die zu diesem Zweck eingesetzt werden können (siehe auch [8]).

In einer sehr häufig anzutreffenden Variation dieser Konfiguration wird auf einen eigenen Firewall-Router verzichtet und dessen Routing- und Paketfilter-Funktion ebenfalls vom Linux-Gateway übernommen. Diese Konfiguration hat ein hervorragendes Preis/Leistungsverhältnis und ist je nach eingesetzter Hardware gut für kleinere bis mittlere Netze geeignet.

### **6.2.3. Samba als File/Printserver**

Linux kann vielerlei Protokolle und Datenformate interpretieren. Insbesondere soll hier die Möglichkeit des Datenaustauschs mit Microsoft Betriebssystemen beleuchtet werden. Dabei spielt das Samba-Projekt eine zentrale Rolle (<http://de.samba.org/samba/samba.html>).

#### **Das SMB Protokoll und Samba**

Zur rechnergestützten Kommunikation über ein Netzwerk wurde von Microsoft und IBM das sogenannte Server Message Block (SMB) Protokoll entwickelt. Seit DOS Version 3.0 dient dieses Protokoll dem Datenaustausch zwischen Microsoft basierten Systemen mit Unix Servern über ein TCP/IP Netzwerk. In aktuellen Windows Versionen wird ein überarbeitetes Protokoll namens CIFS (Common Internet File Standard) statt des bisherigen SMB Protokolls eingesetzt.

Die freie Implementierung des SMB Protokolls auf verschiedenen Unix Plattformen – insbesondere unter Linux – ist als Projekt Samba bekannt. Samba wurde von Andrew Tridgell in Canberra, Australien, ins Leben gerufen. Tridgell ist noch immer der führende Entwickler des Projekts und koordiniert die weltweit tätigen freien Entwickler. Der ursprüngliche Name des von Tridgell geschriebenen Fileservers war SMB Server. Aus

lizenzrechtlichen Gründen konnte dieser Name allerdings nicht weiter verwendet werden. Als alternativer Name für das Projekt wurde Samba gewählt.

Im RFC 2708 befindet sich die grundlegende Beschreibung des SMB Protokolls. Weite Teile des Quellcodes von Samba wurden durch sogenanntes Reverse-Engineering der SMB und Windows Domain Service Funktionalität nachgebildet. Da die Dokumentation dieser Funktionalitäten nicht vollständig ist, kann auch nicht garantiert werden, dass Samba allen denkbare Features der Netzkommunikation aller Microsoft Betriebssysteme beherrscht. Allerdings ist Samba seit mehreren Jahren praxistauglich und wird inzwischen weltweit an den unterschiedlichsten Stellen eingesetzt. Momentan nicht unterstützte Funktionalitäten von Samba sind beispielsweise die Backup Domain Controller, Secondary WINS Server und Local Backup Browser Dienste.

### **Einsatzbereiche von Samba**

Die Integration von Linux mit den Microsoft Betriebssystemen Windows (3.11, 95, 98, NT 3.51, NT 4.0, 2000) kann über verschiedene Serverdienste geschehen. Dabei werden in der Praxis sehr häufig die File- und Printserver-Dienste über das SMB Protokoll eingesetzt. Linux kann sowohl beim File- als auch beim Printsharing beide möglichen Aufgaben des Clients und des Servers übernehmen. Windows Maschinen können auf einen Linux Fileserver zugreifen und dort Daten speichern und lesen. Linux Maschinen können dagegen auch von Windows Servern zur Verfügung gestellte Shares einhängen und darauf lesend sowie schreibend zugreifen.

Für alle diese Netzwerkzugriffe zwischen Windows und Linux Maschinen gibt der Linux Rechner vor, selbst ein Windows Rechner zu sein. Linux Server identifizieren sich durch Samba auf den an sie angeschlossenen Microsoft Rechner als Windows NT 4.2. Die von Samba erreichte Transparenz in der Netzwerkfunktionalität führt in der Praxis dazu, dass sowohl Linux Server als auch Clients vom Microsoft-Anwender nicht von anderen Microsoft Maschinen unterschieden werden. Der Anwender muss insbesondere keine andersartigen Bedienerfunktionalitäten erlernen sondern arbeitet wie in einem reinen Microsoft basierten Netzwerk.

### **Sambaserver**

Ein Linux Rechner kann mit Hilfe der Samba Software viele Dienste der Microsoft Welt anbieten. Darunter fallen unterschiedliche Services eines typischen Microsoft basierten Netzwerkes die im folgenden aufgeführt sind:

- Fileserver
- Printserver
- Primary Domain Controller Dienst
- Domain Master Browser Dienst
- Local Master Browser Dienst
- Primary WINS Server
- Windows 95/98 Authentifizierung

Diese oben aufgeführten Dienste werden nicht durch ein einziges Programm ausgeführt. Im Falle eines Samba Servers werden auf dem Linux Rechner zwei hintergrundaktive Programme (sogenannte Deamons) gestartet.

Der Daemon `smbd` ist für die Verwaltung der zu Verfügung zu stellenden Ressourcen wie File-, Print- und Browserservices verantwortlich. Weiterhin wird über `smbd` die Authentifizierung des Benutzers sowie der Datenaustausch über das SMB-Protokoll abgewickelt.

Der Nameservice des Netzwerks wird über den zweiten aktiven Daemon `nmbd` implementiert. Alle von Clients auftretenden WINS und NetBIOS Namensanfragen werden hierbei abgedeckt.

Ein Sambaclient – eine Linux Maschine welche auf Microsoft Maschinen zugreifen möchte – enthält dagegen mehrere Programme die vom Benutzer direkt oder über den Umweg einer grafischen Benutzeroberfläche aufgerufen werden können. Darunter fallen die Programme `smbclient`, `smbtar`, `nmblookup`, `smbpasswd` und `smbstatus`. Diese ermöglichen den Datenaustausch zwischen den unterschiedlichen Plattformen als auch die administrative Abwicklung von Passwortänderung und Statusabfrage des evtl. auf der selben Maschine laufenden Samba Servers.

#### **Administration eines Samba Servers**

Die Administration eines Samba Servers muss nicht in dem von Unix Betriebssystemen bekannten Kommandozeilenmodus geschehen. Im Kommandozeilenmodus kann der Server direkt über das simple Editieren der Konfigurationsdatei `smb.conf` im Textmodus manipuliert werden.

Ebensogut kann über diverse GUIs diese Datei in grafisch aufbereiteter Form bearbeitet werden. Eines der bekanntesten Samba Administrations-GUIs ist SWAT. SWAT ist ein Programm, welches die Samba Server Administration über einen beliebigen HTML fähigen Browser wie beispielsweise Netscape Navigator durchführt. Der Vorteil der Trennung von Programm und Visualisierung zeigt sich bei der Betrachtung mehrerer im Netzwerk verteilter Samba Server. Jeder einzelne Server kann über eine HTTP-Verbindung (Standardmäßig mit Port 901) von einem einzigen Rechner aus administriert werden. SWAT kann hier sowohl zur reinen Kontrolle der Bereitschaft des Servers als auch zum interaktiven Bearbeiten der Konfiguration dienen.

#### **Einsatzbeispiel**

In einem typischen Einsatzfall kann ein Samba Server, der die oben angesprochenen Dienste bietet, für den Benutzer transparent einen bestehenden Windows File- und Printserver ersetzen. In vielen Firmen wurden und werden Windows NT Server entlastet bzw. ersetzt durch Samba Server auf Linux Basis. Diese kostengünstige Alternative zu rein Microsoft basierten Netzen ist seit einiger Zeit im Einsatz. Wie oben erwähnt ist der Austausch eines Microsoft Servers durch einen Samba Server für den Anwender völlig transparent. Daher fallen auch keinerlei Schulungs- bzw. Weiterbildungskosten in den Betrieben an.

#### 6.2.4. X.500 Verzeichnisdienste und LDAP

Verzeichnisdienste – neudeutsch auch Directoryservices genannt – spielen eine zentrale Rolle innerhalb der IT-Infrastruktur größerer Organisationen.

Mit größerem Erfolg als in anderen Bereiche, hat der OSI<sup>14</sup> Standard X.500 nicht nur die theoretischen Grundlage für Verzeichnisdienste gelegt, sondern es gibt auch eine Vielzahl von Produkten, die ihre Leistungsfähigkeit in der Praxis beweisen. Der OSI Standard X.500 ist die weitestgehende offene Definition eines globalen Verzeichnisdienstes. X.500 Produkte werden daher inzwischen nicht nur für die Realisierung elektronischer Konzernadressbücher verwendet, sondern sind aufgrund der offenen Definition in der Lage, nahezu beliebige Informationen für große Netzwerke bereitzustellen. Bahnbrechend war der Teilstandard X.509, der die Voraussetzung für Zertifikate auf der Basis asymmetrischer Kryptografie geschaffen und damit die Realisierung von Public Key Infrastrukturen (PKI) erst ermöglicht hat.

Die Schnittstelle, die X.500 für den Zugriff auf die Directory System Agents (DSA) definiert, ist das Directory Access Protocol (DAP), das von den Directory User Agents (DUA) verwendet wird, um mit den DSAs zu kommunizieren. Dieses Protokoll hat jedoch aufgrund seiner Komplexität und den damit verbundenen Kosten auf der Clientseite keine große Verbreitung gefunden.

Da X.500 Verzeichnisdienste aber auch für die Internetgemeinde aufgrund ihrer Generalität von großem Interesse waren, hat man Anfang der 90er Jahre damit begonnen, Zugriffsmöglichkeiten auf der Basis von TCP/IP Protokollen zu entwickeln. Die Abbildung des DAP auf ein einfacheres TCP/IP Protokoll führte schließlich zum Lightweight Directory Access Protocol (LDAP). LDAPv2 (RFC 1777) wurde von der University of Michigan als freie Implementierung von LDAP durchgeführt. Inzwischen wird im Open Source Projekt OpenLDAP (<http://www.openldap.org/>) an der Implementierung von LDAPv3 (RFC 2251) gearbeitet, das derzeit in einer Betaversion verfügbar ist<sup>15</sup>. Praktisch alle DSAs verfügen über einen LDAP-Dienst, der meist auf den Quellen der Open Source Software beruht.

Ein wesentlicher Vorteil von LDAP ist, dass keine Änderungen an den DSAs notwendig sind, da der LDAP Service Daemon (ldapd) als Middleware zwischen dem Client und dem DSA arbeitet. Ein weiterer Vorteil besteht darin, dass Clients über den vorhandenen TCP/IP-Stack ohne großen Protokolloverhead ein Directory abfragen können.

Der große Erfolg von LDAP als Middlewareprotokoll hat dazu geführt, dass bereits seit LDAPv2 ein Standalone LDAP Server (SLAPD) verfügbar ist, der als Backend nicht mehr auf ein X.500 Directory angewiesen ist, sondern über eigene offengelegte Schnittstellen u.a. auch an relationale Datenbankmanagementsysteme (RDBMS) angebunden werden kann.

Damit wird LDAP zu dem Standardzugriffsprotokoll für Informationsabfragen im Intranet und Internet. Neben X.500 unterstützen mittlerweile auch proprietäre Informationsdienste

<sup>14</sup> OSI Steht in diesem Zusammenhang für Open System Interconnection, bekannt durch das OSI Referenzmodell, das durch ISO und der ITU-T (früher CCITT) definiert wurde.

<sup>15</sup> OpenLDAP ist ein von SuSE gefördertes Open Source Projekt.

LDAP Zugriffe: Lotus Notes Adressbuch ab Version 4.6, Novell Directory Services (NDS), Microsoft Active Directory (ADS), sowie spezielle Verzeichnisdienste wie der Netscape Directory Server, der SUN Directory Server oder IBMs DSSeries LDAP Directory Server.

Dass LDAP auf dem besten Weg zu einem vollständigen Internet Directory ist, zeigt sich auch an der Definition einer LDAP-URL (RFC 1738). Damit kann von einem Browser wie z. B. dem Netscape Navigator 4.7 eine LDAP Abfrage durchgeführt werden. Ein Link wie z. B. *ldap://ldap.meine-domain.de/cn=Nachname Vorname* führt zu einer Abfrage auf einem LDAP-Server, deren Ergebnis vom Browser in einer HTML-Seite dargestellt wird.

LDAP ermöglicht den einheitlichen Zugriff auf Informationen aus verschiedensten proprietären Datenquellen, für die sonst jeweils ein eigener proprietärer Client erforderlich wäre.

### **Einsatzbeispiel Authentisierung**

Ein typisches Problem in Netzen ist die Verwaltung und Authentifizierung von Benutzern. Ursprünglich gab es nur die Möglichkeit, Benutzerinformationen wie z. B. Login-Name und Passwort lokal auf den Arbeitsplatzrechnern zu speichern. Wenn Benutzer auf mehreren Rechnern arbeiten wollten, war es erforderlich, diese Informationen zu kopieren, was bereits in kleineren Netzen fehleranfällig und unpraktikabel ist. Daher wurden Dienste entwickelt, die eine Benutzerverwaltung auf einem Arbeitsgruppenserver zur Verfügung stellen wie z. B. Network Information System (NIS) und Kerberos unter UNIX und Domains unter Windows NT. Diese Dienste sind sehr einfach, mit Ausnahme von Kerberos teilweise unsicher und sehr spezialisiert. Mit der Verfügbarkeit von Verzeichnisdiensten gibt es nun die Möglichkeit, vorhandene oder noch zu schaffende Unternehmens-Directories auch für die Authentisierung zu nutzen.

Linux verfügt mit Pluggable Authentication Modules (PAM) über eine Schnittstelle, die es ermöglicht eine Vielzahl von Authentisierungsverfahren zu konfigurieren. Unter anderem gibt es auch ein LDAP-PAM, das die Standardauthentisierungsmethode des Betriebssystems durch eine Directory Bind Operation ersetzt. Eine Bind Operation stellt eine Kommunikationsbeziehung zwischen einem Client und dem Directory her. Dazu können die Authentisierungsfunktionen des Directories verwendet werden. Der Vorteil dieses Verfahrens liegt auf der Hand, wenn bereits ein Directory vorhanden ist, das personenbezogene Informationen wie Namen, Telefonnummern, E-Mail-Adressen u.s.w. enthält.

### **Einsatzbeispiel: LDAP als einheitliche Schnittstelle zu vorhandenen Diensten**

Der Zugriff auf vorhandene X.500 Verzeichnisdienste, sowie auf Datenbanken mit oder ohne LDAP Unterstützung, kann mit Hilfe eines Standalone-LDAP-Servers vereinheitlicht werden. Der SLAPD verfügt über Schnittstellen, die die Anbindung unterschiedlicher Datenquellen (Backends) erlauben. Damit kann gegenüber den Clients LDAP als generelles Abfrageprotokoll eingehalten werden. Darüber hinaus ermöglicht diese Methode eine für den Client transparente Aufspaltung von Abfragen auf verschiedene Datenquellen. Es lassen sich somit neue Sichten auf Daten erzeugen, ohne dass

Änderungen an den Datenquellen vorgenommen werden müssen.

### 6.3. Verschlüsselung: Mail-V., Platten-V. und Digitale Signaturen

Für die private Kommunikation werden Verschlüsselungsverfahren immer interessanter. Die Rechenleistung von Computerchips verdoppelt sich, wie vom sogenannten Mooreschen Gesetz beschrieben, seit den 70er Jahren etwa alle 18 Monate. Aufgrund der dadurch inzwischen erhältlichen Rechenleistung auf PCs wird Datenverschlüsselung für den Privatanwender inzwischen praktikabel.

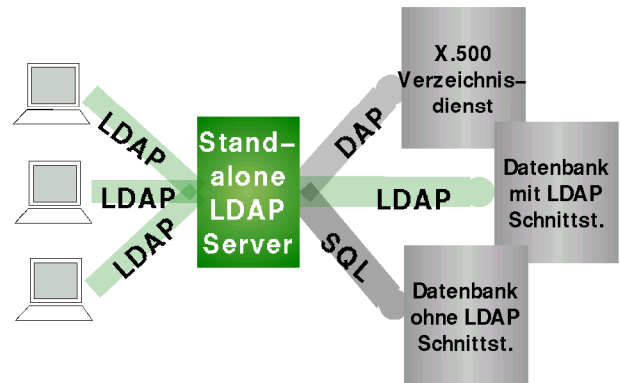


Abbildung 3: LDAP als allgemeine Schnittstelle

#### 6.3.1. Begriffsbildung

Verschlüsselung ist der Prozess bei welchem *Klartext* in sogenannten *Ciphertext* überführt wird. Dabei werden spezielle mathematische Funktionen (Verschlüsselungsalgorithmen) und ein *key* genanntes Verschlüsselungspasswort benötigt. Entschlüsselung ist der oben beschriebene Prozess in inverser Reihenfolge. Auch hier wird ein *key* genanntes Entschlüsselungspasswort benötigt.

Man unterscheidet zwei grundlegende Verschlüsselungsverfahren anhand der Anzahl der verwendeten *keys*. Beim symmetrischen Schlüsselverfahren (*private key cryptography*) wird im Ver- und im Entschlüsselungsvorgang derselbe Schlüssel benutzt. Dagegen wird in asymmetrischen Verschlüsselungsverfahren (*public key cryptography*) zwei verschiedene Schlüssel zum Ver- und entschlüsseln der Nachricht verwendet.

Zusätzlich zur Verschlüsselung taucht häufig das Problem der Authentifizierung auf. Dabei muss die Identität der Kommunikationspartner zweifelsfrei sichergestellt werden. In diesem Zusammenhang muss der Begriff der Digitalen Signatur gesehen werden. Prinzipiell liegt allerdings das gleiche Problem wie bei der Verschlüsselung zugrunde und wird auch über ähnliche Methoden behandelt.

#### 6.3.2. Algorithmen

Die meisten Algorithmen bestehen aus n-fach wiederholten XOR Verknüpfungen. Um die Invertierbarkeit der Algorithmen möglichst auszuschließen werden zusätzlich modulo-Operationen eingesetzt.

Es gibt eine prinzipiell nicht entschlüsselbare Methode. Diese Methode ist als »one time pad« Methode bekannt. Dabei wird der Klartext mit einem nur ein einziges Mal verwendeten Schlüssel chiffriert. Allerdings muss Sender und Empfänger über sehr viele identische Schlüssel verfügen. Diese Methode wird beispielsweise beim »Roten Telefon« zwischen dem russischen und amerikanischen Präsidenten bzw. in der Kommunikation zwischen Botschaften und Außenministerien eingesetzt. Ohne Kenntnis des jeweils gültigen Schlüssels kann eine chiffrierte Nachricht nicht rekonstruiert werden.

Im Wesentlichen gibt es zwei weitere Verschlüsselungssysteme. Sie sind im weiteren beschrieben.

#### Private Key Systeme

Im folgenden sind die heute gebräuchlichen *private key* Systeme aufgelistet:

<b>System</b>	<b>Beschreibung</b>	<b>Key [Bit]</b>
ROT13	Einfacher Usenet Algorithmus – Cäsar cipher – unsicher	–
crypt	Ursprüngliches UNIX Programm – stream cipher – unsicher	variabel
DES	Von NIST und IBM in den 70ern entwickelt – block cipher – unsicher	56
RC2	Block cipher von Ronald Rivest – proprietär	1–2048
RC4	Stream cipher von Ronald Rivest – proprietär	1–2048
RC5	Block cipher von Ronald Rivest (1994) – proprietär	variabel
IDEA	In PGP benutzt – patentiert	128
skipjack	Algorithmus von der NSA für den sog. Clipper chip entwickelt – GPL	80

#### Public Key Systeme

<b>System</b>	<b>Beschreibung</b>	<b>Key [Bit]</b>
Diffie–Hellman	Key Austausch Protokoll – patentiert	variabel
RSA	Public Key Verschlüsselung und digitale Signaturen	variabel
EIGamal	Public key Verschlüsselung und digitale Signaturen	variabel
DSA	Digitale Signaturen – patentiert	512–1024

#### 6.3.3. Vorteile der Open Source Verschlüsselung

Im praktischen Einsatz für die verschlüsselte Kommunikation über Computernetzwerke wird als *public key* Verfahren meist ein Hybrid aus beiden oben besprochenen Schlüsselverfahren benutzt. Dabei wird zu Beginn der Verbindung über einen asymmetrischen Schlüssel ein symmetrischer Schlüssel für die Kommunikation ausgehandelt. Da asymmetrische Schlüssel sehr rechenintensiv – dafür allerdings noch schwerer zu brechen – sind, wird die Kommunikation anschließend über einen symmetrischen Schlüssel gesichert. Der symmetrische Schlüssel wird in vorbestimmten Zeitintervallen während der Verbindung durch einen neuen ersetzt.

In der Anfangszeit der computerbasierten Kryptografie wurde nach dem als »security by obscurity« bekannten Modell verfahren. Danach wurden sowohl die Algorithmen als auch die Schlüssel geheim gehalten, um sich vor Missbrauch zu schützen. Inzwischen wurde

dieser Ansatz weitgehend aufgegeben. Inzwischen werden Verschlüsselungsalgorithmen schon vor ihrer eigentlichen Implementierung öffentlich publiziert. Dadurch können Schwachpunkte des Algorithmus deutlich schneller erkannt werden. Auf diese Weise ergibt sich die Sicherheit der Verschlüsselungsverfahren einzig aus der Geheimhaltung der Schlüssel und auf der Faktorisierbarkeit großer Zahlen.

#### **6.3.4. Verschlüsselungsprogramme unter Linux**

Die oben beschriebenen Verschlüsselungsalgorithmen sind als Bestandteile vieler verschiedener Programme auf allen möglichen Computerarchitekturen vorzufinden. Im Spezialfall sollen hier die in der SuSE Linux Distribution mitgelieferten Programme betrachtet werden.

##### **Verschlüsselte Kommunikation zwischen Rechnern**

Um die altbekannten und unsicheren Fernzugangsprogramme *rlogin*, *rsh* und *telnet* zu ersetzen eignen sich die Pakete *ssh* und *openssh*. Das Programm *ssh* von Tatu Ylonen war bis zur Version 1.X freie Software und wird seit der Version 2.0 als kommerzielles Produkt vertrieben. Daher ist das in der SuSE Linux Distribution mitgelieferte Paket die Version 1.2.27. Dabei ist *openssh* der Vorzug zu geben, da dieses Paket auch Kommunikation mit der *ssh* Version 2 beherrscht.

Für den Aufbau von VPNs (*Virtual Private Networks*) können die Pakete *CIPE* und *FreeSWan* benutzt werden.

##### **Mailverschlüsselung und Digitale Signaturen**

Wie auch auf Microsoft Plattformen bekannt, existiert auch unter Linux das Paket PGP (*Pretty Good Privacy*) von Philip R. Zimmermann. Allerdings ist in der SuSE Linux Distribution nur die Version 2.6.3i enthalten, welche die letzte Freeware-Version von PGP darstellt. Da spätere Versionen von PGP zusätzliche Schlüsselverfahren nutzen, kann eine Kommunikation zwischen PGP auf unterschiedlichen Plattformen der vorherigen Abstimmung und evtl. neuer Schlüsselgenerierung bedürfen.

Alternativ kann auch das Paket GPG (*Gnu Privacy Guard*) eingesetzt werden. Dieses Programm ist eine Implementation nach dem OpenPGP (RFC 2440) Standard. Es kann sowohl mit PGP Version 2 als auch Version 5 verschlüsselte Mitteilungen entschlüsseln.

Beide Verschlüsselungsprogramme arbeiten mit asymmetrischen Schlüsseln und verschiedenen Verfahren und können zudem digitale Signaturen erzeugen.

##### **Plattenverschlüsselung**

Da aus technischen Gründen Plattenverschlüsselung eine Modifikation des Betriebssystemkerns bedarf, wird in der SuSE Linux Distribution kein Plattenverschlüsselungsprogramm mitgeliefert. Allerdings kann ohne weiteres ein Plattenverschlüsselungsprogramm wie *ppdd* oder *cryptofs* auf ein entsprechendes Linux System installiert werden.

## **6.4. Web- und Intranet-Server**

Informationsaustausch kann sehr effizient durch Webserver im öffentlichen Internet wie auch im internen Intranet durchgeführt werden. Hier soll nun ein Überblick gegeben werden über die Eigenschaften und Möglichkeiten von Webservern auf Linux Basis.

Um den Informationsaustausch innerhalb der Landesverwaltung, bestehend aus den einzelnen Behörden, auf organisierte Art elektronisch darstellen zu können, werden Intranetserver eingesetzt. Als Intranetserver wird dabei die abgeschlossene innere Kommunikation innerhalb und auch zwischen den einzelnen Behörden bezeichnet. Das Intranet wird durch das Landesverwaltungsnetz beziehungsweise eines Teilnetzes davon festgelegt.

Die Kommunikation zwischen den Landesbehörden und der Öffentlichkeit wird auch in Zukunft immer mehr über Webserver stattfinden. Hier sollen ausschließlich für die Öffentlichkeit bestimmte Informationen abgelegt werden. Diese Server sind allerdings vom öffentlichen Internet wie auch vom internen Intranet aus erreichbar. Diese Server sind besonders zu schützen, um ein unerwünschtes Eindringen von außen in das Landesverwaltungsnetz zu verhindern.

### **6.4.1. Intranetserver**

Die bisherigen Intranetserver der Landesbehörden bestehen aus zwei grundsätzlich unterschiedlichen Lösungen. Eine Version der Intranetserver wurde ausschließlich für den internen Dokumentenaustausch eines Bereiches konzipiert. Dabei werden auf einem Fileserver spezielle Ablagen nach Themen- oder Benutzergruppen geschaffen. Diese können von bestimmten Nutzergruppen mit unterschiedlichen Berechtigungen angesprochen werden. Solche bereits existierenden Intranetserver können problemlos beibehalten werden, da sie dem Funktionsprinzip nach reine Fileserver darstellen (siehe dazu den Abschnitt 6.4 Samba als File/Printserver).

Die zweite Art eines Intranetserver besteht aus einem Server, der HTML Dokumente zur Verfügung stellt. Ein typischer Server hierfür wäre mit dem Apache Server (siehe auch Abschnitt 3.6.2 Internetserver) gegeben. Dieser Intranetserver entspricht bis auf das Entfallen der Notwendigkeit zur Absicherung durch Proxys vollständig dem Webserver im nächsten Abschnitt.

### **6.4.2. Webserver**

Die Software Apache ist gegenwärtig weltweit der am häufigsten eingesetzte Webserver. Auch andere frei erhältliche Webserver wie beispielsweise Roxen oder Aolserver konnten die Vorherrschaft von Apache auf diesem Gebiet bisher nicht brechen.

#### **Einsatz von Webservern**

Bestimmte Bereiche eines Webserverns können mit entsprechend gewählten Berechtigungen nur für eine begrenzte Gruppe an Benutzer zugänglich gemacht werden. Auch können Webserver direkt auf Datenbanken zugreifen und daher sehr flexibel eingesetzt werden.

Insbesondere durch den Einsatz mit Dokumenten Management Systemen läßt sich eine hohe Effizienz bei der Produktion und Verteilung vieler Dokumente erreichen. Dokumente können wesentlich zeitnaher verteilt werden als dies in Papierform oder auf magnetischen Datenträgern möglich ist. Da neuere Dokumente ältere ersetzen können, kann außerdem die Aktualität und Auffindbarkeit der Dokumente verbessert werden.

#### **Schutz des Webservers im Internet**

Um den Webserver vor dem direkten Kontakt mit dem Endbenutzer zu schützen und dadurch die Möglichkeit zur Kompromittierung des Servers zu verringern, können sogenannte Proxys eingesetzt werden. Diese Proxys bilden den Endpunkt der Internetverbindung des Benutzers. Die Anforderungen des Webclients des Benutzers wird nach entsprechender Prüfung durch den Proxy an den Webserver durchgereicht. Ebenso die Antwort des Webservers auf die entsprechende Anfrage. Der ganze Prozess geht für den Endbenutzer völlig transparent vor sich und der Proxy tritt – außer bei eventuellen Fehlermeldungen – niemals in Erscheinung. In der SuSE Linux Distribution kann der Proxy Squid als sogenannter Reverse-Proxy zum Schutz eines Webservers in der oben beschriebenen Weise konfiguriert werden.

#### **6.4.3. Software**

Zusätzlich zum Webserver Apache sind viele Softwareerweiterungen verfügbar, welche unterschiedliche Funktionalitäten zu den eigentlichen Apache-Funktionen bieten.

#### **Zusatzmodule zum Webserver**

Immer häufiger werden inzwischen auch dynamische Webseiten eingesetzt. Diese Seiten erlauben direkte Interaktion mit dem Webbrowser. Dabei werden die darzustellenden Webseiten dynamisch vom Server generiert. Um dynamische Webseiten zu erzeugen, sind mehrere Möglichkeiten denkbar. Die historisch älteste Möglichkeit solche dynamischen Webseiten zu erzeugen, besteht in der serverseitigen Ausführung bestimmter Skripte in einer Shell. Dabei wird vom Webserver eine Schnittstelle zum Betriebssystem geöffnet und das entsprechende Skript in einem Shelldialekt oder auch in Perl ausgeführt. Diese Methode kann allerdings zu Einbrüchen auf dem Webserver mißbraucht werden.

Über in Apache einladbare Module kann die Ausführung von Skripten zum einen beschleunigt und zum anderen sicherer ausgeführt werden. Als Standardmodule werden bei SuSE Linux beispielsweise `mod_perl` und `mod_php` mitgeliefert. Ebenfalls auf der SuSE Linux Distribution enthalten ist die Software JServ. Dadurch können auf dem Webserver Java Servlets genannte Java Programme gestartet werden.

Um vertrauliche Informationen zwischen Webserver und Webclient austauschen zu können, hat sich die Verschlüsselung durch SSL (*Secure Socket Layer*) zu einem quasi Standard im Internet entwickelt. Das Modul `mod_ssl` – welches ebenfalls Bestandteil der SuSE Linux Distribution ist – stellt diese Funktionalität auch für Apache zur Verfügung. Bei der Einrichtung des Webservers müssen zusätzlich Sicherheitszertifikate, die von einer

Zertifizierungsstelle wie der Deutschen Telekom oder Verisign signiert wurden, hinterlegt werden. Diese Zertifikate bewirken eine Authentifizierung des Webservers gegenüber dem Benutzer.

#### **Zusatzsoftware**

Um einen schnellen und für den Ersteller von Webdokumenten bequemen Weg zur Publikation zu ermöglichen, existiert spezielle Software. Diese als Web Content Management Systeme bezeichneten Programme können über einfache Schritte komplexe Dokumente in Webseiten integrieren. Ebenso erleichtern diese Systeme die Wartung von Webseiten. Im Lieferumfang der SuSE Linux Distribution ist die Software NPS enthalten. Diese mit einer Sybase Datenbank gekoppelte Software erlaubt unter Linux ein Dokumenten Management auf Webbasis.

Webseiten, die nach speziellen Suchbegriffen durchsucht werden können, stellen eine deutliche Verbesserung für den Benutzer dar. Für diesen Einsatzzweck kann die Software htdig verwendet werden. Dabei können auch mehrere Webserver indiziert und damit durchsuchbar gemacht werden.

## 7. Empfehlungen

Die Chancen und Vorteile von Open Source Software, die in dieser Studie aufgezeigt wurden, können nur erschlossen werden, wenn bei der behördeninternen Standardisierung nicht ausschließlich proprietäre Dateiformate, Programmpakete und Architekturen festgeschrieben werden. Nur eine Hinwendung zu offenen Standards schafft ein Klima, in dem wieder mehr Wettbewerb möglich ist.

Eine solche Entwicklung fand bereits vor ca. 10 Jahren mit der Festlegung auf die offenen internationalen Standards nach ISO bzw. OSI/CCITT statt. Diese Entwicklung scheiterte letztendlich an der mangelnden Umsetzbarkeit in wettbewerbsfähige Produkte.

Mit der allgemeinen Durchsetzung der Internet-Standards und dem gleichzeitigen Entstehen der Open Source Bewegung stehen wir heute vor einer gänzlich anderen Situation: Es gibt Alternativen zu den eingeführten Systemen, die bereits erprobt sind und im Ruf stehen stabil, ressourcenschonend und kostengünstig zu sein.

Der Einsatz von Open Source Software spart Lizenzkosten und senkt durch die Stabilität und gute Administrierbarkeit die Betriebskosten. Ein weiterer wettbewerbsfördernder Faktor ist die Unabhängigkeit von einzelnen Herstellern. Leider gibt es heute noch keine umfassende Analyse wie die TCO (Total Cost of Ownership) von Open Source Software im Verhältnis zu anderen Systemen tatsächlich aussieht. Man ist daher auf eigene oder fremde Erfahrungen angewiesen.

Auf der anderen Seite liegt es auf der Hand, dass eine Öffnung hin zu Open Source Software auch Kosten erzeugen wird. Den größten Anteil daran werden Schulungen und Beratungsleistungen einnehmen.

Letztendlich hängt vieles davon ab, wie erfolgreich sich die Ergebnisse der Open Source Bewegung am Markt durchsetzen werden. Im Server Bereich ist dieser Erfolg bereits eingetreten, wie unabhängige Analysen belegen. Im Desktopbereich, der durch die Officeanwendungen bestimmt wird, steht die Verbreitung von Open Source Software erst am Anfang. Die verfügbaren Desktop- und Bürokommunikationsanwendungen haben jetzt einen Reifegrad erreicht, der professionellen Anforderungen entspricht.

Unsere Empfehlung lautet daher, Open Source Software als Alternative uneingeschränkt für den Einsatz im Serverbereich zuzulassen. Die Eignung für den Desktopbereich sollte ernsthaft in Pilotprojekten überprüft werden, um auch das hierin liegende Einsparungspotenzial nutzen zu können.

## 8. Index

- Adobe 20
- AFS 17
- AIDE 26
- Andrew Filesystem 17
- Andrew Tanenbaum 49
- Andrew Tridgell 36
- Aolserv 44
- Apache 8f, 19, 29, 44, 50ff
- Apache (2) 52
- Apache Webserver 8
- Application-Level-Gateway 33
- Application-Proxy 33, 35
- AS/400 8, 15
- BMWi4
- Caldera 11
- CIFS (Common Internet File Standard) 35
- CIPE 42
- Coda 17
- Compaq 8, 11
- Computerviren 25
- Content Management Systeme 45
- Corel 11, 30
- Daniel Riek 10
- Debian 11
- demilitarisierten Zone 35
- digitale Signaturen 43
- DMZ 35
- Dokumentenformate 20
- Domain Name Service 49
- E-Mail 34
- E-Mail Service 35
- E-Mail Virus 34
- Embedded Systems 12
- Eric Allman 18
- Eric Raymond 50
- Eric S. Raymond 6, 57
- Extended Markup Language 20
- Failsafe 23
- Filterregeln 35
- Firewall 32ff, 50, 57
- FreeBSD 29, 49
- Free Software Foundation FSF 49
- Free Standards Group 8
- FreeSWan 26, 42
- FTP 34
- Fujitsu Siemens Computers 11
- Gartner 23
- Gartner Group 6
- Gewährleistung 10
- Ghostscript 18
- GNU 12, 15, 49
- GPG (Gnu Privacy Guard) 43
- Halloween 50
- The Halloween Documents 57
- htdig 45
- IBM 11, 15
- IBM S/390 8
- IDC 4, 16
- ID-Pro 11
- IETF (Internet Engineering Task Force) 9
- ILOVEYOU 25
- Informix 11, 50
- Innominate 11
- Installationssupport 12
- Intel 8, 15, 20, 23, 32, 49
- Internet 6
- Internet Operating System Counter 19
- IP-Masquerading 33
- ISO Standard 8613 ODA 20
- KDE 31
- K Desktop Environment 31
- Kerberos 16, 39
- KOffice 12, 31
- Kommandozeilenmodus 37
- Koordinierungs- und Beratungsstelle der Bundesregierung 4
- Kryptografie 42
- Larry Wall 49
- Linus Torvalds 13, 49
- Linux-Firewall 33
- Linux Professional Institute(LPI) 8
- Linux Standard Base (LSB) 8
- Linux-Tag e.V. 4
- LIVE Linux Verband e.V. 10
- Lotus 30
- Mail-Relay 35
- Mailserver 34
- Mail Transfer Agent (MTA) 18, 35
- Mandrake 11
- Melissa 25
- Microkernel 13, 34
- Microkernel Architektur 34
- Microsoft 20
- Microsoft Office 20, 30
- Minix 49
- Mozilla 11, 50
- Multitasking 14

NCSA	19, 50
NetBIOS	37
NetCraft Survey of Web Sites	19
Netscape	11
Netscape Navigator	37, 39
Network Address Translation (NAT)	33
Network Information Service (NIS)	16
NFS	17
NPS	45
NSA (U.S. National Security Agency)	22
NSAKEY	22
O'Reilly	11
Office Document Architecture	20
OpenPGP	43
Open Source Initiative(OSI)	8
openssh	26, 42
Oracle	11, 50
OS/2	17
OSD	7
OSI	7
Paketfilter	34
Paketfilter-	35
Patente	9
PDF	20
Perl	49
PGP	28
PGP (Pretty Good Privacy)	42
Philip R. Zimmermann	42
Portable Document Formats	20
Port Forwarding	33
Postfix	18
PostScript	18
PowerPC	8
Public Key Infrastrukturen (PKI)	38
Red Hat	11
Releasewechsel	23
Release-Zyklus	9
Request for Comments	9
RFC	9
RFC 2026	9
RFC 2440	43
RFC 2708	36
Richard Stallman	49
Router	35
Roxen	44
Samba	17, 36
SAP	11
Sendmail	9, 18
Server Message Block (SMB)	35
SGI	11, 23
Siemens	11
Simple Message Transfer Protocol (SMTP)	18
SMB	17
SMTP	34
Software AG	11
Squid	44
ssh	42
SSL	28
StarDivision	30
Staroffice	4
StarOffice	30, 32
SUN	11
SUN Sparc	8
Superuser	25
SuSE	11
SuSE Press	11
SWAT	37
Tatu Ylonen	42
TCO	23
TCO (Total Cost of Ownership)	46
Thin-Client	18, 31
Tripwire	26
trojanische Pferde	22, 34
Turbo Linux	11
UDP	17
Urheberrecht	9
Verschlüsselung	17, 26, 28, 40ff
Viren	32, 34
Virtual Private Networks	42
VMware	15, 29
VPN	42
Wietse Venema	18
Windows 2000	17, 22
Windows 95	14
Windows NT	13, 17, 19, 36f, 39
WINS	36f
WordPerfect	30
X.500	38f
X.509	38
X11-Protokoll	31
XML	20
X-Server <sup>13</sup>	31
Yast	16

## 9. Anlagen

### 9.1. Anlage I: Historische Meilensteine der Open Source Bewegung

(In Auszügen zitiert aus [4])

- 1969 Bell Laboratories und MIT beginnen mit der Entwicklung des Betriebssystems Multics.
- 1971 Ken Thompson und Dennis Ritchie entwickeln aus Multix das »Uniplexed Information and Computing System Unix« aus dem Unix hervorgeht.
- 1973 Dennis Ritchie schreibt den Quellcode von Unix mittels der von ihm entwickelten Programmiersprache C um.
- 1974 Das »Transmission Control Protocol« TCP wird spezifiziert.
- 1976 Das Programm »Unix-to-Unix-Copy« UUCP für Modem basierte Peer-to-Peer Netzwerke wird entwickelt.
- 1977 Das Unix-Derivat »Berkeley System Distribution« entsteht an der Universität von Berkeley, Kalifornien.
- 1979 Mit der »Edition 7« erscheint die letzte »freie« Unix-Version aus den Bell Laboratories. Die Kommerzialisierung von Unix beginnt.
- 1980 Mit BSD 4.1 erscheint »sendmail«, mit dem heute 75% des Mailaufkommens im Internet abgewickelt werden.
- 1982 Gründung von EUNET, um E-Mail und Usenet auch in Europa zu ermöglichen.  
TCP/IP entsteht.
- 1983 TCP/IP wird militärischer Standard.  
Richard Stallman gründet die »Free Software Foundation FSF«.
- 1984 Richard Stallman gründet das Projekt »Gnu is Not Unix« GNU, das zusammen mit FSF das Ziel verfolgt, ein freies Unix-basiertes Betriebssystem zu entwickeln.  
Der Verzeichnisdienst »Domain Name Service« vereinfacht die Zuordnung von IP-Adressen.
- 1986 Larry Wall entwickelt die Programmiersprache »Practical Evaluation and Reporting Language« Perl.
- 1987 Andrew Tanenbaum entwickelt das Lehr-Betriebssystem »Minix« für Intel-Prozessoren.
- 1991 Linus Torvalds, Student an der Universität von Helsinki, kündigt die erste Version von Linux 0.02 an.  
Im europäischen Kernforschungszentrum CERN entsteht das »World Wide Web« WWW. Der eingesetzte Webserver stammt vom National Center for Supercomputing Applications (NCSA).
- 1993 Start des Projekts »FreeBSD«.

- 1994 Release 1.0 von Linux wird freigegeben.
- 1995 Release 1.0 des Apache («a patchy server») der Apache Group, einem Team von Webmastern der NCSA und anderen Interessierten, erscheint.
- 1996 Release 2.0 des Linux-Kernel.
- 1997 Eric Raymond hält auf dem 4. Linux Kongress in Würzburg den Vortrag »The Cathedral and the Bazaar«, der die Vorteile einer frei-organisierten Softwareentwicklung hervorhebt.
- 1998 Der »Apache« Webserver erreicht einen Marktanteil von 50%.
- Browser-Krieg zwischen Microsoft und Netscape. Netscape gibt den Quellcode für den Navigator über »Mozilla.org« weltweit frei.
- Eric Raymond prägt den Begriff »Open Source« und schafft hierfür das erste Lizenzierungsverfahren.
- Oracle und Informix geben bekannt, ihre Datenbank-Systeme auch auf Linux verfügbar zu machen.
- Microsoft interne Studien über Open Source Software und Linux werden der Öffentlichkeit als »Halloween« Papiere zugänglich gemacht [5].
- 1999 Compaq, Dell, Fujitsu-Siemens, HP, IBM, SAP, SCO, Silicon Graphics Inc. (SGI) Sun kündigen ihre Unterstützung für Linux an.
- Release 2.2.0 des Linux-Kernels mit verbessertem SMP-Support, integrierter Firewall-Technologie und erweiterten Multimedia-Fähigkeiten.
- KDE 1.1 erscheint
- Red Hat geht als erster Linux-Distributor an die Börse.

**9.2. Anlage II: OSS-Installationen in der Landesverwaltung Baden-Württemberg**

Stand: 22.08.00

Lfd. Nr.	Ministerien usw. Nachgeordn.Beh.u.DSt.	Kurzbeschreibung der Installationen	Bemerkungen
1	<b>Staatsministerium</b>  LV Berlin	Internetangebot mit Linux / Apache Web-Server Linux mit Checkpoint-Firewall Linux mit Checkpoint-Firewall	Externer Betrieb
2	<b>Innenministerium</b>  ZKD  Polizei	Internetangebot mit Linux / Apache Web-Server, vgl. Nr. 1 Firewall mit Linux Firewall-Log-Host-System mit Linux Firewall-e-Mail-Backup-System für Administratoren DNS mit Linux Host-Emulation (70) Router auf ausgedienten PC (200) DNS- und Sendmail-Mail-Server (55) Workgroup-Server (Samba) Timeservice Internet-PC (150) Firewalls (6) Web-Server mit Apache, Adabas D VMware	
3	<b>Min. f. Kult. und Sport</b>	-	
4	<b>Justizministerium</b>	Internetangebot mit Linux / Apache Web-Server, vgl. Nr. 1	
5	<b>Finanzministerium</b>  Finanzämter	Internetangebot mit Linux / Apache Web-Server, vgl. Nr. 1 Einführung von StarOffice geplant	
6	<b>Wirtsch.ministerium</b>  LA f.Geol.,R.u.Bergb.         Verm.Verwaltung	Internetangebot mit Linux / Apache Web-Server, vgl. Nr. 1 Linux / Apache Web-Server (Internet) Linux / Intranet-Name-Server Linux / Interner und ext. Mail-Server Linux / File- und Printserver in 5 Dienstgeb. Linux auf Arb.PI.Systemen, 1 x Vmware mit MS-Windows als Gastsystem 1 x FreeBSD Netzwerkdienste Überlegungen, BK-Tests unter Linux durchzuführen Gepl. Anwendungen mit Internettechnik und OSS Eingesetzte Arb.PI.-Linux-PC (2 je VermA/Dienstst.) werden durch NT-Systeme im Rahmen einer Vereinheitlichung der Betriebssystem-Landschaft ersetzt	Die Erfahrungen mit Linux sind ausnahmslos sehr gut. Insbesondere die Stabilität und Effektivität sowie der äußerst geringe Wartungsaufwand des Betriebssystems sind überzeugend.

OSS IN DER LANDESVERWALTUNG BADEN-WÜRTTEMBERG

Lfd. Nr.	Ministerien usw. Nachgeordn.Beh.u.DSt.	Kurzbeschreibung der Installationen	Bemerkungen
7	<b>Min. Ländl. Raum</b> LFL (EBZI)	Linux Web-Server mit Apache (2) Linux mit DNS Linux mit Firewall MySQL-Server unter NT (Test)	Betrieb im Wesentlichen störungsfrei, mit sehr geringem administrativem Aufwand
8	<b>Sozialministerium</b> LGesAmt	Linux mit Firewall	
9	<b>Min. f. Umwelt und Verkehr</b>  LfU  Lfs/StraßenbauVerw.	Geplant im 2.Halbjahr 2000: Linux Web-Server mit Apache Linux mit DNS und Oracle-Anwendungen Testrechner mit SuSE 6.4 und Red Hat 6.2 im Einsatz (2) Linux File- und Print-Server mit Samba (47)  Linux Web-Server mit Apache Linux Proxy-Server für Internet Linux Router (8) Diverse Tools, u.a. tcpdump, tkined Geplant: Ausstattung von zwei weiteren Dienststellen mit Linux / Samba / evtl. Mail sowie 120 Dienststellen mit Linux-Routern	Sowohl SuSE als auch Red Hat sind geeignet, vorauss. kommt SuSE zum Einsatz      Es werden Überlegungen für ein neues Serverkonzept angestellt, in denen Linux voraussichtlich eine wichtige Rolle spielen wird
10	<b>Min. f. Wiss. u. Kunst.</b>	Linux / Apache Web-Server, vgl. Nr. 1	
11	<b>Kommunen</b>	Der Datenzentrale sind keine Installationen bekannt. Experimentiert wird z. Tl. mit Linux / Apache als Basis für Web- oder Name-Server.	

### 9.3. Anlage III: Standards des Landessystemkonzepts Baden-Württemberg (Auszug)

(ergänzt um Alternativprodukte aus dem OSS-Umfeld)

#### 8. Standards der Bürokommunikation (BK)

Zu den Standards, zur Migration auf diese Standards und zur ressortübergreifenden Abstimmung wird auf die VwV-BK (12) verwiesen.

Standard	Angaben zum Standard	Details	Produkt	Lizenz
<b>8.1 MAIL-Standards</b>				
X.400	ISO 10021, EN 41201/2 etc.	Standard für die ressortübergreifende und externe (Länder, Bund, EU) elektronische Post; <b>Bestandteil der einheitlichen IuK-Infrastruktur (1-8, 10, 12)</b>	Nicht bekannt	
SMTP	Internet-Standard	SMTP wird als ein mit X.400 gleichberechtigter Standard eingesetzt. Mit dem ZKD ist zu klären, wie im Einzelfall die Mail-Anbindung betrieben wird. (15)	Sendmail Postfix	Frei Frei
Sonst	Firmen-Standards	Als lokale MAIL in Absprache mit der Stabsstelle	Lotus Notes	kommerziell
<b>8.2 Verzeichnisdienst</b>				
X.500	ISO 9594, ENV 41210, etc.	Einheitliches elektronisches Benutzer-/Adressverzeichnis innerhalb der einheitlichen Bürokommunikation; Exchange-Verzeichnis (7, 10, 12); <b>Bestandteil der einheitlichen IuK-Infrastruktur</b>	OpenLDAP	frei
<b>8.3 Dokumenten-Struktur</b>		Landeseinheitliche Dokument-Strukturierung für einen möglichst problemlosen elektronischen Dokumentenaustausch (2), siehe auch Nr. 8.3.3		
<b>8.3.1 Dokumenten-Formate</b>				

Standard		Angaben zum Standard	Details	Produkt	Lizenz
	WinWord 6.0, 8.0 oder 9.0	de-facto-Standard	Die Ressorts können im Format WinWord 6.0, 8.0 oder 9.0 elektronische Dokumente mit ihren BK-Systemen verarbeiten und mit anderen Behörden austauschen. Detaillierte Regelungen trifft die Stabsstelle für Verwaltungsreform bei Bedarf. Der Geschäftsbereich des MLR erhält bis 01.01.2001 Dokumente im Format WinWord 6.0; <b>Bestandteil der einheitlichen IuK-Infrastruktur (10, 12, 19)</b>	StarWrite WordPerfect	Frei kommerziell
	HTML/XML	Internet-Standards	Aufgrund der WWW-Technologie als Standardformat für Hyperlink-basierte Dokumente und WWW-Informationangebote insbesondere im Landes-Intranet (9)	Apache	OSS
<b>8.3.2 Schrift-Typen</b>					
	Arial	de-facto-Standard	Größe:10, 12, 14, 20, 24; normal, fett, kursiv, unterstrichen; <b>Bestandteil der einheitlichen IuK-Infrastruktur (3, 10, 12)</b>	Unter Linux verfügbar Helvetica	frei
<b>8.3.3 Dokument-Vorlagen</b>			Erarbeitung einheitlicher Vorlagen, die der LSA für verbindlich erklärt: Der LSA beauftragte den AK-IT am 10.03.1999, eine einheitliche IuK-Anwendung zur Erstellung der standardisierten Dokumente für alle BK-Systeme im Kernbereich zu entwickeln und bis 31.12.2001 zu installieren. Eine erste Stufe wurde vom AK-IT freigegeben (20). <b>Bestandteil der einheitlichen IuK-Infrastruktur (16)</b>		

Standard	Angaben zum Standard	Details	Produkt	Lizenz
<b>8.3.4 Weitere BK-Funktionen</b>				
Tabellenkalkulation	de-facto-Standard	MS-Excel; <b>Bestandteil der einheitlichen IuK-Infrastruktur (10, 12)</b>	StarCalc	frei
Grafikprogramm	de-facto-Standard	MS-Powerpoint; <b>Bestandteil der einheitlichen IuK-Infrastruktur (10, 12)</b>	StarImpress	frei
Datenaustausch	de-facto-Standards	Microsoft-Standards: ODBC, OLE, DDE, MAPI; <b>Bestandteil der einheitlichen IuK-Infrastruktur (7)</b>	N.A.	
Komprimierungsprogramme	de-facto-Standards	WinZip (derzeit V. 7.0) und Squeez (derzeit V. 2.0) <b>(18)</b>	Zip gzip (GNU Zip) compress	OSS  Linux
Elektronische <sup>16</sup> Ablage	de-facto-Standard	NT-Filesystem (NTFS); <b>Bestandteil der einheitlichen IuK-Infrastruktur (10, 12)</b>	Ext2fs ReiserFS SAMBA	Linux Linux frei
Ende-zu-Ende-Verschlüsselung der Elektronischen Post	nationaler Industrie-Standard (TeleTrust)	In der Landesverwaltung werden im Rahmen der einheitlichen Bürokommunikation solche Produkte für die Ende-zu-Ende-Verschlüsselung der Elektronischen Post eingesetzt, die dem MailTrust-Standard in den Spezifikationen 1.1 und insbesondere 2.0 entsprechen. Die noch erforderlichen Entscheidungen zum Einsatz der Verschlüsselungstechnik beim Dokumentenaustausch werden von den Organisationsreferenten vorbereitet. <b>(17)</b>	PGP GPG	Frei OSS

## 9. Nutzung und Gestaltung von IuK-Anwendungssystemen

<sup>16</sup> Unter Linux ist eine Vielzahl von Filesystemtypen verfügbar. U.a. unterstützt Linux auch NTFS.

Standard	Angaben zum Standard	Details	Produkt	Lizenz
<b>9.1 WWW-Browser</b>				
<ul style="list-style-type: none"> <li>• <b>Microsoft Internet Explorer</b></li> <li>• <b>Netscape Communicator</b></li> </ul> – jeweils ab Version 4.x –	Firmen-Standards	Von diesen beiden Firmen-Standards werden grundsätzlich nur die Funktionen genutzt, die von beiden unterstützt werden. Damit soll so viel Herstellerunabhängigkeit wie möglich erzielt werden. Insbesondere die Finanz- und Personalsysteme sollen über diese Browser nutzbar sein. Sämtliche Funktionen sind zugelassen, soweit sie von beiden Browsern unterstützt werden, also insbesondere <ul style="list-style-type: none"> <li>• digital signierte Applets</li> <li>• https</li> <li>• Download von Daten</li> <li>• Bürokommunikations-Komponente. <b>(1)</b></li> </ul>	Netscape Communicator 4.7 KDE/KFM	Frei  OSS
<b>9.2 Applet-Programmierung</b>				
<b>JDK Version 1.1 nach Verfügbarkeit auch JDK Version 1.2</b>	Firmen-standard	Java Visual Age, Javabeans und weitere produktivitätssteigernde Hilfsmittel oder Klassenbibliotheken sind zugelassen. <b>(1)</b>	Java2 1.2.2 IBM Developer Kit für Java2 Technology Edition	
<b>9.3 Seitengestaltung</b>				
nach HTML, XML	Internet-Standards	Die graphische Gestaltung der Seiten soll auf angemessenen Aufwand beschränkt werden. <b>(1)</b>		
<b>9.3 Object Request Broker</b>				
<b>CORBA/IIOP</b>	OMG-Standards	Homogene Anwendungen sind mit möglichst wenig technischem Overhead zu realisieren. <b>(1)</b>	Mico	OSS

#### 9.4. Anlage IV: Quellenverzeichnis

	<b>Titel</b>	<b>Autor/Hrsg.</b>
[1]	The Cathedral and the Bazaar, Oktober 1999, O'Reilly, ISBN: 1565927249 <a href="http://www.tuxedo.org/~esr/writings/cathedral-bazaar/">http://www.tuxedo.org/~esr/writings/cathedral-bazaar/</a>	Eric S. Raymond
[1a]	Homesteading the Noosphere <a href="http://www.tuxedo.org/~esr/writings/homesteading/">http://www.tuxedo.org/~esr/writings/homesteading/</a>	Eric S. Raymond
[2]	The Open Source Definition <a href="http://www.opensource.org/osd.html">http://www.opensource.org/osd.html</a>	Open Source Initiative
[3]	Debunking Open-Source Myths: Development and Support, 15.5.2000, Gartner Group <a href="http://gartner3.gartnerweb.com/public/static/hotc/hc00088469.html">http://gartner3.gartnerweb.com/public/static/hotc/hc00088469.html</a>	N. Drakos
[4]	Linux – Ein Pinguin kann fliegen Februar 2000, WestLB Research GmbH	Loeken, Hopkinson
[5]	The Halloween Documents <a href="http://www.opensource.org/halloween/">http://www.opensource.org/halloween/</a> <a href="http://ID-PRO.de/linux/halloween.html">http://ID-PRO.de/linux/halloween.html</a> (deutsche kommentierte Version)	
[6]	KBSt-Brief Nr. 2/2000 »Open Source Software in der Bundesverwaltung«, Februar 2000 <a href="http://www.kbst.bund.de/papers/briefe/02-2000/brief2-2000.html">http://www.kbst.bund.de/papers/briefe/02-2000/brief2-2000.html</a>	Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik
[7]	Firewalling unter Linux 1.4 <a href="http://www.pro-linux.de/work/server/andere/firewall.html">http://www.pro-linux.de/work/server/andere/firewall.html</a>	Samuel Stähle
[8]	Maximum Linux Security 2000 SamsPublishing, ISBN 0-672-31670-6	Anonymous
[9]	Statusbericht über die Rechtsprechung und Erteilungspraxis in Bezug auf softwarebezogene Erfindungen <a href="http://www.sicherheit-im-internet.de/download/hoessle-bericht1.pdf">http://www.sicherheit-im-internet.de/download/hoessle-bericht1.pdf</a>	Hössle & Kudlek Patentanwälte Stuttgart, München
[10]	Verzeichnisdienste in unternehmensweiten TK- und DV-Infrastrukturen VDE Verlag 1999	A. Badach (Hrsg.) M. Reinwarth K. Schmidt
[11]	Keine Entwarnung bei SW-Patenten Linux Verband kritisiert Haltung der EU-Kommission zu Software Patenten <a href="http://www.linux-verband.de/aktuell/News_60.de.shtml">http://www.linux-verband.de/aktuell/News_60.de.shtml</a>	L I V E Linux Verband e.V.

- |      | <b>Titel</b>                                                                                                                                                    | <b>Autor/Hrsg.</b>                           |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| [12] | ISIS Linux Report Edition 1–2000<br>ISBN 3–933194–58–X<br><a href="http://www.nomina.de/info/c_info_linrep.htm">http://www.nomina.de/info/c_info_linrep.htm</a> | Nomina Informations–<br>Service              |
| [13] | Dasein oder Nicht–Dasein<br>Analyse der Ausfallzeiten von Web–Servern<br><br>c't 2000, Heft 8, seite 174                                                        | Jürgen Schmidt                               |
| [14] | Using Samba,<br>O'Reilly Verlag, Jan. 2000, ISBN 1–56592–449–5                                                                                                  | R. Eckstein, D. Col–<br>lier–Brown, P. Kelly |
| [15] | Practical Unix & Internet Security,<br>O'Reilly Verlag, Apr. 1996, ISBN 1–56592–148–8                                                                           | S. Garfinkel, G. Spaf–<br>ford               |
| [16] | Kryptographie,<br>O'Reilly Verlag, 2000, ISBN 3–89721–155–6                                                                                                     | G.W. Selke                                   |