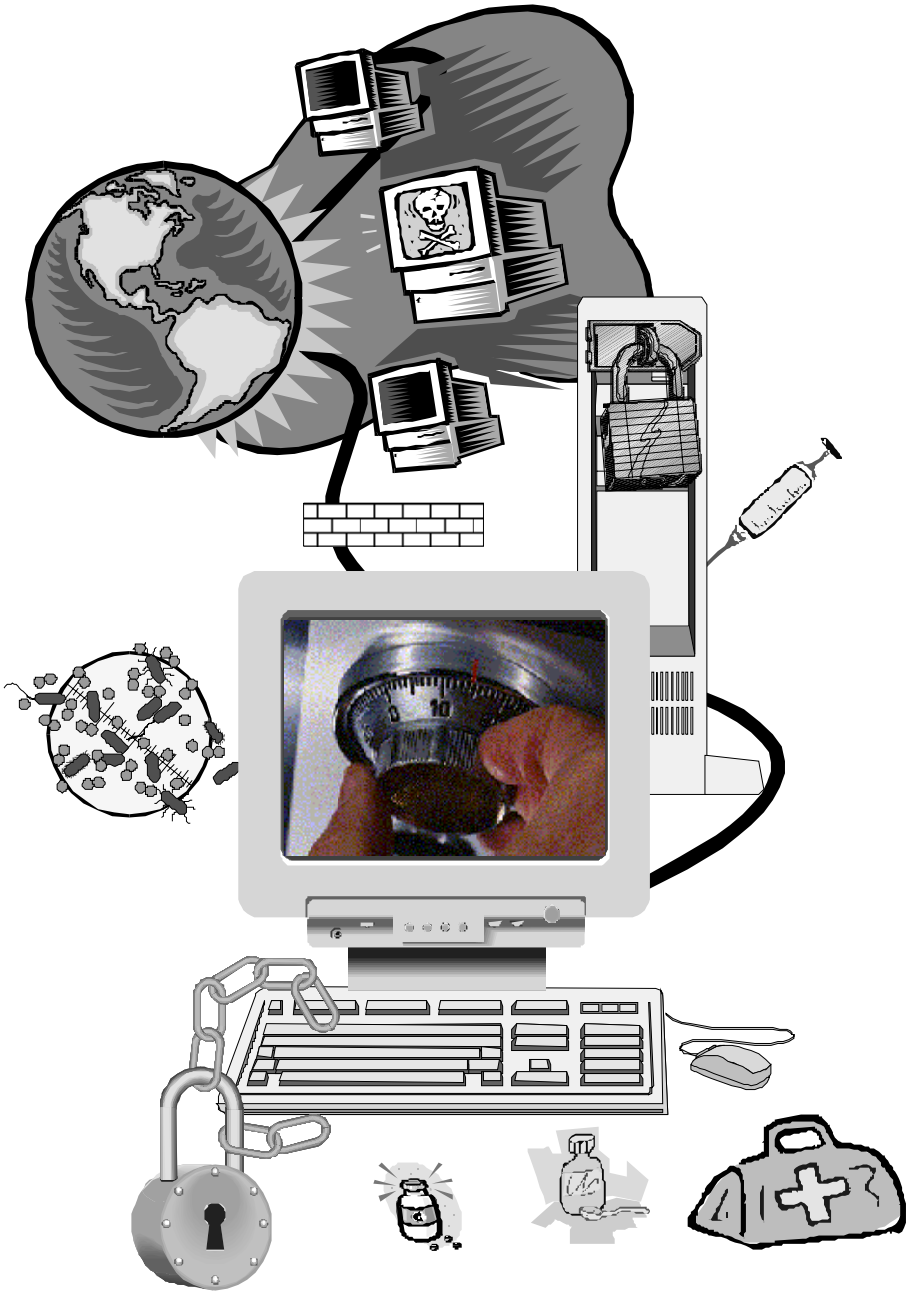
# SPLITTER

*IT-Nachrichten für die Berliner Verwaltung Nr. 3/1999 - 9. Jahrgang*

## DATENSICHERHEIT IM NETZ

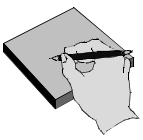


***IN DIESER AUSGABE:*** ***Schwerpunkt*** *"Datensicherheit im Netz"*

***Online • Infos • CD-ROM • Projekte & Verfahren • Tips & Tricks • Literatur ...***

Berlin

# Verkehrssicherheit wie im Mittelalter?



Wegelagerer und Plünderer vereinigen sich in Chaos-Clubs und arbeiten mit den großen Handelshäusern eng zusammen, um die Schwachstellen der Verkehrswege aufzudecken. Auf dem Marktplatz werden die günstigsten Stellen für Überfälle auf Goldtransporte ausgerufen. Die schlausten Halunken treten auf Jahrmärkten auf und prahlen mit ihren erfolgreichen Aktionen...

So schlimm war es nicht ...

Das hat es im Mittelalter **nicht** gegeben. Die Bedeutung sicherer Verkehrswege für die wirtschaftliche Entwicklung war schon seit Urzeiten klar.

Und heute?

Die Daten-Verkehrswege entwickeln sich zum bedeutensten Infrastrukturfaktor unserer modernen Informationsgesellschaft. Die Sicherheitsvorkehrungen für den Datentransport sind auf einem hohen technischen Stand. Vorkommnisse sind im Verhältnis zum Volumen des Datentransports sehr selten. Nur die Diskussion über die Sicherheit in Datennetzen bewegt sich noch auf einem vormittelalterlichen Stand.

... so schlimm ist es heute!

Wegelagerer auf der Datenautobahn lassen sich als Robin Hood des Informationszeitalters feiern. Strafverfolgung und Verbrechensaufklärung werden wenig unterstützt und hecheln ständig der neusten technischen Entwicklung hinterher. Das Unrechtsbewußtsein bei Angriffen auf den Lebensnerv unserer Gesellschaft ist nicht vorhanden. Anschläge auf das Datennetz sind zu einem akzeptierten Freizeitvergnügen gesellschaftlicher Randgruppen geworden, die im Internet ungehindert Erfahrungen austauschen.

Die öffentliche Verwaltung steht unmittelbar vor den entscheidenden Schritten in Richtung elektronisches Rathaus und muß vorher die Sicherheitsprobleme hinterfragen und vollständig klären. Also genug Anlaß für ein SPLITTER-Schwerpunktthema. Und das ist nicht nur interessant für die Technikfreaks. Jeder Blick in die Büro-Glotze, jedes Hämmern auf die Tastatur sollte mit einem ausgeprägten Sicherheitsbewußtsein erfolgen. Lesen Sie also die Beiträge und bringen Sie sich als verantwortungsbewusster Verwaltungsmitarbeiter/in auf den aktuellsten Stand der Diskussion.

**http://www.bsi.de/**
ist die wichtigste Informationsquelle

Sie werden wieder einige Hinweise auf Material des Bundesamtes für Sicherheit in der Informationstechnik (BSI) finden. Für die Bereitschaft, uns dieses Material für eine Veröffentlichung zur Verfügung zu stellen, möchte ich mich an dieser Stelle herzlich bedanken.

Sicherheit in unseren Datennetzen ist nur durch derartige Kooperationen zu erzielen. Ein Netzwerk der Systemverantwortlichen in der öffentliche Verwaltung muss entstehen, in dem Erfahrungen und Informationen über aktuelle Angriffe auf die Netzsicherheit ausgetauscht werden. Ich hoffe, daß unser Schwerpunktthema Sie zu weiteren Schritten in diese Richtung angeregt hat.

Im Namen der SPLITTER Redaktion
Ihr

Rainer Hensel

# In dieser Ausgabe:



## Editorial

Verkehrssicherheit wie im Mittelalter? 2



## Schwerpunktthema

Hackers Guide oder was man über Cracker wissen muß 4
Berliner Polizei ermittelt im Internet 8
Stateful Dynamic Signature Inspection (SDSI) für sichere Daten im Netz 9
Sichere Intranet/Internet-Mail 12
PC-Viren? Keine Panik! 13
Allgemeingültiger Leitsatz für mehr Datensicherheit: 13
Firewall-Systeme im Landesnetz 14
Open Source-Software – eine neue Chance für die Sicherheit? 16
Definitionssache: Datenschutz – Datensicherheit 16
IT-Sicherheit: Sichere Kommunikation mit zertifizierten elektronischen Signaturen 19
Der Feind im Telefon 21
Computer Emergency Response Team 23
Der Internet-Zugang birgt immer Gefahren 24



## Parlament & Senat

IT-Ausstattung und IT-Planung in der Senatsverwaltung für Stadtentwicklung, Umweltschutz und Technologie 25
Jugendarbeit und Computer in Kinder- und Jugendbibliotheken 30
Jahresberichte des Berliner Datenschutz-beauftragten 33



## Verwaltung

Hochschulbibliothek der FHVR Berlin: Retro-Konversionsprojekt 35
Solum Star 37



## Berichte & Infos

Aktuelle Projekte aus dem Deutschen Insitut für Urbanistik 38
„Die virtuelle Zukunft der öffentlichen Verwaltung – und wo bleibt der Mensch?" 39
Mit elektronischer Aktenführung zu schnellen Entscheidungen 42
Neues aus dem Hause Microsoft 45
Sicherheitslücken bei der Jahr-2000-Umstellung 47
Kurzmeldungen 49
Amt für Logistik und Informationstechnik im BA Lichtenberg 1998 49



## Online

Stadtpläne online 51
Kurz-Info zum Intranet-Angebot der Senatsverwaltung für Inneres 51
Kfz-Wunschkennzeichen reservieren! 52
Lokale Agenda 21 online 52
Die besten Suchmaschinen im Internet 53
Internet Cafes in der Jugendarbeit 53
debitel akquiriert die „erste Adresse" Deutschlands im Internet 53



## Tips & Tricks

Link in einem neuen Fenster öffnen 54
Hier spricht das Testlabor 54
Copyright im Internet – Teil III 55



## Veranstaltungen

Digitale Archive – ein neues Paradigma? 57
Neue Medien stellen neue Herausforderungen 60
CeBIT 2000 im EXPO-Jahr bereits im Februar 61
OPENNET 99 62
SYSTEMS 99 62
Jubiläums-IFA: Rekordbeteiligung mit 849 Aussteller aus 36 Ländern 62



## Literatur

Broschüre „Arbeiten im Call Center" 63



## CD-ROM

Statistik regional jetzt auch auf CD-ROM 63

## Dies & Das

Internetsucht 64



Impressum 64

# Hackers Guide oder was man über Cracker wissen muß

***Guido Stepken hat ein sehr informatives Handbuch für Linux 2.0 und 2.2 geschrieben, das nicht nur für System-Administatoren von Linux-Servern interessant sein dürfte. Insbesondere die allgemeinen Tips und Tricks zur Sicherheit sind sehr lesenswert und werden den SPLITTER-Lesern zum Schwerpunktthema auszugsweise mit freundlicher Genehmigung des Autors zur Verfügung gestellt. Guido Stepken ist unter der Email-Adresse stepken@little-idiot.de zu erreichen. Das Firewallhandbuch (ca. 300 Seiten) gibt es im Internet unter der URL http://www.little-idiot.de/firewall/ zum Lesen und zum Download und Ausdrukken als PDF-Datei.***

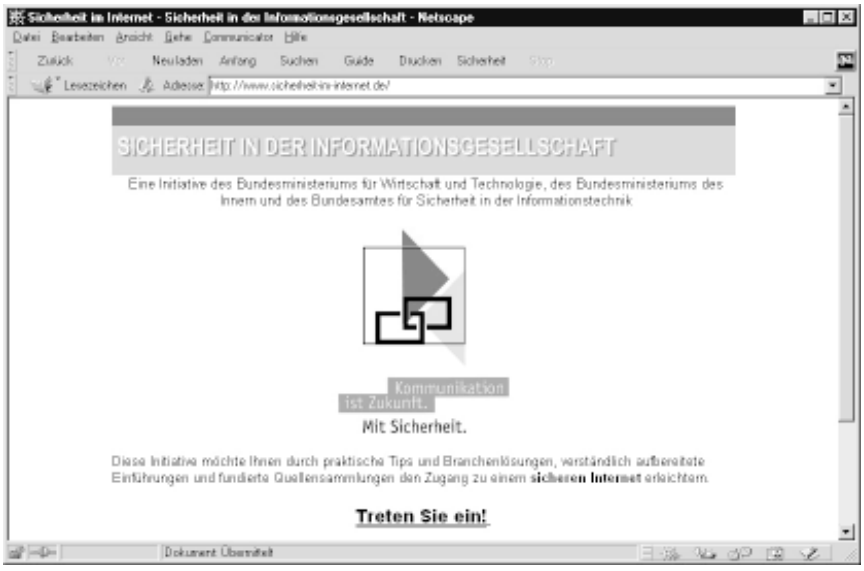
Hackerangriffe haben in der letzten Zeit wiederholt für Schlagzeilen in der Presse gesorgt. Von Angriffen auf Unternehmen wurden nur wenige Fälle offziell bekannt. Allein im letzten Jahr konnte ich allein auf denen von mir betreuten Servern hunderte von Angriffen registrieren. Viele darunter waren einfache Versuche von Hackern mit den im Internet verbreiteten Werkzeugen, ein paar dutzend Hacker hatten offensichtlich etwas mehr Skill.

Auf der Suche nach geeigneten Abwehrmaßnahmen gegen solche Angriffe mußte jedoch zuvor analysiert werden, wie die Hacker in das System eingedrungen sind, und ob eventuell der Einsatz einer Firewall möglich ist. Das Resultat ist ernüchternd, zumal Firewalls gegen viele Angriffe auf Server keinerlei Schutz bieten können.

Einige genauere Untersuchungen haben aber auch gezeigt, daß Firewalls, die Intranets absichern sollen, doch etwas anders überwunden werden, als viele der Systemadministratoren sich dieses vielleicht vorstellen. Der Grund liegt nicht im Versagen evtl. einer Firewall, sondern zumeist in gravierenden Mängeln bei der Erstellung und Umsetztung eines Sicherheitskonzeptes, auch Security Policy genannt, welche einen Einbruch in das Netzwerk sehr erleichtern.

Um jedoch Sicherheitskonzepte aufbauen zu können, sind Erfahrungen notwendig, die man nicht einigen Prospekten von Firewallherstellern oder Büchern entnehmen kann. Insbesondere trifft es unerfahrene Systemadministratoren hart. In dem Artikel soll vielmehr die Sicherheit aus der Sicht des Hackers oder besser gesagt, Crackers geschildert werden. Um ein Netzwerk erfolgreich schützen zu können, sind Hintergrundwissen und viel Erfahrung notwendig. Insbesondere sollte man sich selber einmal als Cracker betätigt haben. Als Anfangsübung sollte ein standardmäßig installierter Windows NT Server oder ein LINUX Server genügen. Nur wer die Lücken und Schwächen der von ihm betreuten Systeme kennt, weiß, wonach er im Falle eines Angriffs suchen muß, und wie er diese Systeme schützen kann.

Angriffe auf den TCP/IP-Stack sind gegenwärtig die Ursache von immensen Ausfällen bei ISPs und innerhalb des Netzwerkes von Unternehmen. Verantwortlich sind hierbei häufg mangelhafte TCP/IP-Stacks in Servern und Routern, die empfindlich auf defekte Netzwerkkarten und speziell konstruierte TCP/IP- Pakete reagieren. Diese Pakete werden von Programmen erzeugt, die im Internet im Quellcode und als Windows-Programm veröffentlicht werden. Diese werden Exploits genannt und sind im BUGTRAQ-Archiv zu finden (http://www.geek-girl.com). Sie sind fast ohne Netzwerkkenntnisse von jedermann ausführbar und greifen Internet-Server, arglose Surfer und vor allem PCs im internen Netzwerk an. Insbesondere Fa. Microsoft hat sich hierbei nicht mit Ruhm bekleckert, die Folgen waren allerorts zu spüren: Computerwoche, SWF3, Microsoft, Netscape... -Internet-Server und viele andere waren wochenlang "offline", hunderttausende von Surfern werden mit DoS-Angriffen belegt, die ein Einfrieren vor allem von Windows 95/98/NT Workstations bewirken. ➔




***„Sicherheit in der Informationsgesellschaft" ist eine Initiative des Bundesministeriums für Wirtschaft und Technologie, des Bundesministeriums des Innern und des Bundesamtes für Sicherheit in der Informationstechnik. Die Website (URL http://www.sicherheit-im-internet.de/ bietet viele fundierte Informationen zum SPLITTER-Schwerpunkthema.***

### ← Zeitaufwand und Einbruchswerkzeuge

Erst durch das vertraglich verbotene „reengineering", d.h. die Zurückverwandlung in Assembler/C-Quellcode offenbart erst das wahre Ausmaß der Systemunsicherheit. Toolkits, wie „windasm", NUMEGAs SoftIce oder „boundschecker" sind die Standardtoolkits, mit welchen sich ohne Probleme sogar Dongle und Seriennumern-Abfragen deaktivieren lassen. Hier einige Beispiele für den Zeitaufwand, den ein einigermaßen erfahrener C-Programmierer und Assembler-Kenner benötigt, um folgende „Probleme" zu beseitigen: (Exploits = Programme zur Ausnutzung einer Sicherheitslücke)

- Dongle-Abfrage eines WIN/INTEL-Programmes beseitigen: 1-2 Tage
- Seriennummer-Abfrage eines WIN/INTEL Programmes beseitigen: 1/2 Tag
- Bekannten Exploit suchen und anwenden (Lamer): 10 Minuten
- Exploit (buffer overfow) von INTEL- > MIPS/SPARC portieren (LINUX): 1 Tag
- Exploit schreiben nach einem konkreten Hinweis aus BUGTRAQ: 2 Tage
- Reverse Engineering von Patches (Binary): 2-3 Tage
- Reverse Engineering von Quellcode- Patches: 1 Tag
- Exploit schreiben mit durchsuchen des Quellcodes (UNIX): 1 Tag
- Exploit schreiben ohne Kenntnis des Quellcodes (UNIX): 1 -2 Tage
- Exploit schreiben ohne Kenntnis des Quellcodes nach konkretem Hinweis (NT 4.0 IIS 2.0): 1 Stunde bis 2 Tage
- Auffinden von möglichen exploits (Quellcode 1000 Zeilen C): 3 Stunden-1 Tag
- Reverse Engineering von JAVA-Bytecode-Quellcode (kleine Anwendung): 1 Stunde
- Reverse Engineering von VB 4.0 Bytecode-Quellcode: 1 Stunde
- Reverse Engineering von 2 KByte Binary > Quellcode: = Zeit für Neuschreiben.
- Fehler in TCP/IP-Stack suchen über Netzwerk und DoS Angriff ausführen: 5 Minuten
- Passwortsniffer unter Windows 95/NT installieren: 5 Minuten
- Passworte aussortieren und Zugriff auf Fileserver/SQL-Server erhalten: 10 Minuten
- Keyboard-Sniffer installieren: 5 Minuten
- BO, NetBus und Plugins remote installieren: 5 Minuten

Diese Beispiele sollen nur ungefähr eine Vorstellung von dem Zeitaufwand geben, den es braucht, mit entsprechenden Vorkenntnissen und Erfahrung bestimmte Angriffe erfolgreich durchzuführen.

### Normale Surfer am Netz und Erpressungen ?

Es gibt in Deutschland bald vier Millionen User mit Internet - Anschluß. Kaum jemand fühlt sich durch Hackerangriffe bedroht, da ja Kontakte über Internet weitestgehend anonym bleiben können. Es gibt aber mit rasant wachsender Anzahl Hacker , die mit z.B. SMB-Scannern riesige Listen von IP- Nummern von DIAL-IN Anschlüssen von Providern tagelang durchforsten. Wer es nicht glaubt, der möge sich einen Scanner installieren und die Pakete, die am PC ankommen, genauer betrachten. Es sind pro Stunde einige Dutzend Einschläge zu verzeichnen. Wer' s nicht glaubt, installiere sich einen Scanner, und warte (http://www.signal9.com). Diese Hacker sind auf der Suche nach PCs, auf denen das Laufwerk C: zum Schreiben freigegeben ist. Haben sie einen gefunden, so installieren sie schnell BO und durchforsten die Festplatte nach Briefen u.s.w. Sehr viele Pädophile oder Homosexuelle Surfer benutzen IRC-Clients, um untereinander zu kommunizieren oder, was weit häufger der Fall ist, gesetzlich verbotene Bilder direkt von Festplatte zu Festplatte über das Internet auszutauschen. Die IP-Nummern von IRC- Mitgliedern werden routinemäßig von Hackern auf Verletzbarkeiten überprüft, um evtl. BO zu installieren. Man kann davon ausgehen, daß tausende von Lehrern, Professoren, Angestellte u.s.w. auf diesem Wege Opfer von Erpressungen werden. Andererseits gibt es im Internet einige zwielichtige Personen, die als selbsterklärte Polizisten auf diesem Wege die Kinderpornografie bekämpfen. Diese geben nach solchen Angriffen Tips an die Polizei.

### Angriffe auf Applikationsebene

Trojanische Pferde sind ein unerläßliches Hilfsmittel für gezielte Angriffe auf Unternehmen. Sie werden von unzähligen Hackern eingesetzt, weil sie unaufällig sind, und mit höchster Wahrscheinlichkeit zum Erfolg führen. Professionelle Angreifer arbeiten mit trojanischen Pferden die sie im Internet platzieren, und dann dafür sorgen, daß diese von den Systemadministratoren auch geladen und installiert werden.

Trojanische Pferde aktivieren sich nach Abfrage bestimmter Kriterien, beispielsweise genau dann, wenn sich ein bestimmter Name in einem File findet (Absender in der Konfigurationsdatei des E-Mailprogrammes), oder die Arbeitsstation eine bestimmte IP-Nummer besitzt, die der Angreifer vorher ausgespäht hat. So ist es z.B. ohne Probleme möglich, einer Weihnachtsmann-Animation noch einen Portscanner oder Sniffer hinzuzufügen, der sich im Hintergrund betätigt. Angreifer erfragen zuvor Namen - Hauptziel sind Systemadministratoren - und übermitteln der Zielperson dann freundliche Grüße mit o.a. URL als Anhang („Den musste mal testen !"). Um dann weitere Daten ausspähen zu können, muß der Angreifer zuerst einen Tunnel durch die Firewall konstruieren.

Hierzu wird er mit Sicherheit Port 80 oder den Default Proxy-Port 8080 ➔

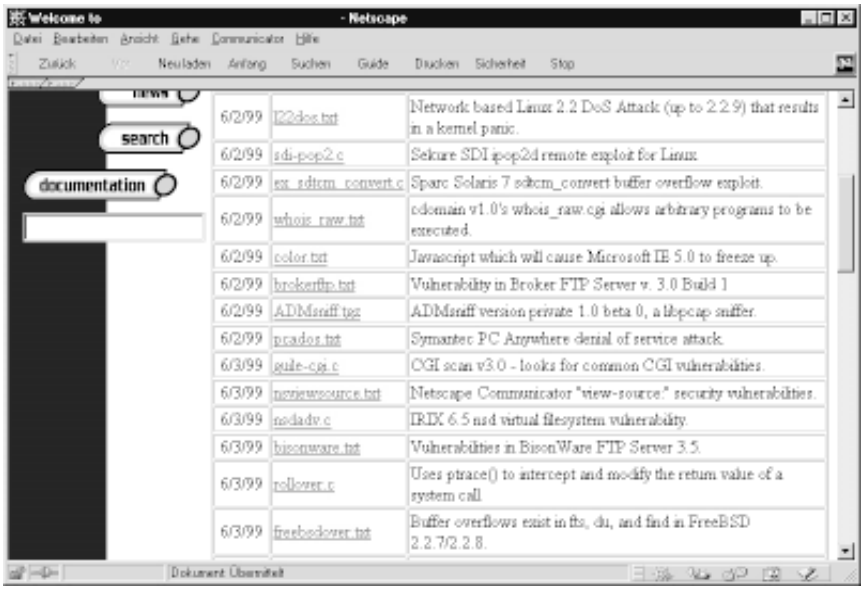
← wählen und den Benutzer dazu irgendwie veranlassen ein Programm zu starten, welches eine Verbindung zum Internet herstellt. Ist erst einmal dieses Programm entweder im Hintergrund (vom Taskmanager verborgen, wie BO oder NETBOS) gestartet, so hat der Benutzer keinen Überblick darüber, ob ein trojanisches Pferd aktiviert ist und was es macht. Ein Eintrag in das Autostartverzeichnis ermöglicht es dem Angreifer, stets zu gewöhnlichen Bürozeiten sein Unwesen im Netz des Unternehmens im Internet zu treiben.

Welche Programme können trojanische Pferde enthalten ?

- Bildschirmschoner
- Aufsätze auf den Internet Explorer
- Makroviren via E-Mail
- E-Mail Attachments
- Tastatur Makros
- Eingeschleuste Pseudo-Updates
- Angriffe über IRC, Quake, ICQ, Netmeeting
- Microsoft Windows als trojanisches Pferd

Bildschirmschoner (http://www.bildschirmschoner.de) sind beliebte trojanische Pferde. Da sie aber Geschmackssache sind, kann ein Angreifer nicht damit rechnen, daß die Zielperson einen bestimmten auf seinem Arbeitsplatzrecher installiert.

NeoPlanet z.B. ist ein Aufsatz auf den Internet Explorer, welcher ein schöneres Design verspricht. Nachteil: Dieser Browser verrät Informationen von der Festplatte und sendet diese an seinen Homeserver auf der Domain „sushiking.com“. Welche dies sind, ist leider unbekannt, da die Informationen verschlüsselt übertragen werden. Eine weitere unangenehme Eigenschaft ist, daß dieser Browser eigenständig die ISDN-Leitung in das Internet öffnet, also sowohl Telefonkosten verursacht, als auch eigenständig Informationen von der Festplatte in das Internet versendet. Das könnten z.B. die schlecht verschlüsselten Passwortdateien des WS-FTP sein, als auch die PWL -Dateien, in welchen die Zugangspassworte zum Server stehen. Ein ideales




***Kleine Auswahl von Hackertools, die aus dem Monat Juni 1999 stammen und jederzeit aus dem Internet zu besorgen sind. Die Adresse geben wir hier einmal ausnahmsweise nicht an :-)***

Werkzeug, da ein Angreifer davon ausgehen kann, daß das Programm längere Zeit auf der Arbeitsstation läuft.

Mit Hilfe des von Microsoft angebotenen Kits, mit welchem man nach eigenem Geschmack Aufsätze auf den Internet Explorer basteln kann, gelingt es einem Angreifer schnell, ein trojanisches Pferd zusammenzubasteln, wie man an dem sehr hübsch gemachten NeoPlanet Browser sehen kann.

Makroviren, die via E-Mail in ein Unternehmen eingeschleust werden, können im Quellcode so ziemlich alle möglichen Programme versteckt haben. Grund ist die Hinterlegung von Office 97 mit dem Visual Basic 5.0 und einem Update auf Winsock2.0/2.1. Hiermit ist es nun möglich, Netzwerksniffer direkt in die Makros von Excel, WinWord oder PowerPoint hinein zu programmieren. Auch BO könnte man via Word Makros auf dem Arbeitsplatzrechner installieren. Schwachpunkt ist immer der Internet-Anschluß. Erst kürzlich wurde entdeckt, daß auch unter Windows NT 4.0 mit Excel-Makros voller Zugriff auf das System möglich ist. (Vasselin Bontchev, BUGTRAQ) Viren-Scanner können einen solchen Angriff leider noch nicht erkennen.

Email-Attachments, wer hat sie noch nicht erhalten. Unter Bekannten tauscht man gerne mal einen “EXE-Gruß” aus. Wer kennt sie nicht: Elchtest aus PCWELT, X-MAS.EXE, Getränkehalter: Die CDROM fährt aus). Aus vermeintlich vertrauenswürdiger Quelle vermutet niemand ein trojanische Pferd. Angreifer kennen meist aber Mail-Adressen von Kollegen und externen Mitarbeitern, da einem Angriff immer eine genaue Untersuchung der Logfiles des E-Mail Exchangers/Relays vorausgeht. Über abgefangene E-Mails, die zumeist noch Cc: -Adressen enthalten, ist der Angreifer durchaus im Bilde, wer in den Augen des Systemadministrators vertrauenswürdig ist, und wer nicht. E-Mail - Exchange-Server von Providern sind oft sehr schlecht gesichert. Die Logfiles enthalten aber →

← wichtige Schlüsselinformationen über Kontaktpersonen, Kunden, Bekannte. Outlook 98 hat z.B. ein gravierendes Problem. Wer eine E-Mail erhält, kann nicht sicher sein, daß der Name der als Antwort-Adresse (reply) angegeben ist, auch tatsächlich diejenige Person ist. Cracker verbergen gerne ihre eigene E-Mail Adresse dahinter und fordern einen User auf, bestimmte Dateien zu senden. Der User versendet dann vertrauliche Daten an eine vertraute Person, nicht wissend, daß sich dahinter in Wirklichkeit die Adresse eines Crackers im Internet verbirgt.

### Makroviren Melissa & Co beleuchtet

Der Makrovirus Melissa ist ein gutes Beispiel für eine neue Generation von Angriffswerkzeugen, die über fast jede Firewall hinweg tunneln.

Wer sich ein wenig im Code umschaut, der wird feststellen, daß dieses Makrovirus zuerst die Sicherheitseinstellungen ausschaltet, um dann völlig ungehindert auf System- und Userdateien (auch unter Windows NT 4.0 SP5) und Server zugreifen kann. Dasselbe betrifft auch Backoffice, SQL-Server und die darin enthaltenen Daten. Dieses Virus ist noch relativ harmlos, es ist aber auch ohne Probleme denkbar, daß dieser sich zuerst im Netzwerk verbreitet, und dann die Festplatten sämtlicher Arbeitsstationen neu formatiert. Hierzu bedarf es nur einer einzigen weiteren Zeile.

Fast alle Virenscanner erkennen Teile (!) dieses Melissa-Codes und beseitigen bzw. sperren dieses Virus. Bei entsprechender Modifikation der für Virenscanner erkennungsrelevanten Teile des Virus hat sich erwiesen, daß es immer noch möglich ist, dieses Virus in Netzwerke einzuschleusen. Gezielte Angriffe auf Datenbestände im Netzwerk hinter der Firewall sind somit zu jeder Zeit möglich. Von Interesse ist auch die Möglichkeit, über die Winsock 2.1 mit Hilfe diese Visual Basic Code auf die Netzwerkkarte der Arbeitsstation direkt zuzugreifen, um z.B. DoS-Angriffe auszuführen, oder Passworte aus dem Netzwerk zu „ersniffen".

Damit nun nicht gleich die Panik ausbricht - Es gibt saubere Lösungen gegen diese Probleme - Z. B. das von mir vorgestellte Konzept der GRAPHICAL FIREWALL, bei der nur Bildschirminformationen, Tastaturdrücke und Mausbewegungen über eine Firewall hinweg übertragen werden. Das System ist nachweislich gegen alle obigen Angriffe immun. Das schönste daran ist - die Software ist völlig kostenlos und läuft auf fast allen Betriebssystemen. In der Praxis hat es sich bisher sehr bewährt.

*GUIDO STEPKEN* ◆

### Glossar

| | |
|---|---|
| **Firewall** | Spezieller Rechner zum Schutze des Netzwerkes |
| **Cracker** | Fälschlicherweise oft als (harmlose) Hacker bezeichnet. Cracker dringen in Systeme ein. |
| **TCP/IP** | Transmission Control Protocol / Internet Protokol. Das Transmission Control Protocol, dient vor allem der Sicherstellung der Datenübertragung im Inter-/Intranet. Das Internet Protocol, dient hauptsächlich der Adressierung im Netz. |
| **ISP** | Internet Service Provider - Firma die den Zugang zum Netz anbietet |
| **LINUX** | Leistungsfähiges Betriebssystem auf UNIX-Basis, das kostenlos ist |
| **Exploits** | Programme zur Ausnutzung einer Sicherheitslücke |
| **DoS-Angriff** | Denial of Service, Angriff auf den TCP/IP-Stack, der zum Stillstand des Rechners führt |
| **Toolkit** | Sammlung von Programmwerkzeugen |
| **Sniffer** | Ein Programm zum "erschnüffeln" von Paßwörtern, Tastatureingaben, Datenverkehr im Netz, etc. |
| **BO** | Back Orifice - ein Trojanisches Pferd (= Programm, das etwas anderes macht, als es vorgibt zu tun) |
| **PlugIn** | Zusatz zu einem Programm mit speziellen Funktionen |
| **SMB** | System Message Block / Server Message Block |
| **DIAL-IN** | Einwahlmöglichkeit per Telefon ins Internet |
| **Port** | Verbindungsnummer für bestimmte Dienste, die auf einem Rechner laufen |
| **Proxy** | Stellvertreter Rechner |
| **IRC** | Internet Relay Chat (eine Art „CB-Funk" im Netz) |
| **Browser** | Programm zum "Stöbern" in Inter-/Intranet |
| **PWL -Datei** | Passwortdatei von Windows 95 /98 |
| **FTP** | File Transfer Protocol, dient der Übertragung beliebiger Daten (Dokumente, Programme etc.) |
| **Winsock** | TCP/IP- Stack von Windows 95/98/NT |
| **Stack** | Eine Liste von Protokollen, die von einem bestimmten System genutzt werden - ein Protokoll pro Schicht (ISO-OSI-Modell) - wird Protocol Stack genannt |
| **ISO-OSI** | „International Standardization Organization" (ISO) - „Open Systems Interconnection" (OSI), sieben Schichten-Modell |

# Berliner Polizei ermittelt im Internet

kg Das Internet bietet neue, bisher nicht dagewesene Möglichkeiten der Informationsbeschaffung für denjenigen der einen Internetzugang hat. Fast täglich wird zudem ein weiterer Lebensbereich auch durch das Internet zugänglich gemacht. Man denke nur an das virtuelle Einkaufen oder Internetbanking um nur zwei Beispiele zu nennen. Die sich ständig erweiterten Möglichkeiten, die das Internet bietet, werden aber auch zu kriminellen Zwecken mißbraucht. Auch hier unterscheidet sich das Internet nicht von der realen Welt. Um das Verbrechen in dieser, stark von Technik geprägten Welt, erfolgreich bekämpfen zu können, ist ein erheblicher technischer Sachverstand notwendig. Auch in Berlin wurde dies erkannt und eine Ermittlungsdienststelle eingerichtet, deren Aufgabe ausschließlich die Durchführung von technischen Ermittlungen im Internet ist. Diese sog. AG-Internet ist beim Landeskriminalamt angesiedelt und unterstützt alle Ermittlungsdienststellen der Berliner Polizei bei der Verbrechensbekämpfung wenn ein Bezug zum Internet besteht. Seit Anfang 1999 arbeiten hier mehrere Spezialisten, deren Hauptaufgabe die Ermittlung von Straftätern im Internet ist.

## *Das Internet bietet keine Anonymität*

Dabei kommt den Ermittlern zugute, daß das Internet keineswegs ein anonymes Kommunikationsmedium ist, für das es von vielen gehalten wird. Um die aus dem Internet abgerufenen Daten der richtigen Person zustellen zu können, braucht jeder Teilnehmer im Internet ein eindeutige Adresse, die sog. IP-Nummer. Diese Nummer wird bei allen Kommunikationsvorgängen im Internet mitprotokolliert, wodurch Absender und Empfänger von Daten jederzeit eindeutig identifiziert werden können. Auch die sog. dynamische IP-Adresse, bei der eine IP-Nummer mehreren Personen zeitlich nacheinander zugeteilt wird, ist nicht anonym, da bei den Providern Benutzername, IP-Nummer und Zeitangaben mitprotokolliert werden. Geht es nun darum den Erzeuger von strafrechtlich relevanten Internetinhalten zu ermitteln, braucht der Internetfahnder nur noch den Weg der IP-Adressen zurückzuverfolgen und gelangt so direkt zum Täter. Im Einzelfall bedeutet dies, daß die Protokolldaten der am Kommunikationsvorgang beteiligten Computer gesammelt werden und die relevanten Einträge wie in einem Puzzle zusammengesetzt werden. Sind alle Teile vorhanden und in die richtige Reihenfolge gebracht worden, so läßt sich der Weg der Daten vom Absender bis zum Empfänger lückenlos nachvollziehen. Aus technischer Sicht sollte es also fast immer möglich sein, den Weg der Daten vom Absender zum Empfänger nachzuvollziehen und die Verantwortlichen für strafrechtlich relevante Daten zu ermitteln. Daß es im Einzelfall doch einmal Probleme geben kann, liegt dann in der Regel daran, daß evtl. nicht mehr alle benötigten Daten zur Verfügung stehen.

## *Schwerpunkt Pornographie/ Kinderpornographie*

Bei den zur Ermittlung anstehenden Delikten handelt es sich bisher hauptsächlich um Straftaten, bei denen die transportierte Information selbst strafbar ist. An erster Stelle ist hier die Verbreitung von Pornographie bzw. von Kinderpornographie zu nennen. Aber auch die Verbreitung verfassungsfeindlicher Schriften und Symbole über das Internet gehört zu den Schwerpunktdelikten. Zudem ist festzustellen, daß mit der Kommerzialisierung des Internet auch immer mehr die Betrugsstraftaten im Internet an Bedeutung gewinnen. Teilweise handelt es sich hier um bekannte Straftaten wie z.B. Warenkreditbetrug, die unter Ausnutzung eines neuen Kommunikationsmediums verübt werden. Andere Straftaten, wie z.B. die Verbreitung von Pornographie bzw. Kinderpornographie haben durch das Internet einen ganz neuen Stellenwert bekommen, da das Internet die Möglichkeiten der Verbreitung und Vervielfältigung potenziert.

Gerade an dem Beispiel Kinderpornographie zeigt sich, wie schnell sich auch der normale Internetbenutzer unter Umständen strafbar machen kann. Hier kollidiert das internationale Internet mit den Gesetzgebungen der unterschiedlichen Länder, die am Internetverkehr teilnehmen. Während in Deutschland bereits der Besitz von Kinderpornographie strafbar ist, haben sich andere Länder dieses Problems per Gesetz noch nicht angenommen. Die Erfahrung zeigt allerdings, daß der normale Internetbenutzer nicht unvermittelt auf Kinderpornographie stößt. Wer allerdings ausgiebig Webseiten aufsucht, auf denen Pornographie und sexuelle Dienstleistungen aller Art angeboten werden, kann unter Umständen auf Bildmaterial stoßen, welches in den Bereich Kinderpornographie fällt. Hierbei ist vielen Internetbenutzern vielleicht nicht klar, daß bei der Betrachtung eines Bildes auf einer Webseite eine Kopie dieses Bildes im Cachespeicher des PC abgespeichert wird. Handelt es sich bei dem Bild um Kinderpornographie, befindet sich diese nun im Besitz des Benutzers, da sie auf seinem PC abgespeichert wurde. Im Prinzip besteht hier die Möglichkeit, daß sich der Internetnutzer damit strafbar macht. Je nach Einstellung der jeweiligen Browser-Software kann ein Bild im Cache durchaus mehrere Wochen oder Monate gespeichert bleiben, bis es gelöscht oder durch neue Daten überschrieben wird. Um der Gefahr zu entgehen sich strafbar zu machen, sollte man Webseiten meiden, auf denen Pornographie oder sexuelle Dienstleistungen angeboten werden.

Hier sollte man auch das bereits gesagte in Bezug auf die Rückverfolgbarkeit der Daten im Internet berücksichtigen. Im Internet ist nicht nur der Absender ➔

← der Daten, sondern auch deren Empfänger eindeutig zu ermitteln. Sollte also z.B. der Webserver eines Anbieters von Kinderpornographie ermittelt und sichergestellt werden, so sind durch Auswertung der gespeicherten Protokolldateien auch alle Personen ermittelbar, welche sich die Webseiten angeschaut haben und damit evtl. Kinderpornographie in Ihrem Browsercache abgespeichert haben.

### *Gefahr durch Computerviren*

Eine weitere Gefahr aus dem Internet stellen Computerviren und sog. „Trojanische Pferde" dar. Computerviren können z.B. als Beigabe zu E-Mails versendet werden. Eine weitere Möglichkeit sich zu infizieren besteht dann, wenn man allzu sorglos die Zugriffsrechte für den eigenen PC freigibt. So können unerwünschte Aktivitäten auch dadurch verursacht werden, daß Webseiten mit aktiven Inhalten aufgerufen werden. Ist die Ausführung von Java- und insbesondere ActiveX-Code erlaubt, kann der in der aufgerufenen Webseite enthaltene Programmcode den eigenen PC völlig kontrollieren. Eine besondere Art der Bedrohung stellen dabei die „Trojaner" dar. Hierbei handelt es sich um Programmcode, der anscheinend harmlos ist, aber eine verborgene Hintertür zum PC öffnet. Bemerkt das Opfer den Angriff durch einen „Trojaner" nicht, hat der Angreifer die Möglichkeit über die Hintertür alle Daten des Opfers auszuspähen und sogar neue Daten und Programme auf den Computer des Opfers zu laden. Durch diese Art der Spionage kann oftmals größerer Schaden angerichtet werden, als durch einen Virus der vielleicht „nur" ein paar Dateien löscht.

Wer nun meint, daß man vom Internet lieber die Finger lassen sollte weil es da nur so vor Gefahren wimmelt, liegt allerdings falsch. Das Internet bietet bei sachgerechter Anwendung vielfältigste Möglichkeiten, sich Informationen zu beschaffen, die früher viel schwerer zugänglich waren. Als Beispiel hierfür seien nur die Onlinebibliotheken genannt, die oft kostenlos ein Verzeichnis ihres kompletten Bestandes im Internet zur Verfügung stellen. Dadurch ist es möglich, in Sekundenschnelle Recherchen vom Internetarbeitsplatz durchzuführen, zu denen man sich früher durch Berge von Karteikarten „wühlen" mußte.

Um sich dennoch vor Ungemach aus dem Internet zu schützen, reichen schon einige simple Verhaltensmaßregeln.

- Wer sich nicht im Umfeld von Webseiten mit zwielichtigen Angeboten (z.B. Pornographie) aufhält, wird meist auch nicht mit strafrechtlich relevanten Webseiten in Berührung kommen.

- Genau wie in der normalen Umwelt sollte man nur Personen vertrauen, die man gut kennt. Wer von einer unbekannten Person eine E-Mail mit einem Programm zugeschickt bekommt und dieses Programm dann auch noch bewußt startet (z.B. aus Neugierde), muß sich hinterher fragen, ob er nicht eine Mitschuld daran trägt, wenn sein PC nachher mit einem Virus verseucht ist.

Gesunder Menschenverstand schützt besser als teure Spezialsoftware. Zur Absicherung des Restrisikos kann man dann immer noch auf kommerzielle Produkte wie z.B. Virenscanner zurückgreifen.

Nach Schätzungen soll die Gesamtmenge an Webseiten momentan ca. 900 Millionen betragen, mit stark steigender Tendenz. Trotz der ständigen Präsenz der Polizei im Internet kann es daher vorkommen, daß Webseiten mit strafrechtlich relevanten Inhalten eine Zeitlang unentdeckt bleiben. Hier ist die Polizei auf die Mithilfe aus der Bevölkerung angewiesen.

Ansprechpartner: AG-Internet, LKA 3-02 (Tel. 7672-56242), Computerkriminalität LKA 3126 (Tel. 7672-56281), Pornographie LKA 4134 (Tel. 699-32911), Kinderpornographie LKA 4138 (Tel. 699-32990) ◆

## Stateful Dynamic Signature Inspection (SDSI) für sichere Daten im Netz

Angesichts der weltweiten Vernetzung ist es für viele Unternehmen überlebenswichtig, ihre sensiblen Daten im Intranet gegen unberechtigte Zugriffe zu schützen. Die Installation einer Firewall ist ein probates Mittel, reicht aber meistens nicht aus. Mehr Sicherheit bieten professionelle Datenschützer in Form von Intrusion-Detection-Systemen (IDS): Sie erkennen Sicherheitslücken und reagieren automatisch darauf. Manche „Spürnasen" im Netz können sogar bei laufendem Betrieb aufgerüstet werden, um auch gegen neueste Sicherheitsrisiken gewappnet zu sein.

### *Wozu Intrusion Detection?*

Der beinahe explosionsartige Anstieg der Internetnutzung in nahezu jedem Unternehmen führt unweigerlich dazu, daß das einstmals vollständig nach außen abgeschirmte Intranet heute mindestens eine Verbindung zum offenen System Internet hat. Gleichzeitig nimmt die Komplexität interner Netze rapide zu – die Transparenz, was in so einem Netz alles passiert, aber im gleichen Maße ab. Als logische Folge entstehen Sicherheitslücken – die Daten sind in Gefahr.

Was ist zu tun? Man installiert zunächst eine Firewall. Bei korrekter Konfiguration und Verwaltung schützt diese „Brandmauer" das Netz wirkungsvoll gegen Attacken aus dem Internet.

In vielen Unternehmen ist man der Ansicht, daß diese Maßnahme zur Gewährleistung der Netzwerksicherheit bereits völlig ausreicht. Das ist aber ein großer Trugschluß: Denn Firewalls filtern den Datenverkehr, verhindern ihn aber nicht - daher können sie die ➔

← Integrität sensibler Daten nicht von vornherein garantieren. Darüber hinaus haben Firewalls keinen Einfluß auf unzulässige Aktivitäten, die innerhalb der Unternehmensnetze stattfinden. IT-Fachleute gehen davon aus, daß heute etwa 60 bis 80 Prozent aller Angriffe auf die Datenintegrität von innen kommen. Fazit: Firewalls sind ein sehr wichtiger Teil eines integrierten Sicherheitskonzepts, aber eben nur einer von mehreren. Das gilt genauso für andere Sicherheitskomponenten wie Security Scanner oder Verschlüsselungstools.

Das wichtigste Kontrollinstrument innerhalb interner Netze sind Intrusion-Detection-Systeme (IDS): Sie halten ständig Ausschau nach verdächtigen oder nicht autorisierten Aktivitäten im Netz und reagieren automatisch darauf. Webserver, Firewalls und Router, Anwendungen und Datenbanken werden so ständig überprüft. Im Gegensatz zu Sicherheitsscannern erfassen IDS nicht nur potentielle Schwachstellen im Netz, sondern sie erkennen in Echtzeit tatsächliche Angriffe auf die Datensicherheit. Man unterscheidet im wesentlichen zwei grundlegende Verfahren der Netzwerküberwachung: Netzwerk- und Host-basierte Intrusion-Detection-Systeme.

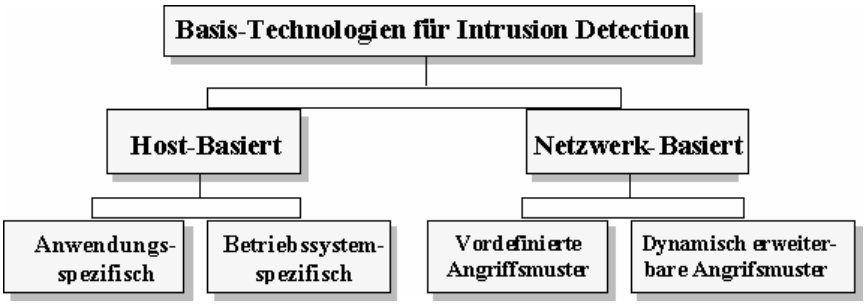
Das Netzwerk-basierte IDS entspricht der Überwachungskamera in einer Bank; das Host-basierte System ist in diesem Fall die Alarmanlage für den Tresor beziehungsweise für die Kasse.

### Die Alarmanlage: Host-basierte Intrusion Detection

Host-basierte Intrusion-Detection-Systeme überwachen die Aktivitäten an den einzelnen Systemen („Hosts“) und den daran angeschlossenen Geräten im Netz. Jede verdächtige oder nicht autorisierte Aktion über Webserver, Firewalls und Routern, in Anwendungen und Datenbanken wird in Echtzeit registriert.

Zu diesem Zweck überprüfen diese Systeme in erster Linie Protokolldateien. Jeder Zugriff auf einen Netzwerkrechner mit Angaben zum Beispiel über Benutzernamen, Paßwörter, Zugriffszeit und -dauer wird in die jeweilige Log-Datei eingetragen. Diese Informationen wertet das ID-System kontinuierlich aus. Kommt ihm dabei etwas verdächtig vor, schlägt es Alarm: zum Beispiel wenn ein nicht autorisierter Anwender mehrfach falsche Paßwörter für den Administrator-Zugang eingibt oder versucht, das Login-Programm zu überschreiben.

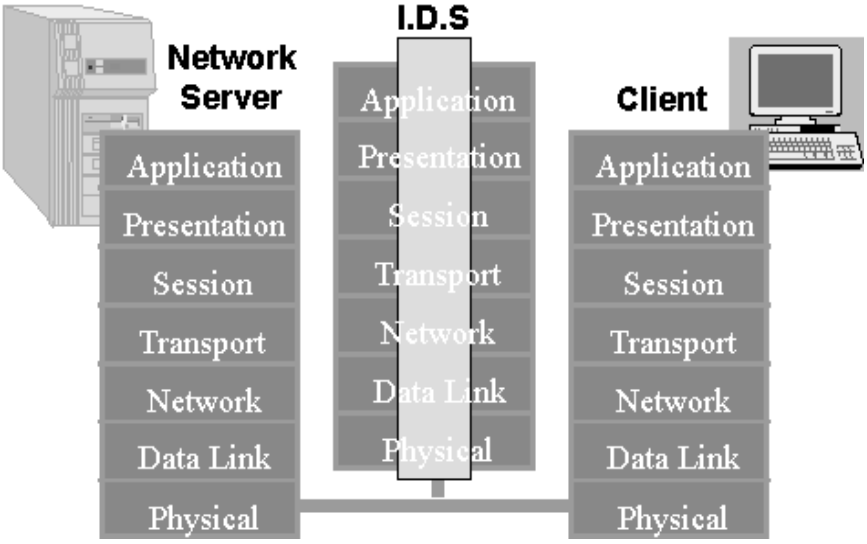
Host-basierte Systeme arbeiten entweder auf Betriebssystem- oder auf Anwendungsebene, das heißt, die Überprüfung erfolgt am Application Server, zum Beispiel Datenbank- oder Web-Server. Bei modernen IDS überwachen sogenannte Agents jedes einzelne System, auch bei weitverzweigten und komplexen Netzen. Diese Agenten sind mit mehreren Intrusion-Detection-Managern verbunden, die ihrerseits an die zentrale Intrusion-Detection-Konsole angeschlossen sind. Die Konsole dient zum Installieren und Updaten der Agenten, zur Definition von Abwehrszenarien und zum Verfolgen von Einbruchsversuchen im gesamten Netz. Trotz der komplexen Funktionsweise ist ein solches Manager/Agent-IDS relativ einfach in der Handhabung: Host-basierte IDS sind vergleichsweise leicht zu konfigurieren, die Sicherheitsüberprüfung kann an spezifische Anwendungen angepaßt werden. Allerdings ist es dabei nicht möglich, Attacken aufzuspüren, die auf einem Netzwerk-Übertragungsprotokoll basieren.




***Für die Suche nach Eindringlingen oder Saboteuren im Netz gibt es zwei verschiedene Basis-Technologien: Host-basierte Systeme kontrollieren einzelne Anwendungen oder Betriebssysteme am Host; Netzwerk-basierte überprüfen Datenpakete im Netzverkehr nach spezifischen Angriffsmustern. Diese sind vordefiniert; bei intelligenten Systemen können sie auch dynamisch erweitert werden.***

### Die Überwachungskamera: Netzwerk-basierte Intrusion Detection

Für große Multi-Plattform-Netze reicht es allerdings nicht aus, nur einzelne Betriebssysteme oder Applikationen zu überwachen. Vielmehr müssen hier alle Ebenen der Kommunikation im Netz auf Unregelmäßigkeiten überprüft werden. Diese Anforderung erfüllen Netzwerk-basierte Intrusion-Detection-Systeme, die zwischen Client und Server „sitzen“, dabei den Netzverkehr nach verdächtigen Aktivitäten überprüfen und anschließend entsprechende Gegenmaßnahmen einleiten. Netzwerk-basierte IDS analysieren die einzelnen Datenpakete in Netzwerksegmenten und vergleichen diese mit bekannten Angriffsmustern, sogenannten Attack Signatures. Nicht autorisierte Zugriffe werden identifiziert, aufgezeichnet und beendet. Der Vorteil: Die Software muß nicht in jedem einzelnen System installiert werden, die Überwachung erfolgt tatsächlich in Echtzeit und ohne Performance Overhead am Server oder bei Anwendungen. Darüber hinaus ist diese Art der Intrusion Detection komplett plattformunabhängig. Angriffsarten, →

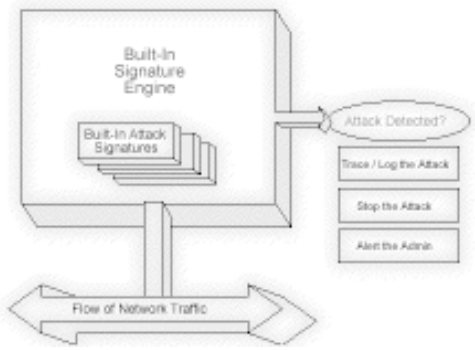



← die mit der Überwachung des Netzverkehrs erkannt und bekämpft werden können, sind unter anderem Ping of Death, Syn Flood, Teardrop, WinNuke oder Back Orifice.

**Netzwerkbasierte Intrusion-Detection-Systeme überwachen alle Ebenen der Kommunikation im Netz.**

Ein praktisches Beispiel für den Nutzen Netzwerk-basierter IDS sind von Host-basierten Systemen nicht bemerkte Denial-of-Service-Attacken. Diese führen dazu, daß das Netz bestimmte Dienste wegen Überlastung nicht mehr anbieten kann, in schlimmeren Fällen aber auch den Ausfall ganzer Systeme zur Folge haben können. Das geht ganz einfach: Man schickt beispielsweise ein Datenpaket an einen Router und gibt als Absender und Empfänger dieselbe IP-Adresse an – die des Routers. Dieser versucht das Paket daraufhin immer wieder an sich selbst zu senden und blockiert sich damit auch selbst. Das Intrusion-Detection-System erkennt den Trick und beendet den Angriff.

Ganz entscheidend für die Netzwerk-basierte Störungssuche ist die Art und Weise, wie Eindringlinge aufgespürt werden: Die meisten Intrusion-Detection-Systeme überprüfen den Netzverkehr rein statisch, das heißt, sie erkennen Attacken ausschließlich auf Basis vordefinierter Angriffsmuster, die im System gespeichert sind. Für jedes einzelne Angriffsmuster („Attack Signature“) ist dabei eine eigene Routine erforderlich. Dieses Verfahren hat zwei wesentliche Nachteile: Erstens sind solche Systeme nicht lernfähig – jede neue Attack Signature muß einzeln „nachinstalliert“ werden, und in dieser Zeit findet keine Überwachung statt; zweitens wird die Performance des IDS mit jeder zusätzlichen Abwehrroutine schlechter - je mehr Angriffsmuster erkannt und abgewehrt werden, desto langsamer läuft der gesamte Vorgang.




Herkömmliche Netzwerk-basierte Intrusion Detection-Systeme verwenden ausschließlich vordefinierte („Built-in“) Angriffsmuster. Für jedes Update muß das IDS komplett vom Netz genommen werden.

### *Effizienter Datenschutz mit Stateful Dynamic Signature Inspection-Technologie*

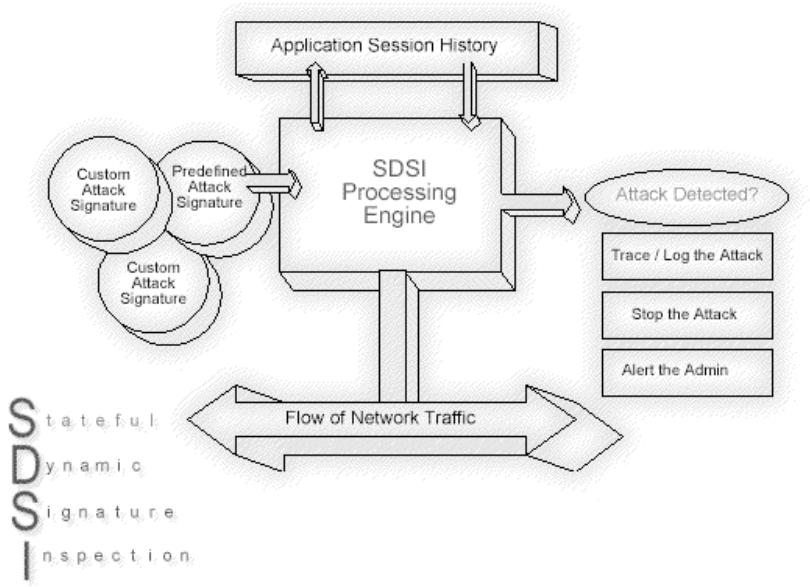
Um diese Beschränkungen aufzuheben, setzt Axent auf die sogenannte Stateful Dynamic Signature Inspection-Technologie (SDSI). Was bedeutet das?

Ein wesentlicher Fortschritt liegt darin, daß die Software nicht mehr vom Netz genommen werden muß, wenn neue Angriffsmuster hinzugefügt werden. Die Erweiterung erfolgt dynamisch, sozusagen „on the fly“ – gefährliche zeitliche Lücken im Monitoring gibt es nicht mehr.

Ein weiterer Vorteil: Die Software bietet dem Systemadministrator die Möglichkeit, die Funktionsweise des Abwehrsystems unternehmensspezifisch zu beeinflussen, das heißt festzulegen, was zusätzlich zu den standardmäßig gespeicherten Angriffsmustern entsprechend der eigenen Sicherheitsstrategie als Angriff gewertet und damit bekämpft wird. Sämtliche Attack Signatures werden als eine Befehlskette betrachtet, die der „virtuelle Prozessor“ des IDS nacheinander ausführt. Diese Befehlsketten können entsprechend individuell erweitert und verändert werden. Für jeden kontrollierten Server im Netz gibt es ein eigenes Paket von Angriffsmustern, sowohl für das Betriebssystem als auch für die Applikationen, die der Server unterstützt.

Hinzu kommt: Der Datenverkehr im Netz wird wesentlich effizienter analysiert und beeinträchtigt ihn daher weniger stark. Um die Performance des Netzverkehrs nicht zu belasten, prüft der virtuelle Prozessor nicht alle „vorbeikommenden“ Datenpakete, sondern nur die potentiell gefährlichen. Als Hilfsmittel dient dabei ein →

← spezieller Cache, in dem protokollierte Informationen über den Status der aktuellen Anwendungssitzung gespeichert werden. Und diese Informationen berücksichtigt das IDS bei der Datenanalyse: Pakete, die eindeutig der aktuellen Anwendungssitzung zuzuordnen sind, können das IDS ohne Detailkontrolle passieren.




Mit SDSI-Technologie sind die Attack Signatures dynamisch erweiterbar. Die Angriffsmuster können benutzerspezisch angepaßt werden. Bei der Paketprüfung berücksichtigt das System Daten der aktuellen Anwendungssitzung.

### *Zusammenfassung: Vorteile der SDSI-Technologie gegenüber herkömmlichen Systemen*

- Der „virtuelle Prozessor" versteht Angriffsmuster als komplexe Anweisungen (Befehlsketten); individuell ausformulierte Attack Signatures werden so bei der sicherheitsrelevanten Paketanalyse berücksichtigt.
- Die Netzwerk-Überwachung wird dynamisch – das heißt in Echtzeit und ohne Abstriche an der Performance - um zusätzliche Angriffsmuster ergänzt.
- In einem speziellen Cache gespeicherte Informationen zum Status der aktuellen Anwendersitzung werden bei der Paketüberprüfung berücksichtigt und optimieren so die Überprüfung des Netzverkehrs.
- Höhere Performance im Datendurchsatz, weil nicht alle Pakete geprüft werden, sondern nur die potentiell bedrohlichen.

Weitere Informationen sind von der AXENT Technologies, Siedlerstraße 2, 85774 Unterföhring, Tel.: 089 - 99 549-110, Fax: 089 - 99 549-200, Internet: http://www.axent.com, zu bekommen. ◆

***Elektronische Post verschlüsselt und mit elektronischer Unterschrift***

## Sichere Intranet/ Internet-Mail (Secure Mail)

kg

Wer über einen Windows NT-Arbeitsplatzrechner verfügt, der über das lokale Netzwerk (LAN) mit dem Intranet des Berliner Landesnetzes verbunden ist und bereits die Dienste im elektronischen Postverbund der Berliner Verwaltung (Exchange- oder SMTP-Mail) nutzt, kann mit einem neuen Angebot des Landesbetriebes für Informationstechnik (LIT) die Kommunikation sicher durchführen. Mit den Kommunikationspartnern kann die elektronische Post verschlüsselt und nach den Regelungen des Signaturgesetzes mit einer elektronischen Unterschrift versehen ausgetauscht werden.

Die Kommunikationspartner benötigen dazu eine Authentifizierungs- und Verschlüsselungssoftware in den Mail-Programmen, die dem MailTrust Standard (mtt) entsprechen. Dieser Standard wurde von deutschen Kryptoherstellern in Zusammenarbeit mit dem Bundesministerium des Inneren erarbeitet und erprobt. Künftig wird diese Sicherheitssoftware auch den Internet-Sicherheitsstandard S/MIME unterstützen, so daß dann weltweit sicher kommuniziert werden kann.

Der LIT bietet dazu in der Berliner Landesverwaltung folgende Komponenten an:

- Ausstellung eines PSE (Personal Security Environment) mit einem geheimen Schlüssel (PrK) und einem vom LIT elektronisch unterschriebenen öffentlichen Schlüssel (PbK), dem Zertifikat. →

- Verwaltung des Zertifikates: Einstellen in einen Verzeichnisdienst, Sperren auf Antrag, Verlängerung der Gültigkeit, Neuausstellung bei Verlust, gesicherte Aufbewahrung aller Zertifikate, damit archivierte verschlüsselte Dokumente wieder entschlüsselt werden können.

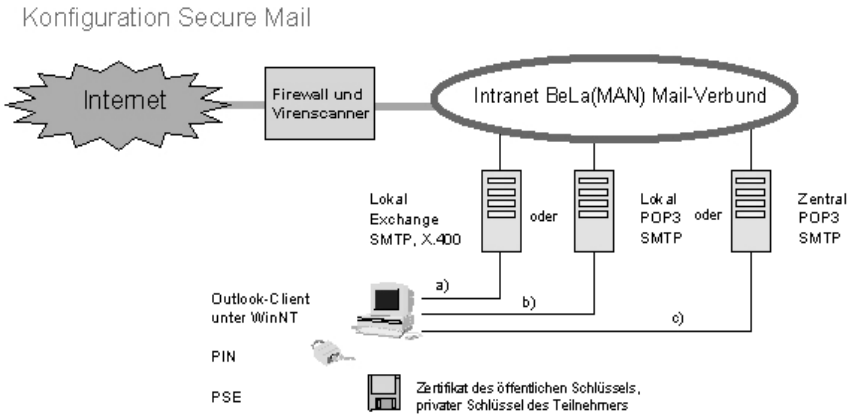
- Bereitstellung einer Sicherheitssoftware mit Installationsanleitung und elektronischem Benutzerhandbuch für den Outlook97/98-Client. Mit diesem Client kann die elektronische Post nach dem mtt-Standard verschlüsselt und unterschrieben versandt und empfangen werden. Auf Anforderung unterstützt der LIT die Installation dieser Sicherheitssoftware.

- Bereitstellung eines Outlook98-Clients, sofern dieser noch nicht im Exchange-System oder MS Office installiert wurde.

- Bereitstellung eines elektronischen Postfachs (POP3-Account) auf dem zentralen SMTP-Server (Mail-Server) der Berliner Verwaltung für einen zu vereinbarenden Zeitraum, wenn kein lokales Mail-System verfügbar ist (POP3: ein Protokoll zum Übertragen von Intranet/Internet-Mail vom SMTP-Server auf einen Arbeitsplatzrechner).

### *Schematische Darstellung Secure Mail*

Voraussetzung für die Nutzung des Dienstes ist der Anschluß an das Berliner Landesnetz (BeLa) bzw. ein Zugang per Telefoneinwahl. Soll der Mail-Server mit dem SMTP-Backbone im Land Berlin verbunden werden, so ist ein eigener DNS-Server (Domain Name System) oder ein vom Service- und Administrations-Zentrum (SAZ) des LIT bereitgestellter DNS-Server notwendig.




a) Anwender hat eigenen Exchange-Server

b) Anwender hat eigenen Mail-Server mit Postfächern (z.B. LinkWorks, OnGo)

c) Anwender nutzt zentralen Mail-Server des LIT

Die Kommunikation kann über 3 verschiedene Anbindungsmöglichkeiten an den Mail-Verbund geführt werden.

Die nachfolgende Abbildung zeigt die Vorgehensweise zur Ausstellung eines PSE. Dieses Verfahren ist konform zum Signaturgesetz. Das TrustCenter LIT ist ➔

## PC-Viren? Keine Panik!

kg

Wie das Einsteigermagazin Computer easy berichtet, lauern jeden Monat alleine im Internet bis zu 200 neue Virenarten auf ungeschützte Rechner. Killer-Software wie Melissa oder der CIH-Virus sorgte in letzter Zeit weltweit für Schäden und Aufregung. Dennoch sollten Anwender nicht in Panik verfallen. Mit geeigneten Maßnahmen sind die ungebetenen Eindringlinge sicher abzuwehren.

In der Septemberausgabe testete die Computer easy die acht wichtigsten Anti-Viren-Programme. Ausführliche Erläuterungen der „Ansteckungswege" und der „Therapie" des Rechners machen deutlich, wie der Schutz per Software auf dem eigenen Rechner eingerichtet wird.

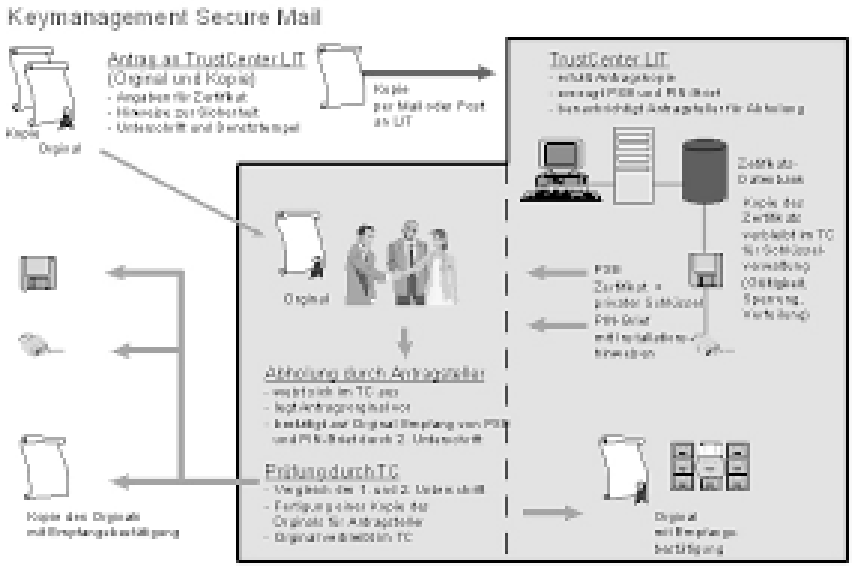
Laut Computer easy eignet sich das Antiviren-Kit von G-Data am besten für die Beseitigung bereits eingedrungener Viren. Norton Antivirus wurde wegen seiner einfachen Bedienung gelobt. Computer easy-Testsieger wurde VirusScan 4.02 von MacAffee. Es ist als einziges Schutzprogramm in allen Bereichen gleichmäßig gut und läßt kaum Wünsche offen. Mit rund 70 Mark liegt dieser „Ansteckungsschutz" auch beim Preis-Leistungs-Verhältnis auf Platz eins.

Im gleichen Heft werden auch ausführlich und verständlich die wichtigsten Schutzmaßnahmen für den eigenen PC beschrieben. Vom Passwort-Schutz beim Einschalten über das Kennwort beim Windows-Bildschirmschoner bis zu Spezialprogrammen erklärt und bewertet die Computer easy geeignete Sicherheitsmaßnahmen. ◆

## Allgemeingültiger Leitsatz für mehr Datensicherheit:

Je mehr die Konfiguration vom Standard abweicht, um so schwieriger hat es ein Angreifer.

← aber nicht durch die entsprechende oberste Bundesbehörde zertifiziert, da hier sowohl technische Lösungen, als auch organisatorische Regelungen noch im Fluss sind. Innerhalb des Landes Berlin und mit dazu verbundenen Bundes- und Landesbehörden wird die Zertifizierung des LIT für behördliche Zwecke anerkannt (Cross-Zertifikat).




### *Voraussetzungen für die sichere E-Mail*

Es müssen beim LIT eine Ausstellung eines PSE und den Anschluß an Secure Mail beantragt werden. Dazu ist ein entsprechendes Formular auszufüllen und an den LIT zu schicken und danach kann das PSE abgeholt werden. Es ist vorgesehen das Schlüsselmanagement künftig dezentral durchzuführen, so dass dadurch mehr Sicherheit für den Anwender geboten wird. Die Installation wird in der Regel von der IT-Stelle selbst vorgenommen.

Für die Sicherheit des PSE ist jeder selbst verantwortlich. Im TrustCenter des LIT verbleibt lediglich das Zertifikat, aber nicht der geheime Schlüssel. Sollte dieser verlorengehen oder nicht autorisierten Personen bekannt werden, muß durch den LIT das Zertifikat gesperrt und ein neues PSE ausgestellt werden.

Das PSE wird zunächst auf Diskette, in einer späteren Version auf einer Chipcard bereitgestellt. Die Diskette/Chipcard muß eingelegt sein, wenn die Sicherheitsfunktionen genutzt werden soll. Mit einer PIN-Eingabe wird diese Funktionen freigeschaltet. Wenn der Arbeitsplatzcomputer kein Diskettenlaufwerk hat, muss das PSE auf der Festplatte oder einem Netzlaufwerk abgelegt werden. Der Schutz des PSE ist dabei aber eingeschränkt, wenn andere Nutzer, wie Administratoren, Zugriff auf die Festplatte oder das Netzlaufwerk haben.

Zur Abwicklung des Verfahrens ist der Abschluß einer Servicevereinbarung mit dem LIT Berlin notwendig. Die genannten Bezeichnungen und Spezifikationen stellen den technischen Stand zu diesem Zeitpunkt dar. Weitere Informationen gibt der Leiter des Fachbereiches KISS, Dr. Klaus Biedka, Telefon: (030) 90 12 60 01, Fax: (030) 90 12 31 12, eMail: Klaus.Biedka@lit.verwalt-berlin. oder der Vertrieb des LIT, Telefon: (030) 90 12 70 22, Fax: (030) 90 12 39 08, eMail: vertrieb@lit.verwalt-berlin.de. ◆

## Firewall-Systeme im Landesnetz

kg

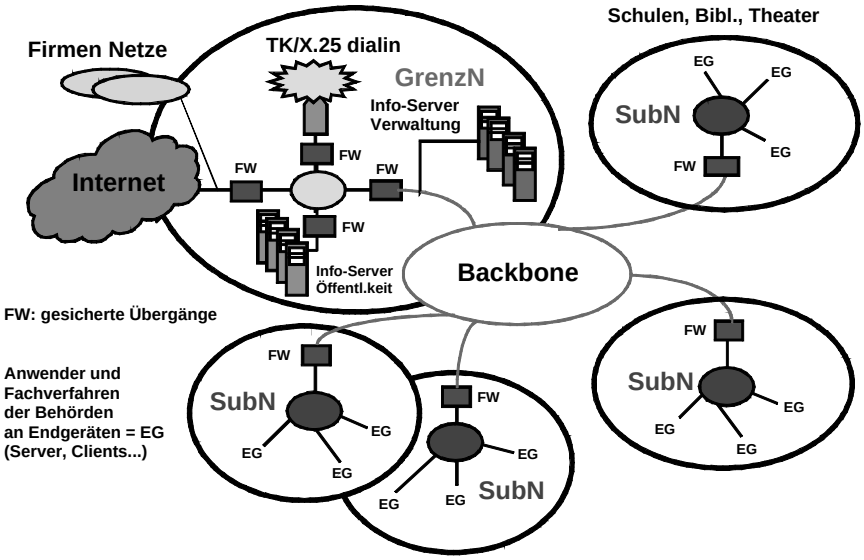
Der Landesbetrieb für Informationstechnik (LIT) betreibt ein Grenznetz, das über einen gesicherten Pfad (Firewall) mit dem Backbone (Netzwerkrückrat) des Verwaltungsnetzes verbunden ist. Durch diese Architektur wird ein besonders hohes Maß an Sicherheit gewährleistet. Server mit Informationsangeboten für das Internet befinden sich innerhalb des Grenznetzes in einer sogenannten demilitarisierten Zone (DMZ), Server mit Informationen für die Berliner Verwaltung werden in einem ComNet des Grenznetzes aufgestellt. Der Schutz des Berliner Landesnetzes mit Firewall-Systemen ist hierbei aus Sicherheitsgründen unabdingbar.

Unter einer Firewall („Brandschutzmauer") wird ein kontrollierter Übergange zwischen zwei Netzen verstanden, der überwunden werden muss, um Systeme im jeweils anderen Netz zu erreichen. Die Hauptaufgabe einer Firewall besteht darin, zu erreichen, daß jeweils nur zugelassene netzübergreifende Aktivitäten möglich sind und dass Missbrauchsversuche frühzeitig erkannt werden. Üblicherweise wird dabei davon ausgegangen, dass die Teilnehmer des internen Verwaltungsnetzes vertrauenswürdiger sind als die Teilnehmer des Internet.

Gleichwohl sind Firewall-Lösungen auch geeignet, die „grenzüberschreitenden" Aktivitäten der internen Nutzer, d.h. den Übergang zwischen verschiedenen Teilnetzen (z.B. Ressortnetze) innerhalb eines Verwaltungsnetzes zu begrenzen. Mit Hilfe von Firewall-Systemen lassen sich die vorher in der Kommunikationsanalyse definierten Anforderungen weitgehend technisch erzwingen.

Die Einrichtung lokaler Netze in der Berliner Verwaltung wächst ständig weiter. Hieraus sowie in →

## Netzarchitektur BeLa (MAN)




***Verbindung Internet und Backbone mit angeschlossenen Netzwerken***

← Umsetzung der Richtlinien des IT-Koordinationsausschuß Berlin (IT-KAB) resultiert ein ebenfalls steigender Bedarf an Firewall-Systemen zum Schutz dieser Netze. Bei der Vielzahl der Systeme sind ebenfalls zahlreiche IT-Stellen mit ihren Mitarbeitern/Innen incl. Vertreter/innen betroffen. Für die Kontrolle des ein- und ausgehenden Datentransfers ist demzufolge ein hoher Abstimmungsaufwand zu erwarten.

Aus den bisher gemachten Erfahrungen des LIT lassen sich folgende Aussagen zum derzeitigen Sachstand des Einsatztes solcher Systeme in der Landesverwaltung treffen:

- Es sind 15 Firewall-Systeme in der Berliner Verwaltung im Einsatz (Stand Juli 99).
- Der LIT betreibt davon vier Systeme (im Grenznetz und drei Kunden-Systeme). Weitere 13 Kundensysteme (Verwaltungen, Krankenhäuser) sind für dieses Jahr in Planung und werden durch den LIT realisiert.
- Das ausgewählte System der Firma Checkpoint (FW-1) hat sich vielfach bewährt. Das Produkt ist immer noch Marktführer.
- In den letzten zwei Jahren gab es nur einen Angriff auf den Grenznetz-Firewall mit Wirkung: Im Juli 98 wurde der extere DNS-Server zeitweilig zum Absturz gebracht. Die Logfiles der Firewall weisen täglich mehrere gezielte Angriffe aus, die aber bis auf die genannte Ausnahme alle ins Leere liefen.
- Zur Zeit bedienen sich 61 Kunden des LIT der Grenznetzdienste. Das Aufkommen der Datenübertragung vom und zum Internet hat sich gegenüber dem 1. Halbjahr 1998 verdoppelt, ohne dass Sicherheitsverletzungen nachzuweisen waren.
- Zunehmend werden Zugänge zum Landesnetz (MAN) für Servicezwecke sowie für Telearbeitsplätze eingerichtet.

Der Betriebsaufwand für Firewall-Systeme ist nicht zu unterschätzen. Man kann davon ausgehen, dass zwei Mitarbeiter/innen je System vorgehalten werden müssen (davon ein Mitarbeiter/in zu 100 Prozent, ein Mitarbeiter/in zu 20 Prozent). Im LIT sind Synergien durch den Betrieb vieler Firewall-Systeme und damit geringere Kosten möglich. Die Vorteile bei dieser Vorgehensweise liegen auf der Hand:

- Erfüllung der datenschutzrechtlichen Anforderungen.
- Angebot einer Komplettlösung (Sicherheitsanalyse, Beschaffung, Konfiguration, Betrieb) durch den LIT.
- Beschaffung über zwei Finanzierungsmodelle möglich.
- Preisgestaltung unter Berücksichtigung des zu erwartenden Arbeitsanfalls, Staffelung nach der Anzahl der zu verwaltenden Adressen.
- Einsatz von geschulten LIT-Mitarbeitern in diesem sicherheitsrelevanten Aufgabenbereich.
- Keine zusätzlichen Belastungen für den Auftraggeber durch Personaleinsatz, Schulungen usw.
- Möglichkeit zur Gestaltung und Kontrolle der LIT - Leistungen.
- Reduzierung des Abstimmvolumens zwischen den Verwaltungen, ohne deren dezentrale Verantwortung zu beeinträchtigen.

Weitere Informationen gibt der Leiter des Fachbereiches KISS im LIT, Dr. Klaus Biedka, Telefon: (030) 90 12 60 01, Fax: (030) 90 12 31 12, Klaus.Biedka@lit.verwalt-berlin.de oder an der Vertrieb, Telefon: (030) 90 12 70 22, Fax: (030) 90 12 39 08, eMail: vertrieb@lit.verwalt-berlin.de. ◆

**FRAGEN ?**



**Rufen Sie an :**

**INFOLINE**

**VERTRIEB**

**90 12 (912) 60 80**

# Open Source-Software - eine neue Chance für die Sicherheit?

*OpenSource-Software kann durch ihre "Philosophie der nachhaltigen Transparenz" einen wesentlichen Beitrag zur Sicherheit von IT-Systemen leisten. Von PD Dr. Olaf Winkel, Institut für Politikwissenschaft der Universität Münster.*

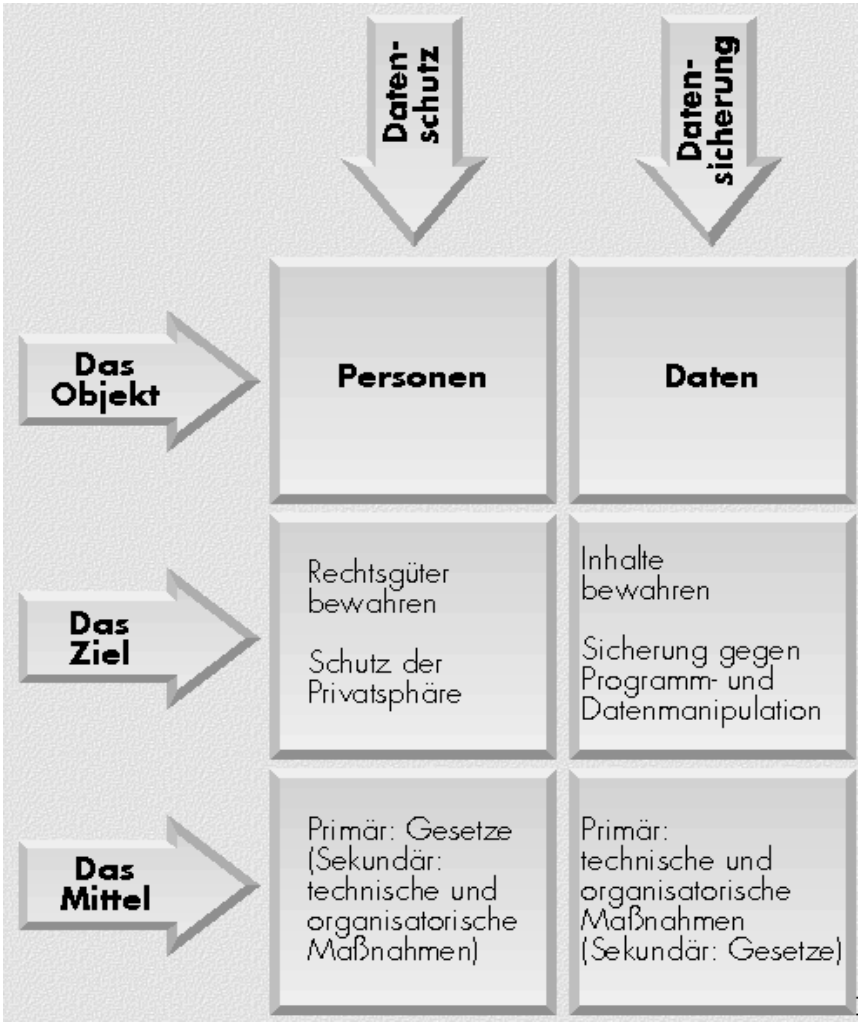
## *Open Source-Systeme auf dem Vormarsch*

Open Source steht für Software, deren Quellcode allgemein einsehbar ist, und die prinzipiell von jedermann geprüft, weiterentwickelt, an konkrete Bedarfslagen angepaßt und genutzt werden kann.

Dies ist nach den Spielregeln der Free Software Foundation (FSF) allerdings nur unter der Maßgabe erlaubt, daß die Modifizierungen und Ergänzungen wieder in den allgemein verfügbaren Quellcodebestand zurückfließen und damit wiederum selbst einer breiten Öffentlichkeit von Programmierern und Anwendern zugute kommen können. Die auf diese Weise ausgelösten Schneeballeffekte haben dazu geführt, daß freie Software für die sogenannten proprietären Systeme inzwischen in unterschiedlichen Bereichen zu einer ernstzunehmenden Konkurrenz geworden sind. Als proprietäre Systeme, die bis heute die Softwarelandschaft bestimmen, bezeichnet man Produkte wie die des Marktführers Microsoft, deren Quellcodes von ihren Besitzern als zentrales Unternehmensgeheimnis angesehen und eifersüchtig gehütet werden.

Zu den erfolgreichen Open Source-Systemen zählen das Serverprogramm Apache, das heute über die Hälfte aller Webdienste steuert, die E-Mail Software Sendmail, die inzwischen zwei Drittel der elektronischen Post verteilt, ➔

# Definitionssache: Datenschutz - Datensicherheit

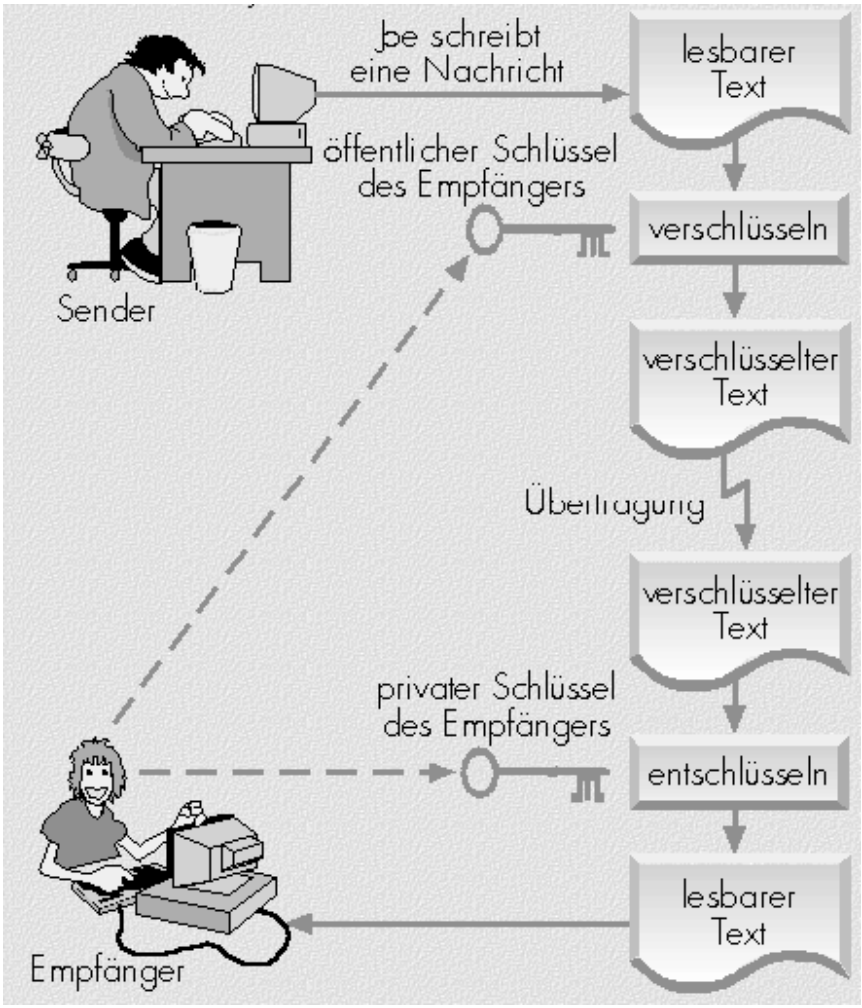



## *Verschlüsselung,*

Kodieren (Code) von Daten mit dem Zweck, sie unleserlich zu machen. Mittel der Datensicherheit, um selbst denen, die sich Zugriff auf Daten verschaffen, das Verstehen der Nachrichten unmöglich zu machen.

Man unterscheidet symmetrische und asymmetrische Verschlüsselungsverfahren. Bei symmetrischen Verfahren wird zum Verschlüsseln und zum Entschlüsseln der gleiche Schlüssel verwendet, wobei das Problem der Übersendung des Schlüssels entsteht. Bei asymmetrischen Verfahren (z.B. RSA) gibt es zwei Schlüssel. Man kann mit Schlüssel A verschlüsseln und mit Schlüssel B entschlüsseln aber auch mit Schlüssel B verschlüsseln und dann mit Schlüssel A entschlüsseln. Wenn man den einen Schlüssel als sog. Private Key geheimhält und den anderen als sog. Public Key veröffentlicht, ergeben sich zwei Anwendungstypen:

a) Vertrauliche Nachricht: Nur der gewollte Empfänger kann sie entschlüsseln. Prinzip: Die Verschlüsselung erfolgt mit dem Public Key des Empfängers (siehe Grafik). ➔




← b) Elektronische Unterschrift: Absender und Inhalt sind authentisch. Prinzip: Verschlüsselung mit dem Private Key des Absenders.

### *Viren,*

inzwischen auch in den Computer eingekehrte Krankheitserreger. Computerviren arbeiten ähnlich wie Bio-Viren durch Selbstkopie. Die Infektion geschieht durch Datenkontakt in Netzen oder durch Einsatz bereits infizierter Software, meist in Form von „Raubkopien". Die ausgelösten Krankheiten reichen von harmlos über schlimm bis „tödlich" , d.h. totaler Datenverlust. Wie Grippe-Viren sind die Schädlinge äußerst wandlungsfähig und schwer zu bekämpfen. Auch die Inkubationszeiten sind unterschiedlich lang.

Quellenangabe: alle Definitionen aus dem GMO-Lexikon (http://www.gmo.de/htmlpages/gmolex.htm). Das GMO Lexikon ist auf der WebSite in einer ständig aktualisierten Version verfügbar Die GMO ist eine Unternehmensberatung für Management- und Organisationskonzepte und ihre Umsetzung. Die Firma berät Kunden bei der Optimierung ihrer Geschäftsprozesse durch Integration aller Leistungsfaktoren, insbesondere in Fragen des effektiven Einsatzes der Informationstechnik. ◆

← und insbesondere das Betriebssystem Linux, dessen Nutzerzahl nach den neuesten Schätzungen zwischen zehn und fünfzehn Millionen liegt. Seit etwa einem Jahr ist der Trend zu beobachten, daß sich immer mehr Branchenriesen - unter ihnen auch Netscape/AOL, Apple, IBM und SAP - gegenüber der Open Source-Bewegung aufgeschlossen und oder zumindest kooperationsbereit zeigen. Selbst beim Marktführer Microsoft denkt man inzwischen laut darüber nach, zumindest gewisse Teile des Windows-Quellcodes kostenlos abzugeben.

### *Netzwerksicherheit als vielschichtiges Phänomen*

Die Behandlung der Frage, ob und inwieweit die Open Source-Bewegung neue Chancen eröffnet, um die IT-Sicherheitslage von Unternehmen, Behörden und Haushalten zu verbessern, wirft die Frage auf, was unter Netzwerksicherheit überhaupt zu verstehen ist und auf welchen Faktoren sie beruht. Gemeinhin werden in diesem Zusammenhang vier Sicherheitsdimensionen unterschieden, und zwar die der Verfügbarkeit, der Verbindlichkeit, der Integrität und der Vertraulichkeit.

Verfügbar sind Informationen und Kommunikationsbeziehungen, wenn ein berechtigter Anwender im Bedarfsfall auf sie zugreifen kann. Verfügbarkeitsverluste treten ein, wenn die Funktionsfähigkeit der Systeme beeinträchtigt ist, die der Verarbeitung, Speicherung und Übermittlung von Informationen dienen.

Als verbindlich gelten Kommunikationsakte, wenn sie den Kommunikationspartnern verläßlich und nachweisbar zugeordnet werden können.

Integrität steht für die unverfälschte Übertragung von Informationen zwischen berechtigten Partnern, und sie geht verloren, wenn Nachrichten auf ihrem Weg zwischen Absender und Adressatem durch Dritte manipuliert werden. ➔

← Als vertraulich bezeichnet man Informationen und Kommunikationsbeziehungen, die nur ausgewählten Teilnehmern bekannt sein sollen.

Schädigende Vertraulichkeitsverluste können nicht nur durch einen unberechtigten Zugriff auf Informationsinhalte entstehen - etwa durch das Abfangen eines per Telefax übermittelten Angebotes - sondern ebenso durch eine unberechtigte Kenntnisnahme von Kommunikationsakten. Man denke etwa an eine Privatperson, die mit der Schuldnerberatung Kontakt aufnimmt, oder an einen Informationsaustausch zwischen Unternehmensleitern, der auf die Bildung einer neuen strategischen Allianz schließen läßt.

Die Übertragung wesentlicher gesellschaftlicher und wirtschaftlicher Kooperationsbeziehungen auf offene Netzwerke - populäre Begriffe wie Electronic Commerce, Electronic Banking und Teleadministration bezeichnen hier nur die Spitze eines Eisberges - ist allein unter der Voraussetzung möglich, daß Verfügbarkeit, Verbindlichkeit, Integrität und Vertraulichkeit von Informationen und Kommunikationsbeziehungen gewährleistet sind. Und dies gilt nicht nur in objektiver Hinsicht, d.h. im Sinne von faktischer Verläßlichkeit, sondern ebenso in subjektiver Hinsicht, d.h. im Sinne der Entwicklung von Sicherheitsvertrauen.

So kann ein sicherheitstechnisch einwandfreier Kommunikationsdienst, dem aber der Ruf anhaftet, daß die mit seiner Hilfe übermittelten Informationen mit großer Wahrscheinlichkeit verloren gehen, verfälscht werden oder in die falschen Hände geraten, die ihm zugedachten Transportaufgaben ebenso wenig erfüllen wie ein technisch einwandfreies Passagierflugzeug, von dem man aber allgemein annimmt, daß es die nächsten hundert Flugkilometer nicht überstehen wird. Auf der anderen Seite ist die Herausbildung von Vertrauen in ein technisches System aber auch davon abhängig, ob und inwieweit es sich im alltäglichen Gebrauch als faktisch zuverlässig bewährt. Wo gravierende Mängel vorliegen, die immer wieder zu Betriebsstörungen und Unfällen führen, ist selbst die beste Öffentlichkeitsarbeit nicht in der Lage, Sicherheit zu suggerieren.

## *Open Source und faktische Sicherheit*

Im Hinblick auf die tatsächliche Verläßlichkeit von Informationen und Kommunikationsbeziehungen weisen Open Source-Produkte sowohl Vorteile als auch Nachteile auf. Die entsprechenden Stärken resultieren vor allem daraus, daß die breit angelegte Kooperation bei der Softwareentwicklung und die kontinuierliche Veränderung und Infragestellung des Bestehenden gute Voraussetzungen für die Herausbildung von Lösungen bieten, die unter Aspekten der Verfügbarkeit, Verbindlichkeit, Integrität und Vertraulichkeit gleichermaßen überzeugen können.

Die Philosophie der nachhaltigen Transparenz findet ihren Ausdruck auch darin, daß innerhalb der Open Source-Community allgemein zugängliche Fehlerdatenbanken geführt werden: Benutzer können jederzeit Fehlerberichte einschicken und werden sofort informiert, wenn die Bearbeitung eines Problems abgeschlossen ist. Vertraulichkeitsverletzungen, wie sie etwa manche Anwender von Windows 95 hinnehmen mußten, weil der Explorer das Setzen von sogenannten Controls ermöglicht und damit Angreifern die Chance gibt, den Inhalt einer Festplatte zu analysieren, sind unter derartigen Bedingen kaum zu erwarten.

Gerade in Anbetracht der Tatsache, daß Sicherheit kein statisches, sondern ein dynamisches Gut ist, das in einer sich stetig wandelnden Umwelt immer wieder neu hergestellt werden muß, erscheint die Fähigkeit bedeutsam, Sicherheitsprobleme unverzüglich aufdecken und im Rahmen eines tragfähigen Sicherheitsmanagement einer raschen Bearbeitung zuführen zu können. Ein weiterer Vorteil von freier Software, dessen Genuß allerdings im wesentlichen den Kreisen der Serverbetreiber und der technisch versierten Nutzer vorbehalten bleibt, betrifft vor allem die Gewährleistung von Verfügbarkeit.

Er äußert sich darin, daß die hohe Flexibilität, die auf Open Source basierenden Anwendungen zu eigen ist, bei drohenden Verfügbarkeitsverlusten in ein effektives Krisenmanagement umgemünzt werden kann: So hat ein Unternehmen, das auf freie Software setzt, bei der Bewältigung des Jahr-2000-Problems größere Spielräume als eines, das mit proprietären Systemen arbeitet, weil potentielle Fehlerquellen und Risiken leichter erkannt und von Experten der eigenen Wahl entschärft werden können.

Die Nachteile, die Open Source-Systeme unter Gesichtspunkten der faktischen Sicherheit aufweisen, erwachsen nicht zuletzt daraus, daß es sich hier noch immer häufig um Produkte handelt, die Fachleute wie Informatiker und Programmierer in erster Linie mit Blick auf ihresgleichen entwickelt haben und weniger mit Blick auf eine breite Anwenderschaft. Viele Open Source-Programme haben keine graphische Benutzeroberfläche oder sind schwer zu installieren bzw. zu konfigurieren, häufig mangelt es an einer ausreichenden Unterstützung durch die Hardwarehersteller, und außerdem fehlt es nach wie vor an einem ausreichenden Support, d.h. an einer leistungsfähigen Hotline für die breite Anwenderschaft. Der letztgenannte Punkt ist insbesondere unter dem Verfügbarkeitsaspekt als gravierende Schwachstelle zu werten, die den marktbeherrschenden proprietären Konkurrenzprodukten in vielen Absatzbereichen einen entscheidenden Wettbewerbsvorteil verschafft. Im ungünstigsten Fall laufen technisch weniger versierte Nutzer von freier Software unter diesen Umständen sogar Gefahr, über einen längeren Zeitraum von →

← ihren Kommunikationsbeziehungen und digitalisierten Informationsbeständen abgeschnitten zu werden. Allerdings bemühen sich Teile der Open Source-Bewegung, diesem gravierenden Mangel durch die Gründung von entsprechenden Dienstleistungsunternehmen und die Kooperation mit geeigneten Partnern abzuhelfen, was den Trend der Kommerzialisierung dieses Bereiches weiter verstärkt.

### *Open Source und Vertrauensbildung*

Die positiven Erfahrungen, die von Serverbetreiber und technisch versierten Nutzern in der Vergangenheit mit der funktionellen Zuverlässigkeit von freier Software gesammelt werden konnten, haben in diesen Segmenten zu einem deutlichen Zuwachs an Vertrauen in die Sicherheit von Open Source-Produkten geführt. Außerdem schlägt hier der in den letzten Jahren offenkundig gewordene Umstand positiv zu Buche, daß das Prinzip der Vertrauensförderung durch Risikoverschleierung unter den Bedingungen der modernen Informationsgesellschaft immer weniger funktioniert, und daß Hersteller, Netzbetreiber und Diensteanbieter, die das Vertrauen ihrer Kunden gewinnen und bewahren wollen, gut beraten sind, wenn sie sich statt dessen an den Leitbildern der Transparenz und schnellen Reaktion orientieren.

Und schließlich ist das gute Image, das freie Software in Teilen der Anwenderschaft nicht nur unter Kostengesichtspunkten, sondern ebenso im Hinblick auf die Sicherheit von Informationen und Kommunikationsbeziehungen genießt, auch auf eine offensive Öffentlichkeitsarbeit zurückzuführen. Diese wird von den kommerziell ausgerichteten Kräften innerhalb der Open Source-Bewegung nicht nur in der virtuellen Welt der Netze betrieben, sondern auch auf Veranstaltungen wie dem Linux-Tag, der Ende Juni dieses Jahres in Kaiserslautern stattfand.

Auf der anderen Seite finden aber auch die Lücken in der Hardwareunterstützung, die Unzulänglichkeiten im Bereich der Office-Werkzeuge, die Schwächen in punkto Anwenderfreundlichkeit und insbesondere die Defizite im Support ihren Niederschlag darin, daß freie Software in breiten Schichten der IT-Nutzer nach wie vor auf Skepsis stößt. Ob die Bemühungen zur Beseitigung der Mängel ausreichen werden, um auch in diesen Segmenten einen nachhaltigen Vertrauenszuwachs zu erzielen, bleibt abzuwarten. Sollte dies nicht gelingen, werden Open Source-Produkte die Vormachtstellung der proprietären Software der Branchenführer in den meisten Massenmärkten wohl nicht gefährden können.

### *Open Source und elektronische Verschlüsselung*

Wenn man sich mit Fragen der Netzwerksicherheit befaßt, liegt es nahe, die elektronische Verschlüsselung anzusprechen: Lassen sich doch immerhin drei der vier abstrakten Sicherheitsziele - nämlich Verbindlichkeit, Integrität und Vertraulichkeit - mit Hilfe asymmetrischer Schlüsselverfahren verwirklichen, was diese Technologie zur Grundlage der in der Entstehung begriffenen technischen Infrastruktur der digitalisierten Informationsgesellschaft macht.

Sowohl vertraulichkeitsschützende Anwendungen als auch Anwendungen der digitalen Signatur, die den Austausch manipulationsgeschützter rechtsverbindlicher Willenserklärungen in offenen Netzwerken ermöglichen, setzen aber voraus, daß sichere Schlüssel verwendet werden. Daß dies bis heute keine Selbstverständlichkeit darstellt, ist auf gravierende Interessenkonflikte zwischen Vertraulichkeitsschutz und den Zielen der inneren und äußeren Sicherheit zurückzuführen. Insbesondere die US-amerikanische National Security Agency (NSA) wird immer wieder mit Versuchen in Verbindung gebracht, den Einsatz starker Schlüsselverfahren zum Schutz von Privatsphäre und Wirtschaftsgeheimnissen zu verhindern oder zu unterlaufen, um die Abhörmöglichkeiten staatlicher Sicherheitsbehören unter den veränderten technischen Vorzeichen des elektronischen Zeitalters so weit wie möglich aufrechtzuerhalten.

Wo es um die digitale Verschlüsselung geht, haben leistungsfähige Produkte, die auf einem frei zugänglichen Quellcode basieren, gegenüber proprietären Erzeugnissen wie denen des Marktführers Microsoft einen entscheidenden Vorteil: Weil ihre Eigenschaften und Funktionen allgemein nachvollziehbar sind, lassen sie sich nicht nur problemlos zertifizieren, sondern bieten zudem gute Voraussetzungen dafür, von der IT-Anwenderschaft angenommen zu werden.

Anregungen, Kommentare, Kontakte: PD Dr. Olaf Winkel, Institut für Politikwissenschaft der Universität Münster, Scharnhorststraße 100, 48151 Münster, Tel.: 0251-83-29409, Fax: 0251-83-24372, E-Mail: Olaf.Winkel@t-online.de

(Aus: www.sicherheit-im-internet.de) ◆

## IT-Sicherheit: Sichere Kommunikation mit zertifizierten elektronischen Signaturen

Der Austausch von Nachrichten und Dokumenten über die Grenzen des lokalen Netzes hinaus nimmt auch in der öffentlichen Verwaltung zu. Damit wird die Notwendigkeit für eine sichere Identifizierung des Absenders der Nachricht größer, da die Selbstverständlichkeit der Richtigkeit der Absenderinformation in Weitverkehrsnetzen oder im Internet nicht mehr gilt.

Um eine glaubhafte und gesicherte Absenderinformation zur Nachricht ➔

← zu haben, gibt es die Möglichkeit der elektronischen (oder digitalen) Signatur, die durch Beglaubigung von einer vertrauenswürdigen Instanz zuverlässig wird. In dieser Arbeit wurde nun untersucht, wie die DZ-SH eine Infrastruktur einrichten kann, die einen vertrauenswürdigen Einsatz von digitalen Signaturen im Bereich der öffentlichen Verwaltung Schleswig-Holsteins möglich macht.

In Deutschland wurde 1997 mit dem Signaturgesetz und der Signaturverordnung ein Rahmen geschaffen, der die Beschaffenheit von digitalen Signaturen und vor allem Anforderungen an die vertrauenswürdigen Instanzen, die TrustCenter, regelt. Es handelt sich dabei jedoch um Kann-Vorschriften, die zumindest innerhalb geschlossener Benutzergruppen nicht beachtet werden müssen. Die Gültigkeit der digitalen Signatur in Rechtsgeschäften und Verwaltungsakten ist mit dem Gesetz überhaupt nicht berührt: für die Rechtsgültigkeit muß erst eine Vielzahl von Gesetzen angepaßt werden.

Nach Abwägung der aktuellen Situation wurde der Schluß gezogen, daß ein Beginn der TrustCenter-Tätigkeit ohne Ausrichtung an das Signaturgesetz erfolgen kann, da

- das Signaturgesetz keine zwingende Vorschrift ist;
- die öffentliche Verwaltung in Schleswig-Holstein als geschlossene Benutzergruppe angesehen werden kann;
- eine Durchsetzung der Vorschriften in der jetzigen Form auf EU-Ebene nicht absehbar ist (Widerstand anderer Mitgliedsländer);
- international sich wahrscheinlich andere Normen durchsetzen werden als die im Signaturgesetz zugrunde gelegten.

Als zu nutzendes Produkt wurde PGP ausgewählt, da

- es mit der in Schleswig-Holstein vorherrschenden Systemumgebung kompatibel ist;
- keine hohen Kosten verursacht;
- einfach zu bedienen ist;
- der Keyserver im Quellcode vorliegt und an die Anforderungen anpaßbar ist.

Auf der Basis dieser Entscheidungen wurde ein Betriebskonzept für ein TrustCenter in der DZ-SH entwickelt, das beinhaltet, daß

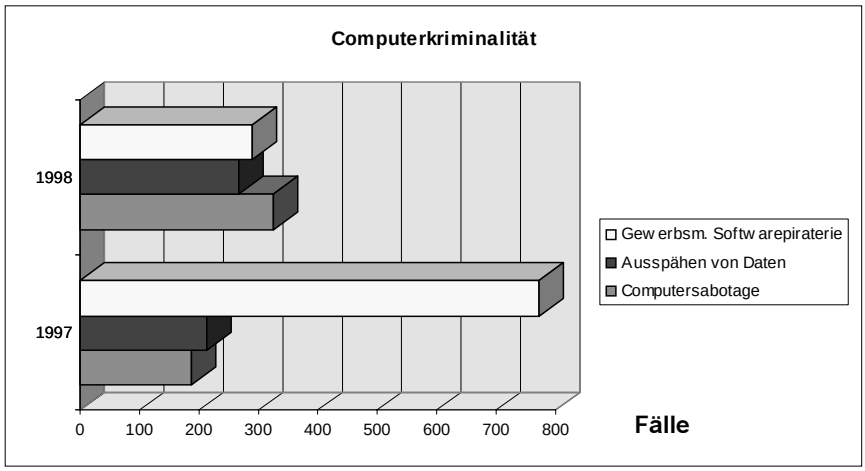
- die Unterbringung der sicherheitskritischen Systemumgebung im geschützten Rechenzentrumsbereich ausreichend sicher ist;
- die Bedienung durch besonders ausgewählte DZ-SH-Mitarbeiter bzw. Mitarbeiterinnen zuverlässig erfolgt;
- die Schlüsselübergabe und Identifizierung der Nutzer und Nutzerinnen durch die jeweilige Personalstelle erfolgt.

Der Ablauf der Generierung eines Signaturschlüssels und dessen Einsatz soll dann wie folgt aussehen:

- ein Antrag auf Schlüsselerzeugung wird an die DZ-SH gestellt;
- ein Schlüsselpaar (privater Schlüssel/öffentlicher Schlüssel) wird auf dem Generierungsrechner in der DZ-SH erzeugt;
- das Schlüsselpaar wird über die Personalstelle an den Nutzer / die Nutzerin ausgehändigt und auf dem Arbeitsplatzrechner implementiert;
- der Schlüssel wird von der DZ-SH mit dem Signaturschlüssel des TrustCenters beglaubigt;
- der private Schlüssel in der DZ-SH wird gelöscht, der öffentliche Schlüssel auf dem Auskunftsserver für Abfragen zugänglich gemacht;
- der Nutzer bzw. die Nutzerin ist nun in der Lage, mit diesem Schlüssel Nachrichten und Dokumente unter Nachprüfbarkeit seiner bzw. ihrer Identität zu signieren und ggf. zu verschlüsseln.

Ein Betrieb des TrustCenters erfolgt schon in 1999, für den sich weitere Interessierte bei der DZ-SH melden können. Der Verzeichnisdienst für die öffentlichen Schlüssel arbeitet bereits und kann unter der Internet-Adresse http://www.landsh.de/pgp/ abgerufen werden.

(Nachdruck aus: Homepage landsh.de/dzsh/aktuell/Grundlagen1998 Copyright © 1999 Datenzentrale Schleswig-Holstein webmaster@landsh.de) ◆




***Quelle: BKA zitiert nach CZ vom 1.7.99***

### *Sicherheit von TK-Anlagen*

# Der Feind im Telefon

Moderne Telekommunikationsanlagen können unbemerkt mit wenig Aufwand mißbraucht werden. Abhören, Abzapfen von Daten, Gebührenbetrug und Manipulationen an den Geräten können dabei riesige Schäden anrichten.

Die Telekommunikationssicherheit wird oft sehr stiefmütterlich behandelt, und Sicherheitskonzepte für diesen Bereich gibt es kaum. Das Risikopotential im Bereich Telekommunikation auf der einen und fehlende oder nicht ausreichende Sicherheitsmaßnahmen auf der anderen Seite kennzeichnen die Situation in der Praxis. Wie konnte es dazu kommen?

Erstens hat die digitale die analoge Technik abgelöst. ISDN-Telekommunikationsanlagen sind komplexe Rechnersysteme, die auf der Software-Ebene bei Programmen und auch Datenbanken manipuliert werden können und deren Leistungsmerkmale durch Mißbrauch bedroht sind.

Der zweite Umstand ist das Zusammenwachsen der rechnergestützten Informationsverarbeitung und der Telekommunikation in den zurückliegenden Jahren. Ein Paradebeispiel ist das Electronic Banking. Telekommunikation und EDV sind derartig aneinander gekoppelt, dass bei Nichtverfügbarkeit des einen Teils die Funktionsfähigkeit des anderen nichts nützt.

Der dritte Grund liegt häufig in unterschiedlichen Zuständigkeiten in den Betrieben. Sie sind für den Bereich Informationsverarbeitung im engeren Sinne, d. h. für Rechnersysteme und -netze sowie für die Telekommunikation, oft nicht zusammengefaßt. So kommt es, daß auf der einen Seite die Abschottung des unternehmensinternen Netzes gegen Angreifer von außen zum Beispiel durch Firewall-Systeme als unverzichtbar und selbstverständlich angesehen wird, bei der Telekommunikation hingegen an Schutzvorkehrungen praktisch nichts vorhanden ist.

Die Gefahren durch mißbräuchliche Nutzung der Fernwartungsmöglichkeit und prinzipiell auch durch Mißbrauch über den D-Kanal bei ISDN sollten keineswegs unterschätzt werden.

Zunächst müssen Manipulations- und Mißbrauchsmöglichkeiten identifiziert und ihr Ausmaß untersucht werden. Anschließend ist bei angemessenem Aufwand die Größe der Sicherheitslücken durch ein Sicherheitskonzept bis auf ein bewußt zu tragendes und transparent gemachtes Restrisiko zu reduzieren. Die Höhe des in Kauf genommenen Restrisikos ist in nicht zu langen zeitlichen Abständen immer wieder neu zu überdenken.

## *Mißbrauch / Manipulation von ISDN-Leistungsmerkmalen*

Moderne ISDN-TK-Anlagen verfügen häufig über so viele Leistungsmerkmale, daß Mitarbeiter nur einen Teil davon nutzen. Um einen Mißbrauch durch die nicht benötigten Leistungsmerkmale auszuschließen, sollten Techniker diese deaktivieren und, falls die technischen Voraussetzungen dafür gegeben sind, sogar ausbauen. Bei TK-Anlagen handelt es sich oft um Serienprodukte für das In- und Ausland. Für den Export, weil vom Kunden im Ausland ausdrücklich gefordert, können aber Leistungsmerkmale wie das „Abhören“ oder eine „Zeugenschaltung“ wichtig sein, die in Deutschland in der Regel nicht erwünscht oder sogar verboten sind.

Hersteller der TK-Anlage sollten beantworten können, ob sich die im Inland vertriebenen Geräte von denen, die ins Ausland exportiert werden, unterscheiden. Ebenso sollten sie wissen, ob unerwünschte Leistungsmerkmale nur deaktiviert und vielleicht nur in der deutschen Dokumentation nicht beschrieben sind.

## *Gebührenbetrug*

Kann das Leistungsmerkmal „Rufumleitung“ remote umprogrammiert werden, liegen die Mißbrauchsmöglichkeiten in Form von Gebührenbetrug auf der Hand. Virtuelle private Netzwerke (VPN) sind ein zweiter Problemkreis. Bieten TK-Anlagen in der Regel die Möglichkeit, spezielle Zugriffsziffern oder virtuelle Adressen für Anrufer aus dem öffentlichen Fernsprechnetz, d. h. von außen, zu sperren, wird dies in der Praxis aber dann nicht realisierbar sein, wenn auch Außendienstmitarbeiter das Corporate Network nutzen sollen.

Eine weitere Möglichkeit zum Mißbrauch ist dadurch gegeben, Berechtigungen derart einzurichten, daß hereinkommende Amtsleitungen abgehende Amtsleitungen belegen können. Dies bedeutet, ein externer Anrufer wird automatisch mit dem Carrier verbunden. Der Anrufer von außen trägt nur die Kosten für die Verbindung bis zur TK-Anlage. Alle anderen Gebühren laufen zu Lasten des betroffenen Unternehmens. Indizien für einen Gebührenbetrug sind ein starker Anstieg der Telefonrechnung durch Ferngespräche, insbesondere ins Ausland, extrem lange Gespräche oder das Auftauchen ungewöhnlicher und auch kostenpflichtiger Rufnummern.

## *Abhören von Räumen*

Die Leistungsmerkmale „Direktes Ansprechen“ in Kombination mit der Option „Frei sprechen“ ermöglichen die Realisierung einer Wechselsprechanlage und können zum Abhören von Räumen mißbraucht werden - eine entsprechende Ausrüstung der Endgeräte vorausgesetzt.

Üblicherweise wird vom Telefonapparat bei Aktivierung des Mikrofons ein kurzer Warnton ausgegeben, die Dauer beträgt ca. 1 Sekunde. Dieser läßt sich aber manipulativ so verkürzen, daß er kaum noch bzw. nicht mehr ➔

← wahrnehmbar ist. Die entsprechende optische Anzeige im Display des Telefonapparates kann teilweise auch von außen unterdrückt werden.

Insbesondere bei Konferenzräumen oder Besprechungszimmern besteht somit Gefahr. Meist kann sich ein potentieller Täter auch noch bequem darüber informieren, wann für ihn ein Lauschangriff Erfolg verspricht: Die Reservierung der Räume wird frühzeitig bekanntgegeben oder läßt sich über das LAN von jedem Interessierten komfortabel abrufen.

### Abhören von Telefongesprächen

„Dreierkonferenz" ist ein weiteres Leistungsmerkmal zum Mißbrauch. Anstatt einen Anruf zu übergeben, kann ein Anwender verdeckt eine virtuelle Konferenzschaltung vornehmen. Meist wird dies jedoch auf dem Display der Telefonapparate angezeigt. Lassen sich in Deutschland unzulässige Leistungsmerkmale, beispielsweise die Zeugenschaltung entsperren, bestehen weitere Abhörmöglichkeiten. Durch die Manipulation von Rufumleitungen können Faxe abgefangen und anschließend mit kaum merklicher zeitlicher Verzögerung an den berechtigten Empfänger weitergeleitet werden. Mit ISDN-Testgeräten lassen sich unmittelbar nach dem Netzabschluss am So-Bus (NTBA) die übertragenen Daten abhören.

Auch für Primär-Multiplex-Anschlüsse S2M gibt es derartige Geräte. Das Anzapfen der Kabel von Endgeräten ist wegen der herstellerspezifischen Schnittstellenprotokolle dagegen beträchtlich aufwendiger. Die frühere Hauptgefahr des Abhörens durch paralleles Aufklemmen ist nur bei analogen Leitungen möglich.

### Ausforschung von Kommunikationsprofilen

TK-Anlagen speichern Kenndaten für die abgewickelte Kommunikation: wer mit wem wie lange verbunden war und welche Gebühren dadurch aufgelaufen sind. Die Diensterkennung gibt Auskunft darüber, ob es sich um Sprach- oder Datenkommunikation oder Faxverkehr gehandelt hat.

Diese Kommunikationsprofile ermöglichen einen Angreifer, gemäß seiner Interessenlage Rückschlüsse zu ziehen. Beispielsweise über Konkurrenzangebote, Projektfortschritte, Kundenvertriebswege usw. Ohne explizite Schutzvorkehrungen liegen die Kommunikationsprofile für den Administrator einer TK-Anlage offen.

Aus den aufgezeigten Mißbrauchs- und Manipulationsmöglichkeiten von ISDN-Leistungsmerkmalen läßt sich ableiten, daß die Administration einer TK-Anlage, die Vergabe, Handhabung und Kontrolle der Administrator-Rechte und in diesem Zusammenhang auch die physische Zutrittsmöglichkeit zu den Räumen sensibel zu handhaben sind.

### Mißbrauch von außen

Fernwartungszugänge von TK-Anlagen ermöglichen prinzipiell nicht nur alle Wartungs- und Administrator-Arbeiten, sondern auch die Abwicklung von sonstigen Management-Funktionen, beispielsweise Alarmsignalisierung und -bearbeitung. Entsprechend bietet ein erfolgreicher Angriff auf den Fernwartungszugang, zum Beispiel durch die direkte Einwahl über DISA (Direct Inward System Access), ausgedehnte Möglichkeiten zu Manipulation und Mißbrauch.

Es ist zwischen externer und interner Fernwartung zu unterscheiden. Erstere wird von außen durch Anwahl über das öffentliche Netz von Dritten ausgeführt, beispielsweise handelt es sich dabei um den Hersteller der TK-Anlage. Der Hintergrund für externe Fernwartung liegt meist darin, daß man aus Kostengründen kein eigenes Wartungspersonal unterhalten kann oder will.
Das Call-back-Verfahren, Servicetools mit Sicherheitsfunktion wie Dongles oder die Abwicklung eines DISA-Zugangs über eine eigene SO-Schnittstelle kommen als Schutzmaßnahmen vor Angriffen in Betracht. Bei externer Fernwartung sind die von außen in der TK-Anlage vorgenommenen Eingriffe für das betroffene Unternehmen letztendlich nicht nachvollziehbar. In der Praxis ist vielfach die aktuelle Anlagenkonfiguration intern nicht bekannt. Häufig wird die Fernwartung ohne Kenntnis des Kunden durchgeführt, und Protokollfunktionen werden entweder nicht genutzt oder die Protokolle nicht ausgewertet. Der externe Zugriff über den Fernwartungszugang erfolgt vollständig unkontrolliert. Der Dienstleister kann selbst Opfer eines professionellen Angreifers werden. Ist dieser erfolgreich, sind ihm die Kundenanlagen schutzlos ausgeliefert.

Bei der internen Fernwartung werden TK-Anlagen, die auf mindestens zwei voneinander entfernte Standorte verteilt sind, im Verbund betrieben. Unter Kosten- und Zeitaspekten ist die Fernwartung/-administration dann meist unverzichtbar: Das interne Service- und Wartungspersonal soll nicht jedes Mal die betroffene TK-Anlage physisch aufsuchen müssen, um entsprechende Arbeiten ausführen zu können. Dabei ist zu bedenken, daß solche Eingriffe allein durch den Umzug eines Teilnehmers erforderlich werden können.

Das Standardszenario ist also, daß der Techniker von seinem Bedienplatz an seinem Standort den Wartungsapparat anwählt, der an den Administrationseingang der remote zu wartenden TK-Anlage angeschlossen ist. Ist diese lediglich über ein einfach zu überwindendes Standardpasswort abgesichert, besteht eine entsprechend hohe Gefahr des Mißbrauchs. Dies gilt gerade dann, wenn es sich bei diesem Standardpasswort zu allem Übel auch noch um die herstellerseitige Grundeinstellung handelt. Für diesen Fall benötigt der Angreifer praktisch nur noch die Rufnummer des Wartungsapparates, eine in der Regel einfach zu erhaltende interne Information. →

### ← Manipulation über D-Kanal

Bei ISDN gibt es die Nutzkanäle B1 und B2 und zusätzlich mit niedrigerer Übertragungsrate einen Kanal zur Steuerung (Signalisierung), den D-Kanal. Mit Ausnahme von DATEX P ist der D-Kanal für die Teilnehmer nicht nutzbar. Zur Steuerung der TK-Anlage und somit der Übertragung werden über den D-Kanal Daten mit der Vermittlungsstelle des Carriers ausgetauscht. Beispielsweise handelt es sich um die Teilnehmer- und Diensterkennungen, Befehle zum Verbindungsauf- und -abbau und die Systemzeit. Der Prozess der Datenübertragung wird also gesteuert, und die digitale TK-Anlage verhält sich dabei gegenüber den über den D-Kanal signalisierten, entstehenden Zustandsveränderungen wie ein Prozessrechner.

Diese Reaktionen erfolgen softwaregesteuert. Professionellen Angreifern wie Nachrichtendiensten oder der organisierten Kriminalität ist es mit großem Aufwand prinzipiell möglich, über den D-Kanal einen schadenstiftenden Programmcode einzuschleusen und den vorhandenen so zu manipulieren. Es können aber auch Befehle übermittelt werden, die der Prozessor der TK-Anlage ausführt, so daß eine mißbräuchliche Nutzung von Leistungsmerkmalen erzwungen wird.

Deshalb sollte also an den Hersteller einer TK-Anlage die Anfrage gerichtet werden, ob eine Manipulation über den D-Kanal sicher, und das heißt hier zu 100 Prozent, ausgeschlossen werden kann. Teilweise wird dies dadurch erreicht, daß ein eigener interner Code benutzt wird und nur ausgesuchte Befehle vom externen in den internen Code übersetzt werden.

Noch relativ neu auf dem Markt ist eine sog. ISDN-Firewall. Es handelt sich dabei um einen Filterrechner, der die Pakete im D-Kanal mit vorgegebenen Einstellungen, den Filterregeln, abgleicht, Abweichungen ermittelt und dann in vorgegebener Art und Weise reagiert. Diese Reaktionen können von der Protokollierung bis zum Abbruch der Verbindung reichen.

Die Filterregeln können sowohl protokoll- als auch teilnehmerbezogen sein. Im ersten Fall prüfen sie auf die Übereinstimmung mit dem benutzten ISDN-Protokoll, im zweiten wird die Nutzung von bestimmten Diensten und Leistungsmerkmalen an Rufnummern gebunden.

*HARALD SEIFFERT*

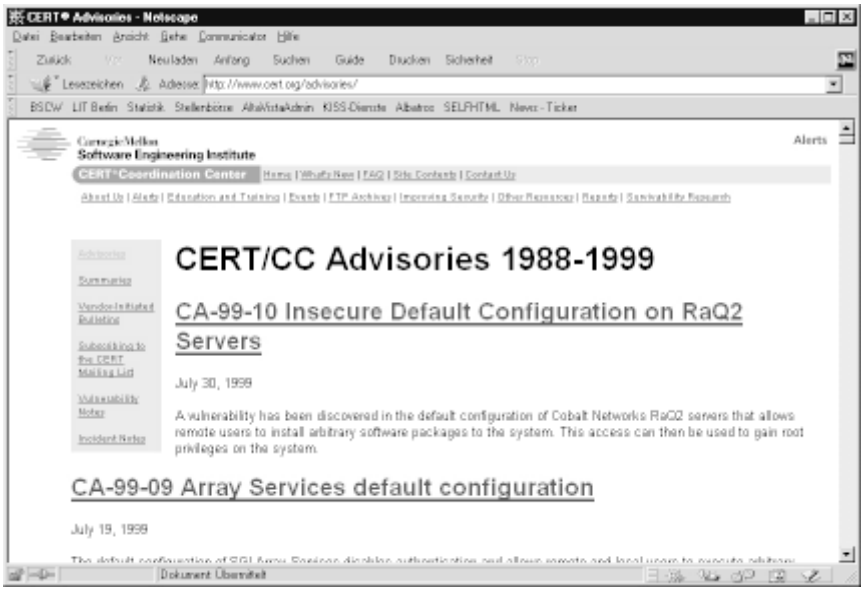
Zum Autor: Dipl.-Kfm. Harald Seiffert ist Prokurist und Gesellschafter der Von zur Mühlen'sche Unternehmensberatungs GmbH (VZM), Sicherheitsberatung, BdSI, 53121 Bonn, Alte Heerstr. 1, Telefon: 0228 - 962 93-0
(Nachdruck mit freundlicher Genehmigung der OFFICE MANAGEMENT Redaktion und dem Autor, Heft 4/99) ◆

## Computer Emergency Response Team

Eine der ersten Anlaufstellen im Internet zum Thema Sicherheit ist das CERT Coordination Center (CERT = Computer Emergency Response Team), ein Teil der Survivable Systems Initiative am Software Engineering Institut, einem Forschnungs- und Entwicklungszentrum der Carnegie Mellon University in den USA. In den sogenannten CERT advisories werden bekannt gewordene Sicherheitslücken und Fehler dokumentiert und Vorschläge zur Nachbesserung gemacht. Wer sich ständig auf dem aktuellen Stand in diesen Sicherheitsfragen halten will, kann sich beim CERT in eine entsprechende Mailingliste eintragen.




Auch in der entsprechenden Newsgroup im Intranet finden sich diese Alarme und Hinweise. Die Name der Newsgroup lautet verw-bln.lit.security.cert ◆



# Der Internet-Zugang birgt immer Gefahren

Seit der Umwandlung vom Landesamt zum Landesbetrieb (1. Januar 1998) wurden die Fachaufgaben der Gruppe KISS (Kommunikations-, Informations- und Sicherheits-Service im Netz) dem Geschäftsbereich I (Projektierung und Beratung) zugeordnet. Durch die Gründung des „Landesbetriebes für Informationstechnik" entstanden neue Ziele und Aufgabenstellungen.

In der Arbeitsgruppe Dienste/ Netzsicherheit sind folgende Aufgaben wahrzunehmen:

- Sicherheit in Netzen (Firewall-Thema: Konzeption, Administration und Konfiguration) - Datenverschlüsselung und Authentifizierung
- Schutz vor Computerviren
- Aufklärung von Sicherheitsverlusten
- Weiterentwicklung in Richtung Trust Center
- Beteiligung bei der Erstellung von Sicherheitskonzepten

**Sicherheitsanforderungen**

Dieser Beitrag behandelt den Einsatz von Anti-Viren-Software. Entsprechend der Erfüllung von Sicherheitsanforderungen als erweiterte Schutzmaßnahme für das Berliner Landesnetz bzw. den LAN's bei Haupt- und Bezirksverwaltungen wurde der Einsatz von Anti-Viren-Software zum Schutz des Internetzuganges ausgeschrieben.

**Bedrohung: E-Mail, HTTP, FTP**

Das auszuwählende Produkt mußte in der Lage sein die Protokolle SMTP, HTTP und FTP auf Viren zu untersuchen. Laut Auswahlverfahren wurde das Produkt „InterScan VirusWall" der Firma Trend Micro Deutschland GmbH beschafft. Das Produkt läuft auf einem NT-Server unter Windows NT 4.0.

Der Virenscanner ist Bestandteil vom ComNet innerhalb des Grenznetzes. Das Berliner Landesnetz ist über ein Firewall-System mit dem Internet verbunden. Zwischen dem Berliner Landesnetz und dem Internet befindet sich das Grenznetz. Im Grenznetz befinden sich WWW-Server, die Informationen der Berliner Verwaltung im Internet bereitstellen.

Weiterhin befindet sich der zentrale Mail-Server der Berliner Verwaltung, der den Posteingang auf die einzelnen Mail-Server im Berliner Verwaltungsnetz verteilt und den Postausgang zu den entsprechenden Servern im Internet leitet. Auf dem zentralen MailServer befinden sich auch Nutzerpostfächer. Der gesamte Datenverkehr wird sowohl ein als auch ausgehend auf Viren überprüft.

Der Zugriff über die Protokolle HTTP und FTP aus dem Verwaltungsnetz in das Internet erfolgt über einen Proxy-Server, der nur berechtigte Kommunikationspartner akzeptiert. Der gesamte Datenverkehr der über diese Protokolle abgewikkelt wird , ist auf Viren zu überprüfen. Destruktive und Java-Applets sind heute schon keine Seltenheit mehr. Dank ActiveX wird sich diese Situation in Zukunft noch verstärken. Moderne Firewalls oder Antivirensysteme müssen deshalb auch eine Option zum Blockieren von Java oder ActiveX beinhalten (verfügbar unter VirusWall).

In der Anfangsphase wurde der gesamte Mail-Verkehr als auch Web-Verkehr über den Virenscanner (NT-Server) geleitet. Hierbei wurden die Sicherheitsfunktionen und der Zugriff auf Konfigurations-Seiten per Web-Browser oder via GUI auf den NT-Server überprüft.

**Umfassende zentrale Verwaltung**

Das Produkt gliedert sich wie folgt:

- SMTP Configuration
- FTP Configuration
- HTTP Configuration - Log Files
- Pattern Update
- Virus Encyclopedia - Technical Support - About
- Performance-Monitor

InterScan VirusWall erkennt, stoppt und meldet Viren in E-Mail, FTP und HTTP bereits am Internet-Gateway, bevor die Viren in das Netzwerk eindringen. Der Datentransfer durch den Gateway zwischen internes Netzwerk und dem Internet wird überprüft, auch komprimierte und kodierte Internet-Dateiformate wie ZIP, UUENCODE und MIME. Häufige Aktualisierung von Virenpattern ist für die Aufrechterhaltung einer sicheren Datenverarbeitung unerläßlich. InterScan VirusWall ermöglicht das automatische Herunterladen der neuesten Virenpattern.

Zwecks möglicher Performance-Einbußen wurde der Datendurchsatz zwischen Virenscanner und Proxy-Server analysiert. Hierbei stellte sich heraus, dass der bisherige Proxy-Server laut Hardware-Ausstattung den Leistungsanforderungen nicht mehr gerecht wird und der NT-Server (Virenscanner) in den letzten drei Monaten bei Mail-Verkehr in Spitzenzeiten (ca. 10:30-11:30 Uhr und 15:00-16:00 Uhr) auf über 90 Prozent Prozessorleistung kam. Hinsichtlich unterbrechungsfreiem Mail-/ Web-Verkehr hat der LIT eine Ersatzbeschaffungsmaßnahme vorgenommen und den alten Proxy-Server durch einen neuen ersetzt.

Zwischenzeitlich wurde das Anti-Viren-Produkt weiterentwickelt und in der Version 3.1 für NT freigegeben. Bedingt durch die hohe Durchsatzraten im Web-Verkehr versucht der LIT die Software „InterScan VirusWall" für Sun Solaris Version 3.0 zu testen.

**Ausblick**

Gerade im Hinblick auf das Angebot von Sicherheitsdiensten sollte ein möglichst reibungsloser Netzbetrieb gewährleistet werden. Wegen besagter Performance-Engpässe in der Vergangenheit sind Tests mit anderen Hardware-Plattformen zwingend notwendig. Desweiteren wurde die Firma Trend Micro gebeten hinsichtlich der Mehrprozessorfähigkeit bei Einsatz von Unix-Maschinen aussagen zu machen. Sobald gezielte Ergebnisse vorliegen wird geprüft, ob der NT-Server durch einen Sun-Server ersetzt wird. Weitere Informationen zum Thema InterScan VirusWall wird die Ausgabe 1/2000 des SPLITTER bringen.

*WILLI HARTMANN* ◆

# (IT)-Ausstattung und IT-Planung in der Senatsverwaltung für Stadtentwicklung, Umweltschutz und Technologie



In der Kleinen Anfrage Nr. 13/4809 wolllte der Abgeordnete Ulrich Manske (CDU) über den „Entwicklungsstand der Informationstechnik (IT)-Ausstattung und IT-Planung in der Senatsverwaltung für Stadtentwicklung, Umweltschutz und Technologie“ vom Senat informiert werden. Er fragte den Senat::

**1.** Welche Investitionen wurden im Rahmen des Fachübergreifenden Informationssystems (FIS) getätigt für

a) Hardware,
b) Software-Produkte,
c) Entwicklung von Fachanwendungen,
d) Schulung,
e) Betreuung der Anwender

für den Zeitraum 1996 bis 1999 aufgeschlüsselt jeweils für die Fachbereiche der Senatsverwaltung und der beteiligten Verwaltungen?

**2.** Wie ist die technische Betreuung der FIS-Infrastruktur zwischen den beteiligten Verwaltungen: der Senatsverwaltung für Stadtentwicklung, Umweltschutz und Technologie, den Bezirken (IT-Stellen, Geschäftsstellen) und dem Landesbetrieb für Informationstechnik (LIT) für den laufenden Betrieb organisiert, und stehen hierfür im Haushalt 1999 die erforderlichen Mittel für Geographische Informationssysteme (GIS) (Bezirkshaushalt, LIT-Haushalt) zur Verfügung?

**3.** Wie ist der Stand des fach- und ämterübergreifenden Datenaustausches für

a) die Bereitstellung von Daten des Automatischen Liegenschaftsbuches (ALB/ALK) und der Amtlichen Topographisch-Kartographischen Informationssysteme (ATKIS) für Fachanwendungen,

b) die Bereitstellung von Daten anderer Fachverfahren für die FIS-Verfahren (Raumordnung, Bauwesen, Städtebau [RBSÜ), Einwohnerdaten, ...),

c) den Austausch von Daten innerhalb des FIS-Verfahrens zwischen den Bezirksämtern und der Senatsverwaltung für Stadtentwicklung, Umweltschutz und Technologie und

d) die Bereitstellung von Daten der FIS-Verfahren an andere Anwendungen in der Berliner Verwaltung?

**4.** Ist für den Zeitraum 2000 bis 2004 eine Fortschreibung der Planung für

a) die Sicherung des laufenden Betriebes der FIS-Verfahren,
b) die Anpassung und Weiterentwicklung der vorhandenen Verfahren,
c) die Pflege der Verfahren (Updates, Upgrades),
d) die Ersatzbeschaffungen (Hard- und Software),
e) die Schulungen
erfolgt?

**5.** Sind Neuentwicklungen (z. B. Landschaftsplanung, Bereitstellung von FIS-Daten der Senatsverwaltung für Stadtentwicklung, Umweltschutz und Technologie und der Bezirke im Intranet der Berliner Verwaltung) zur Unterstützung der fachlichen Aufgaben erforderlich, und wenn ja, wurden diese in der Planung berücksichtigt? (21. April 1999)

Die Antwort des Senats von Berlin (Schlussbericht) auf die KIeine Anfrage Nr. 4809 lautet wie folgt:

**Zu 1. a:** Für die Nutzung durch alle Abteilungen der Senatsverwaltung für Stadtentwicklung, Umweltschutz und Technologie (SenStadtUmTech) wurde im Jahr 1996 ein Datenbankserver für die Automatisierte Liegenschaftskarte (ALK) beschafft, der 1997 und 1999 um Festplattenspeicher erweitert wurde. Im Jahr 1997 wurden für die Bereiche Stadtentwicklungsplanung, Gewässerverzeichnis, Geologie und Grundwasser sowie ökologische Planungsgrundlagen/Umweltatlas grafische Arbeitsplätze ersatzbeschafft und bei den vorhandenen grafischen Arbeitsplätzen eine Festplattenerweiterung vorgenommen. Im Jahr 1998 wurde über den Landesbetrieb für Informationstechnik (LIT) ein Netzzugangsrechner (Firewall) für die Standorte Am Köllnischen Park und Salvador-Allende-Str. beschafft. Für Abteilung I wurde 1999 für die Bearbeitung des Flächennutzungsplans (FNP) ein grafischer Arbeitsplatz ersatzbeschafft und für Aufgaben der Grün- und Freiraumplanung wurden 1996 sieben PC-basierte grafische Arbeitsplätze beschafft. 1996 wurde ein alle Fachbereiche der SenStadtUmTech und für die Bezirke zugänglicher DIN-AO Farbtintenstrahlplotter beschafft, im Jahr 1998 ein entsprechendes Gerät für Abteilung IV.

Im Jahr 1996 wurden die noch ausstehenden neun bezirklichen Umweltämter mit Datenbankservern und 1996 und 1997 die noch ausstehenden sechs Stadtplanungsämter mit grafischen Workstations ausgestattet. In 18 Stadtplanungsämtern und in einem Umweltamt wurden 1997 Festplattenerweiterungen vorgenommen. 1998 wurden ein ORACLE-Datenbankserver für das Bezirksamt Schöneberg, der als Infrastrukturserver neben den ORACLE-Datenbanken des FIS auch andere bezirkliche ORACLE-Anwendungen bedient, 19 Printserver für den Netzanschluß von Grafikdrucken der Bezirke und zwölf Geodatenserver für die Nutzung als gemeinsamer Datenbankserver der Stadtplanungs- und Vermessungsämter (Bezirksinformationssystem) beschafft.

**Zu 1. b:** Die Betriebssystemsoftware, das Datenbanksystem ORACLE sowie SICAD/open und SICAD-BBP wurde mit den Datenbankservern und den grafischen Arbeitsplätzen für die SenStadtUmTech und die Bezirke beschafft. ➔

← Außerdem wurden die Pflege- und Wartungsgebühren für die grafischen Arbeitsplätze, für ORACLE und die YADE-Lizenzen finanziert.

Für die Bearbeitung von ATKIS in der SenStadtUmTech wurde 1997 SICAD/GLOBE beschafft, im Jahr 1998 wurde eine Landeslizenz für die Nutzung des Grünflächeninformationssystems GAIA in der SenStadtUmTech und allen bezirklichen Naturschutz- und Grünflächenämtern beschafft.

Um die Plotter im Netz der SenStadtUmTech gleichzeitig für die Ausgabe von Karten aus SICAD/BS2000, SICAD/open und YADE nutzen zu können, wurde auf einem SICAD-Server der SenStadtUmTech ein Plotmanagementsystem eingerichtet.

**Zu 1. c:** Im Rahmen des Projektes FIS wurden von 1996 bis 1999 folgende Fachanwendungen entwickelt bzw. durch Entwicklungs- oder Einführungsmaßnahmen unterstützt:

In den Jahren 1996 und 1997 wurde externe Managementunterstützung in Anspruch genommen für den Abschluß der Erstinstallation der grafischen Arbeitsplätze in den bezirklichen Stadtplanungsämtern, für die Installation und den Test von FMS (einem auf ORACLE basierenden Auskunftssystem des Automatisierten Liegenschaftsbuches (ALB) in Verbindung mit der grafischen Darstellung unter YADE) und für die Einführung des Lagerbehälterverfahren Pro-Umws.

In den Jahren 1998 und 1999 wurden folgende Projekte finanziert:

- Verfahrensentwicklung und -einführung der Digitalen Bereichsentwicklungsplanung (DiBEP),
- Installation von GAIA und die Entwicklung einer GIS-Komponente für GAIA (öffentliche Grünflächen und Spielplätze),
- Anpassung des B-Plan-Verfahrens an den neuen Objektschlüsselkatalog (OSKA) Bauleitplanung der SenBauWohnV,
- Erstellung einer B-Planübersicht der 1990 bis 1995 bearbeiteten Bebauungspläne einschl. der erforderlichen Erfassungs- und Übernahmeprozeduren,
- Erstellung einer Blockkarte aus ATKIS-Daten,
- Erstellung eines Feinkonzeptes und erste Realisierung eines VeZuDa-konformen universellen Auskunftssystems für die im Bereich Stadtplanung und Umweltschutz benötigten und erzeugten raumbezogenen Datenbestände (FIS-Broker).

**Zu 1. d:** In den Jahren 1996 und 1997 wurden die bezirklichen Anwender (je 2 Wochen) und Anwendungssystembetreuer (3 Wochen) in der Nutzung der eingesetzten Komponenten (IRIX, SICAD/open, BBP und ORACLE) geschult. Im Jahr 1996 fand eine Schulung für die Mitarbeiter der SenStadtUmTech in der Nutzung des Plotmanagementsystems statt.

Seit 1997 werden die Schulungen im Rahmen der FIS-Arbeitsgruppe koordiniert und von der Verfahrensbetreuung der SenStadtUmTech vorgenommen. Jährlich werden hierzu 4 bis 6 Wochen durchgeführt. 1998 fand zusätzlich ein Wiederholungs- und Aufbaukurs für die Anwendung von SICAD-BBP statt.

1999 wurden die Stadtplanungsämter im Umgang mit der Intranet-Technologie geschult.

**Zu 1. e:** Die Anwenderbetreuung der Fachverfahren erfolgt grundsätzlich durch die jeweils zuständigen Verfahrensverantwortlichen. Bei den grafischen Workstations ist die Trennung zwischen Systembetreuung und Anwendungsbetreuung naturgemäß nicht so trennscharf wie bei klassischen Großrechner- oder Client-Server-Verfahren.

Für die Anwenderbetreuung wurden im Projekt FIS im wesentlichen folgende Investitionen getätigt:

Im Jahr 1996 wurden eine Sollkonfiguration, eine Referenzinstallation und eine automatische Installationsprozedur für die grafischen Arbeitsplätze der Stadtplanungsämter erstellt. Diese Prozedur konnte mit geringfügigen Anpassungen für die Installation der Datenbankserver der Umweltämter einschließlich der Fachanwendung ProUmws genutzt werden.

Außerdem wurde in 1996 als Unterstützung bei der Verfahrenseinführung den Bezirken ein Kontingent an Systemunterstützung mit Hotline-Funktion zur Verfügung gestellt.

Im Jahr 1997 wurde in der SenStadtUmTech zum Verfahrenssupport ein Help-Desk eingerichtet, der sowohl Anwenderprobleme als auch technische Probleme entgegennimmt und löst bzw. einer Lösung zuführt. Dieser Verfahrenssupport unterstützt auch die Entwicklung spezieller Fachverfahren (z. B. DiBEP) und hat im Intranet ein umfangreiches Serviceangebot aufgebaut.

Dieser Help-Desk wird von Anwendern, Anwendungssystembetreuern und IT-Stellen in Anspruch genommen.

**Zu 2.:** Die technische Betreuung der FIS-Infrastruktur erfolgt grundsätzlich durch die in den jeweiligen Fachämtern bzw. Fachabteilungen angesiedelten und entsprechend geschulten Anwendungs- und Anwendungssystembetreuer, durch den jeweiligen Verfahrensverantwortlichen, durch die bezirklichen IT-Stellen, die Serviceeinheit IT der SenStadtUmTech (SE IT) sowie den LIT und die jeweiligen Lieferanten (Hardwarehersteller bzw. Verfahrensentwickler).

Im Problemfall ergibt sich dabei ein dreistufiges Verfahren, bei dem zunächst vor Ort eine Problemlösung (durch Anwendungsbetreuung oder IT-Stelle) angestrebt wird, in zweiter Stufe wird SenStadtUmTech eingeschaltet, die wiederum gegebenenfalls den LIT oder die Lieferanten beauftragt. →

# SKIN

## Das UPDATE für Ihre Karriere

Zertifizierung zum
Microsoft Certified System Engineer (MCSE) und zum
Microsoft Certified System Developer (MCSD)

- **SKIN** – Skill Improvement Network – qualifiziert Sie berufsbegleitend zum zertifizierten System-Professional
- Zeitrahmen: ca. 6 Monate
- Eingangstest (kostenlos) als Teilnahmevoraussetzung
- **Selbstlernen** mit Microsoft Trainingsunterlagen
- **Präsenztrainings** u.a. auch in Berlin
- **Online-Lernplattform** auf Global-Learning mit Chat, E-Mail, Newsgroups, virtuellen Lerngruppen und Foren
- **Online-Lernberater** als qualifizierter Ansprechpartner
- Tests zur Zertifizierung
- Kosten: 8.900 DM (inkl. Mehrwertsteuer)

**Anmeldung bei**

PROKODA AG
Elke Lichtenberg
Friedrichstraße 231 · 10969 Berlin
Tel. 030 – 25 39 19–28 · Fax –55
www.prokoda.de · info@prokoda.de

**SKIN** ist eine Initative der Unternehmen

Microsoft PROKODA DITEC Deutsche Telekom



Berlin

← Im Einzelnen ist die technische Betreuung wie folgt organisiert:

Die Bedienung der grafischen Arbeitsplätze erfolgt durch die Anwender bzw. Anwendersystembetreuer. Die Systembetreuung der grafischen Arbeitsplätze der SenStadtUmTech wird durch die SE IT vorgenommen. In den Bezirken erfolgt die laufende Systembetreuung durch die Fachämter oder durch die IT-Stellen. Schwierigere Systemarbeiten werden von der Systembetreuung der SenStadtUmTech über das Netz oder vor Ort erledigt. Betriebssysteminstallationen,Upgrades oder Nachrüstungen werden vom LIT im Auftrag der SenStadtUmTech erledigt, wofür eine Servicevereinbarung abgeschlossen wurde.

Die Datenbankserver werden überwiegend in den Rechenzentren der Bezirke betrieben, mithin erfolgt die technische Bedienung durch die örtliche IT-Stellen. Die Systembetreuung erfolgt wie bei den Grafischen Arbeitsplätzen durch die örtlichen IT-Stellen, die SE IT der SenStadtUmTech und den LIT.

Für die grafischen Arbeitsplätze und die Datenbankserver der Umweltämter (IRIX-Rechner) wurden Hardwarewartungsverträge abgeschlossen. Ferner bestehen Wartungsverträge für die Softwarewartung des Betriebssystems IRIX, von SICAD/open und SICAD-BBP (Bebauungsplanverfahren), des Datenbanksystems ORACLE und von YADE. Diese Verträge laufen in 1999 aus, eine Verlängerung wird zur Zeit mit den Bezirken und mit den Anbietern verhandelt.

Zur technischen Betreuung der Geodatenserver wurde für alle Geräte ein Wartungsvertrag (Hardware- und Softwarewartung) sowie ein Hotline-Servicevertrag abgeschlossen.

Die technische Betreuung der PC-Endgeräte (multifunktionale Endgeräte) erfolgt dezentral durch die jeweiligen Bezirke, gleiches gilt für die Betreuung des lokalen Netzes und der MAN-Zugänge.

Eine Besonderheit hinsichtlich der Verfahrensbetreuung stellt die Digitale Bereichsentwicklungsplanung DiBEP dar: Für diese bezirkliche Aufgabe haben die bezirklichen Stadtplanungsämter eine Arbeitsgruppe gebildet, die Entwicklung und Einsatz des Verfahrens betreut (eine Geschäftsstellungslösung wird angestrebt).

Die Fragen der technischen Betreuung und der Verfahrenskoordination werden in einer regelmäßig tagenden FIS-AG behandelt. Im Rahmen dieser organisatorischen Regelungen wurden die unter 1. aufgeführten Geräte in der SenStadtUmTech und in den Bezirken installiert und betreut. Dabei wurden in allen Bezirken technische Erweiterungen vorgenommen (Plattenerweiterungen, Speicherausbau), und es wurden mehrere Upgrades und Updates aller wesentlichen Systemkomponenten vorgenommen:

- IRIX von Version 5.0, über 5.1, 5.2 nach 5.3
- SICAD/open von 2.0 nach 5.0
- SICAD BBP von 2.0A05 über 2.0A06 nach 2.1A02
- ORACLE von 7.0 über 7.2 nach 7.33
- Digitale Bereichsentwicklungsplanung von 1 über 2.0 nach 2.1

**Zu 3. a:** Den Festlegungen der Vermessungsverwaltung entsprechend werden die Fachämter der Bezirke von ihren jeweiligen bezirklichen Vermessungsämtern mit der ALK beliefert, während die Hauptverwaltungen und bezirksübergreifende Datenlieferungen von der SenBauWohnV versorgt werden.

Für die Zwecke der Stadtplanung wurde im Rahmen des Projektes FIS auf den grafischen Arbeitsplätzen aller 23 bezirklicher Stadtplanungsämter unter SICAD/open eine ALK-Datenbank (GDB) eingerichtet, auf die die verschiedenen Anwendungen der Stadtplanungsämter (z. B. BBP, DiBEP usw.) zugreifen können. Entsprechend wurde in der SenStadtUmTech ein Gesamtbestand der ALK installiert. Die Einrichtung erfolgte in den Jahren 1997 und 1998 durch sukzessive Übernahme der nach Bezirken gegliederten SQD-Dateien (SICAD-Format). Die Objektstrukturen konnten dabei - soweit vorhanden - bereits für die Ausprägung der Daten berücksichtigt werden. Bereits installierte ältere Versionen der ALK wurden dabei ersetzt.

Auf dieser Basis konnte in 13 Bezirken ein geregelter Datenaustausch etabliert werden, indem (ca. im halbjährigen Rhythmus) das bezirkliche Vermessungsamt dem Stadtplanungsamt aktuelle SQD-Dateien über Datenträger oder über das Netz liefert, wofür spezielle Benutzerkennungen eingerichtet wurden. In zwei Bezirken erfolgt die Versorgung über die SenBauWohnV.

Für die SenStadtUmTech wird bei der SenBauWohnV ein Beziehersekundärnachweis (BZSN) eingerichtet und voraussichtlich im halbjährigen Turnus ein inkrementelles Update per EDBS vorgenommen. Die hierfür erforderliche Erstlieferung erfolgte im Mai 1999, die Installation bei SenStadtUmTech wird voraussichtlich im Juni 1999 abgeschlossen werden. Zukünftig soll in den Bezirken die ALK auf den Geodatenservern installiert werden, wobei die Vermessungsämter als Datenanbieter neben der besonders geschützten Produktions-ALK eine Auskunfts-ALK vorhalten, auf die die bezirklichen Fachämter direkt zugreifen können.

**Zu 3. b:** Ein Zugriff auf das von der SenBauWohnV als zentrales BS2000-Verfahren, geführte ALB ist zur Zeit nicht Gegenstand des FIS.

Im Jahre 1997 wurde im Rahmen des FIS gemeinsam mit der Vermessungsverwaltung, den bezirklichen Stadtplanungs- und Vermessungsämtern und den Fachbereichen der SenStadtUmTech die Eignung des aus der Pilotphase des FIS (NUCLEUS Stadtplanung) entwickelten FMS (ORACLE-basierte Auskunftsversion des ALB mit Schnittstelle zu YADE) anhand eines Anwendungstests geprüft. Dabei →

← konnte aber weder eine befriedigende und allgemein nutzbare Anwenderoberfläche noch ein praktikables und den gesetzlichen Anforderungen entsprechendes Zugriffskonzept auf die (personenbezogenen) Daten des ALB erarbeitet werden. Da seitens der Vermessungsverwaltung in Berlin und bundesweit ohnehin an Neuentwicklungen des ALB gearbeitet wird, wurde im Rahmen von FIS dieses Thema nicht weiter bearbeitet.

**Zu 3. c.:** ATKIS wurde für Berlin vom Landesvermessungsamt Brandenburg in Zusammenarbeit mit der SenBauWohnV und der SenStadtUmTech erarbeitet. Eine erste (noch nicht fertige) Version wurde 1998 im EDBS-Format geliefert und in der SenStadtUmTech unter SICAD/open und YADE installiert. Ähnlich der ALK handelt es sich bei ATKIS auch nicht um eine fertige Karte (i. S. einer ausgestalteten Grafik) sondern um ein abstraktes logisches und geometrisches Datenmodell, für dessen Betrachtung oder Verarbeitung beim Endbenutzer zur grafischen und logischen Interpretation spezielle Aufbereitungsprogramme bzw. -tabellen vorhanden sein müssen. Für YADE liegen in der SenStadtUmTech die entsprechenden Instrumente inzwischen vor, so dass die technischen Voraussetzungen für die Verteilung und Nutzung von ATKIS-Daten im FIS gegeben sind. Es ist vorgesehen, noch in 1999 ein geregeltes Verfahren zur Verteilung von ATKIS-Daten im FIS zu etablieren. Eine Fortschreibung über BZSN wie es für die ALK praktiziert wird ist auf Grund der nicht ausreichenden Schnittstellenfunktionen beim Ersteller (LVermB) z. Zt. noch nicht möglich.

**Zu 3. d:** Der Austausch weiterer Daten erfolgt im FIS über unterschiedliche Wege:

Daten mit Nutzungsbeschränkungen werden aktiv verteilt, so liefert z. B. das Statistische Landesamt zweimal jährlich den Adressenbestand des Regionalen Bezugssystems (RBS) und blockbezogene Einwohnerdaten an die SenStadtUmTech, die diese Daten einerseits im LAN für die Fachbereiche vorhält und andererseits bezirksweise aufbereitet an die bezirklichen Umwelt- und Stadtplanungsämter sowohl für die Bearbeitung am PC als auch unter ORACLE über das MAN ausliefert. Ebenfalls verteilt werden die Blockkarte 1 : 5000 (DiGK5) und der Flächennutzungsplan im YADE und im SICAD-Format und die Altlastenkarte im YADE-Format.

Neben den im Informationssystem SenSUT-online aufbereitet abrufbaren Karten, können über das Intranet-Angebot der SenStadtUmTech weitere Datenbestände im GIS-Format abgerufen werden, u. a.:

- DIGKS/Digitale Grundkarte v. Berlin (Blockkarte) (yka)
- FNP/Flächennutzungsplan (yka)

Im LAN der SenStadtUmTech stehen darüber hinaus:

- WSG/Wasserschutzgebietskarte (yka)
- GEWK/Gewässerkarte (yka, dxf)
- BPlan-Auskunft (yka)
- BPlan-Übersicht-Ploterstellung(yka)
- Baunutzungsplan (tif)
- ÜK50/Übersichtkarte von Berlin - einfarbig - (tif)
- ÜK50/Übersichtkarte von Berlin - zehnfarbig - (tif)
- Umlandkarte Berlin (an die DIGK5 angepaßt). (yka)
- Bestand Flächennutzung/Realnutzungskarte (yka)
- Schutzgebiete-Luftbildkataster (tif)
- LEP-EV/Landesentwicklungsplan (yka)
- Denkmalkartierung.
- Luftbilder Berlin flächendeckend

Außerdem werden über entsprechende Verweise bereits von einigen Bezirken Bereichsentwicklungspläne und Bebauungspläne im Intranet präsentiert.

Integraler Bestandteil von Fachverfahren ist der ämterübergreifende Datenaustausch bei den Verfahren Altlastenverdachtsflächenkataster (direkter Zugriff auf die ORACLE-Datenbank der SenStadtUmTech), „Lagerbehälter" und Grünflächeninformationssystem (GAIA).

Desweiteren findet projektbezogen eine Datenweitergabe der im FIS bereitgestellten Daten für Planungsaufgaben der Bezirke durch die bezirklichen Stadtplanungsämter oder durch die SenStadtUmTech statt. So wurden z. B. dem LAROV umfangreiche Datenbestände für den Aufbau des Liegenschaftsfonds zur Verfügung gestellt.

Als erster Schritt zum Aufbau des im Landesplanungsvertrag vorgesehenen Raumordnungskatasters wurde von der Gemeinsamen Landesplanungsabteilung Berlin und Brandenburg eine Übersicht der Geltungsbereiche der zwischen 1990 und 1995 bearbeiteten Bebauungspläne erarbeitet. Diese Übersicht wurde um im Projekt FIS von den Stadtplanern der SenStadtUmTech und der Bezirke gemeinsam erarbeitete Aspekte und um eine Auskunfts- und Fortschreibungskomponente erweitert. Dieses auf YADE basierende System wurde den bezirklichen Stadtplanungsämtern präsentiert und für eine kooperative Fortschreibung des Bestandes angeboten. Eine Fortschreibung des Bestandes bis Ende 1998 wird im Juli 1999 abgeschlossen sein.

**Zu 4. a) bis 4. e):** Die Planung der die FIS-Infrastruktur nutzenden Fachverfahren wird von den jeweils fachlichen zuständigen Stellen vorgenommen.

Mit der Beschaffung und der Einführung der Geodatenserver wird die in der Planungsunterlage von 1993 vorgesehene Hardwareausstattung abgeschlossen. Diese Geodatenserver sind geeignet, den gesamten bekannten Bedarf der raumbezogenen Datenverarbeitung aus den Bereichen Stadtplanung und Umweltschutz abzudecken. Dies schließt nach dem gegenwärtigen Kenntnisstand den Betrieb der im Projekt VeZuDa →

← entwickelten Systeme ein. Bei einer angenommenen Nutzungsdauer von 5 Jahren sind somit für die Jahre 2000 bis 2004 keine Ersatzbeschaffungen notwendig. Eine Ersatzbeschaffung der IRIX-Workstations für SICAD/open in den Stadtplanungsämtern kann entfallen, wenn statt dessen entweder Multifunktionale Endgeräte unter WINDOWS/NT eingesetzt werden oder eine aus Kapazitätsgründen sinnvolle und in einigen Bezirken bereits praktizierte gemeinsame Rechnernutzung von Stadtplanungsamt und Vermessungsamt erfolgt.

Für das für den Zugriff auf heterogene Datenbestände als Teilprojekt von VeZuDa sowohl für den internen Gebrauch als auch für die Nutzung im Intranet konzipierte System FIS-Broker sind die Entwicklung und die erforderlichen Schulungen nach heutigem Stand abgesichert.

**Zu 5.:** Die Fachverfahren und Datenbestände aus den Bereichen Stadtentwicklung und Umweltschutz werden kontinuierlich weiterentwickelt und an sich verändernde inhaltliche und technische Anforderungen angepaßt. Bei diesen Planungen wird die bestehende IT-Infrastruktur und damit das FIS berücksichtigt. Die Belange der von den Verfahren tangierten Stellen werden von der SenStadtUmTech bei der Planung und Entwicklung grundsätzlich mit beachtet.

Zur Zeit werden zum Beispiel folgende Aufgaben bearbeitet:

Denkmalkartierung, B-Plan-Auskunft, Bodenschutzgesetz, Friedhofsplanung, Grünflächeninformationssystem, Schutzgebiete, Landschaftsprogramm.

Berlin, den 01. Juni 1999
In Vertretung
Dr. Ing. Hans Stimmann

Senatsverwaltung für Stadtentwicklung, Umweltschutz und Technologie

(Aus: LPD 15.06.1999) ◆

# Jugendarbeit und Computer in Kinder- und Jugendbibliotheken



Der Abgeordneten Peter Schuster (SPD) wollte in einer Kleinen Anfrage (Nr. 13/4669 vom 3. März 1999) über „ Jugendarbeit und Computer in Kinder- und Jugendbibliotheken" Folgendes vom Senat wissen:

1. Wie viele Computer gibt es zur Verfügung jugendlicher Bibliotheksnutzer(innen) in den öffentlichen Kinder- und Jugendbibliotheken der einzelnen Bezirke?

2. a) Wie viele Computer sind jeweils mit welchen Prozessoren ausgestattet?
b) Wie viele dieser Computer sind multimedial nutzbar?
c) Wie viele dieser Computer haben einen Internet-Anschluß?
d) Wie viele dieser Computer sind mit einem Drucker verbunden?

3. a) In welchen Förderungsprogrammen zur Ausstattung mit Computern sind die Kinder- und Jugendbibliotheken berücksichtigt?
b) Welche Möglichkeiten sieht der Senat zur Verbesserung dieser Situation?

4. Wie hoch sind in den einzelnen Bezirken die Ausleih- und Besucherzahlen in den Kinder- und Jugendbibliotheken?

5. Welche Angebote zur Freizeitgestaltung werden von den einzelnen Kinder- und Jugendbibliotheken gemacht?

6. a) Wie wird die Jugendarbeit in den Kinder- und Jugendbibliotheken finanziert?
b) Wie hoch ist in den einzelnen Bezirken die Summe, die den Kinder- und Jugendbibliotheken für Computer-Hardware und -Software zur Verfügung steht?

7. Wie sind die Kinder- und Jugendbibliotheken konzeptionell in die Jugendarbeit des Landes Berlin und der Bezirke einbezogen?

Die Antwort (Schlussbericht) auf die Kleine Anfrage beantwortete der Senats von Berlin wie folgt:

**Zu 1. und 2.:** In den Berliner Öffentlichen Bibliotheken stehen jugendlichen Bibliotheksnutzern und Bibliotheksnutzerinnen 112 Computer (Stand Mai 1999) zur Verfügung (in der Anlage 1 der Originalantwort ist die Anzahl der Computer nach Bezirken aufgeschlüsselt, die Red.).

Die technische Ausstattung der Computer, die Anzahl der Internetanschlüsse und Drucker, die jugendlichen Bibliotheksnutzer/innen in den Berliner Öffentlichen Bibliotheken zur Verfügung stehen, geht ebenfalls aus der Anlage 1 hervor.

**Zu 3.:** a) Ein spezielles Förderprogramm zur Ausstattung mit Computern für Kinder- und Jugendbibliotheken gibt es derzeit nicht. Erstrebenswert wäre es, die Kinder- und Jugendbibliotheken Berlins in bereits bestehende Programme für die o. g. Zielgruppe, wie z. B. „Computer in die Schulen" (CidS), zu integrieren.

b) Mit dem EDV - Verbund der Öffentlichen Bibliotheken Berlins (VÖBB), der am 1. Oktober 1998 seinen Startschuß in Reinickendorf hatte und bis 2001 rund 160 öffentliche Bibliotheken mit PCs und einer einheitlichen Bibliothekssoftware ausstattet, wird sich auch diesbezüglich die Situation der Kinder- und Jugendbibliotheken entscheidend verbessern. Der Senat von Berlin finanziert die Grundausstattung des VÖBB mit über 20 Mio. DM. Bereits jetzt kann in vielen Kinder- und Jugendbibliotheken der Medienstand im OPAC (Bildschirmkatalog für Benutzer) bezirksübergreifend recherchiert werden.

**Zu 4.:** In den Berliner Öffentlichen Bibliotheken (ohne Schul- und Fahrbibliotheken) stand per 31. Dezember 1998 ein Bestand an Kinder- und Jugendliteratur von insgesamt 1.587.634 Medieneinheiten (ME) zur Verfügung (d. i. 25,82 % des Berliner ➔

← Gesamtbestandes an Medien in den Berliner Öffentlichen Bibliotheken). Die Zahl der Entleihungen von Kinder- und Jugendliteratur*) lag 1998 bei 5.179.426 ME im Jahr (d. i. 24,73 % der Gesamtentleihungen in den Berliner Öffentlichen Bibliotheken). Die Entleihungen und Besucherzahlen in den Kinder- und Jugendbibliotheken sind dagegen bisher berlinweit noch nicht flächendeckend statistisch erfaßt. Die Zahl der Entleihungen in den Kinder- und Jugendbibliotheken (ohne Schul- und Fahrbibliotheken) beträgt für 1998 rund 6.000.000 ME (siehe nachfolgende Aufstellung).

*) betrifft die Gesamtheit der Berliner Öffentlichen Bibliotheken, also auch Haupt- und Stadtteilbibliotheken

Entleihungen (ME) der Kinder- und Jugendbibliotheken (1998)

| | | |
|---|---|---|
| Charlottenburg | | 87 000 |
| Friedrichshain | | 264 029 |
| Hellersdorf | | 305 811[1)] |
| Hohenschönhausen | | 265 000 |
| Köpenick | | 336 304 |
| Kreuzberg | | 335 319 |
| Lichtenberg | | 209 000 |
| Marzahn | | 198 214 |
| Mitte | | 202 512 |
| Neukölln | | 347 985 |
| Pankow | | 200 000 |
| Prenzlauer Berg | | 391 054 |
| Reinickendorf | | 446 455 |
| Schöneberg | | 210 000 |
| Spandau | | 491 000 |
| Steglitz | | 184 582 |
| Tempelhof | | 26 022 |
| Tiergarten | | 252 374 |
| Treptow | | 360 000 |
| Wedding | | 149 038 |
| Weißensee | | 123 980 |
| Wilmersdorf | ca. | 250 000 |
| Zehlendorf | | 83 420 |
| ZLB | | 332 158 |
| Gesamt | ca. | 6 051 257 |

Quelle: Angaben (z. Teil nur in Form von Schätzungen) der Berliner Öffentlichen Bibliotheken v. Mai 1999

[1)] Entleihungen der Kinder- und Jugendlichen nur der Hauptbibliothek

**Zu 5.:** 1998 umfaßte das Angebot der Berliner Öffentlichen Bibliotheken „Bibliotheksunterricht incl. Klassen- und Gruppenführungen" insgesamt 10 375 Veranstaltungen, mit 180 893 Teilnehmern. Die nachfolgende Aufstellung zeigt dieses Ergebnis für jeden Bezirk in Zahlen.

**Spalte 2 = Bibliotheksunterricht incl. Klassen- u. Gruppenführungen (Anzahl)**
**Spalte 3 = Teilnehmer von Bibliotheksunterricht incl. der Klassen u. Gruppenführungen**

| | | |
|---|---|---|
| Charlottenburg | 130 | 1 338 |
| Friedrichshain | 198 | 3 899 |
| Hellersdorf | 231 | 5 609 |
| Hohenschönhausen | 85 | 2 001 |
| Köpenick | 229 | 2 951 |
| Kreuzberg | 921 | 17 657 |
| Lichtenberg | 451 | 8 286 |
| Marzahn | 133 | 2 895 |
| Mitte | 410 | 6 484 |
| Neukölln | 702 | 10 316 |
| Pankow | 61 | 1 373 |
| Prenzlauer Berg | 304 | 5 613 |
| Reinickendorf | 694 | 13 416 |
| Schöneberg | 316 | 6 000 |
| Spandau | 2 648 | 46 212 |
| Steglitz | 222 | 3 842 |
| Tempelhof | 858 | 11 885 |
| Tiergarten | 147 | 3 338 |
| Treptow | 150 | 2 994 |
| Wedding | 866 | 14 641 |
| Weißensee | 17 | 375 |
| Wilmersdorf | 493 | 7 808 |
| Zehlendorf | 109 | 1 960 |
| Gesamt | 10 375 | 180 893 |

Quelle: Jahresbericht der Berliner Öffentlichen Bibliotheken 1998

Weitere Veranstaltungsangebote der Berliner Kinder- und Jugendbibliotheken in Auswahl:

- Ausstellungen
- Autorenlesungen (Leseförderung)
- Einführungsveranstaltungen in die Bibliotheksbenutzung / Klassen- u. Gruppenführungen
- Internationaler Kinderbuchtag „Hans-Christian-Andersen Tag"
- Multimedia Woche für Kinder
- Vorlesewettbewerbe
- Tage der offenen Tür
- Tage des ausländischen Mitbürgers / der ausländischen Kultur
- Internet-Nutzung
- Computerkurse/ Interneteinführungen
- Bastelnachmittage
- Bibliotheksnächte
- Frühlingsfeste
- Hoffeste zu verschiedenen Anlässen
- Kinderfasching
- Kindertheater / Puppentheater / Kinderbuchkino
- Lesefeste in Schulen für geistig Behinderte
- Lesekreise, Schreibwerkstätten
- Märchentage
- Medienwerkstätten
- Preisausschreiben
- Projekttage
- Projektunterricht zu verschiedenen Themen
- Rätselquiz
- Stadtgebietsführungen
- Teilnahme an Kiezfesten
- Veranstaltungen mit Illustratoren
- weihnachtsbezogene Veranstaltungen für Hortgruppen
- Woche der Verkehrsbereitschaft
- Zaubershows u. v. a. m.

**Zu 6.:** a) Die Berliner Öffentlichen Bibliotheken verfügen über keinen gesonderten Ansatz für die Finanzierung der bibliothekarischen Jugendarbeit. Die Finanzierung der o. g. Angebote erfolgt im Rahmen der Haushaltsansätze bei Kapitel 3760 (Stadtbibliotheken) und unterliegt damit den aktuellen Haushaltsrestriktionen der Bezirke. Sie wird im Einzelfall ergänzt durch Spenden der Fördervereine der Berliner Öffentlichen Bibliotheken, aus Honorarmitteln der Bezirke, aus Mitteln der Senatsverwaltung für Wissenschaft, Forschung und Kultur für Zuwendungen für den „Internationalen Kinder- und Jugendbuchtag" und für die Literatur- und Autorenförderung:

b) Bei Kapitel 3760 (Stadtbibliotheken) ist für die Finanzierung von Computer-Hardware und Software in den →

## INFORA - Kompetenter Partner der öffentlichen Verwaltung

INFORA ist seit 1980 für Bundes-, Landes- und Kommunalbehörden sowie öffentlich-rechtliche Institutionen in Deutschland beratend tätig.

INFORA

### Konzeption und Einführung von IT-Systemen

- IT-Strategien
- Sicherheitskonzepte
- Wirtschaftlichkeitsuntersuchungen
- Qualitätssicherung von der Konzeptidee bis zum Echtbetrieb
- Ausschreibungsunterlagen und Angebotsbewertung

### Organisationsberatung

- Organisations- und Schwachstellenanalysen
- Ermittlung von Verbesserungs- und Einsparungspotentialen
- Reorganisation und Prozeßgestaltung unter Berücksichtigung verwaltungsspezifischer Besonderheiten
- Projektmanagement und -controlling

### Schriftgutverwaltung und Vorgangsbearbeitung

- Umfassende Beratung in den Bereichen Workflow-, Dokumentenmanagement, Groupware und optische Archivierung
- Erstellung spezifischer Anforderungsprofile und bedarfsgerechte Produktauswahl
- Einführungsstrategien
- Pilotierung und Produktevaluierung

INFORA GmbH
Konrad-Adenauer-Str. 13
D-50996 Köln
Tel. (0221) 93 50 50 -0
Fax (0221) 35 41 02

INFORA GmbH
Cicerostr. 21
D-10709 Berlin
Tel. (030) 89 36 58 - 0
Fax (030) 89 09 33 26

INFORA GmbH
Gerhart-Hauptmann-Str. 20
D-39108 Magdeburg
Tel. (0391) 73 79 45 - 0
Fax (0391) 73 79 45 - 9

← Berliner Kinder- und Jugendbibliotheken kein eigener Ansatz vorgesehen. Software, CD-ROM u. a. wird in der Regel aus dem Etat zur Ergänzung und Unterhaltung des Bestandes (Titel 523 02) finanziert, unter Verzicht anderer Medien.

Für 1999 sind nach Angaben der Bezirke folgende Summen aus dem regulären Etat (in der Regel Titel 515 01 / 523 02) für die Anschaffung von Computer-Hardware und Software vorgesehen:

| | Verfügbare Summe für Hard- und Software |
|---|---|
| Charlottenburg | 0 |
| Friedrichshain | 7 500 DM für Software |
| Hellersdorf | ca. 3 000 DM |
| Hohenschönhausen | nicht gesondert ausgewiesen |
| Köpenick | 6 000 DM für Software |
| Kreuzberg | 12 000 DM für Anschaffungsmittel Hardware, 11 000 DM Medienetat für CD-ROMS |
| Lichtenberg | nicht gesondert ausgewiesen |
| Marzahn | nicht gesondert ausgewiesen |
| Mitte | nicht gesondert ausgewiesen |
| Neukölln | für Software ca. 10% von Titel 523 02 (Anschaffungsetat) |
| Pankow | 4 000 DM für Software |
| Prenzlauer Berg | nicht gesondert ausgewiesen |
| Reinickendorf | 4 000 DM nur für Hauptjugendbibliothek |
| Schöneberg | ca. 2 000 bis 3 000 DM für CD-ROM |
| Spandau | 6 000 DM für Hardware |
| Steglitz | 500 DM |
| Tempelhof | nicht gesondert ausgewiesen |
| Tiergarten | nicht gesondert ausgewiesen |
| Treptow | nicht gesondert ausgewiesen |
| Wedding | nicht gesondert ausgewiesen |
| Weißensee | nicht gesondert ausgewiesen |
| Wilmersdorf | ca. 20 000 DM für Software |
| Zehlendorf | 0 |

Quelle: Angaben der Berliner Öffentlichen Bibliotheken v. Mai 1999

**Zu 7.**: Die bibliothekarische Jugendarbeit in den Berliner Öffentlichen Bibliotheken wird durch Kooperationen unterschiedlichster Art und Intensität sowohl innerbezirklich als auch bezirksübergreifend begleitet.

Beispiele in Auswahl:

- LesArt e. V., dem Berliner Zentrum für Kinder- und Jugendliteratur (Bereiche „Berliner Bibliothekstage", Veranstaltungen zur Leseförderung u. a.)
- Neue Gesellschaft für Literatur (NGL)
- Senatsverwaltung für Wissenschaft, Forschung und Kultur (Bereich Literatur- und Autorenförderung)
- Zusammenarbeit mit Institutionen der Jugendförderung im Bezirk
- intensive Zusammenarbeit mit Schulen, Kindertagesstätten und Horten
- projektbezogene Kooperation mit soziokulturellen Einrichtungen unterschiedlicher Art
- gelegentlich projektbezogene Kooperationen mit Museen und Freizeitheimen sowie mit Schülertheatern und Tanzgruppen etc.
- Unterstützung durch die Fördervereine der Berliner Öffentlichen Bibliotheken
- Kontakte zu anderen Stadtbibliotheken im In- und Ausland

Grundsätzlich ist bei der konzeptionellen Einbindung der Berliner Kinder- und Jugendbibliotheken in die übergreifende Jugendarbeit die Eigeninitiative der Bezirke gefragt.
(26. Juli 1999)
In Vertretung
Prof. v. P u f e n d o r f
Senatsverwaltung für Wissenschaft, Forschung und Kultur ◆

# Jahresberichte des Berliner Datenschutzbeauftragten



In der Plenarsitzung des Abgeordnetenhauses am 01. Juli 1999 standen die Beratung des Jahresberichtes 1997 des Berliner Datenschutzbeauftragten und die Einbringung des Jahresberichtes 1998 auf der Tagesordnung.

Der Datenschutz erhält heute im Plenum dieses Hauses einen neuen Stellenwert. Erstmals wird nicht nur der Tätigkeitsbericht des Datenschutzbeauftragten zum Vorjahr formal eingebracht, sondern es liegen auch die Ergebnisse der Beratung zum Tätigkeitsbericht 1997 zur Beschlussfassung vor. Dies gilt - wenn auch in engem zeitlichen Rahmen - die Gelegenheit, einige wesentliche Themen anzusprechen, die der parlamentarischen Behandlung bedurften und nach Zustimmung des Abgeordnetenhauses dem Datenschutz in der öffentlichen Verwaltung Berlins entscheidenden Nachdruck verleihen werden.

Die Themen, die der Unterausschuss „Datenschutz" des Ausschusses für Inneres, Sicherheit und Ordnung beraten hat, repräsentieren wie in einem Brennglas Probleme, die die ➔

← Datenschutzdiskussion seit nunmehr fast 20 Jahren geprägt haben. Die Notwendigkeit einer parlamentarischen Debatte zeigt, dass der Datenschutz zwar in der Berliner Verwaltung ein anerkanntes Regelungsziel ist, diesem in der Praxis jedoch nicht immer eine angemessene Bedeutung beigemessen ist.

Die vordergründigste Aufgabe des Datenschutzes ist der Schutz personenbezogener Daten vor unbefugter Kenntnisnahme: Neben den immer wieder vorkommenden Nachlässigkeiten im Umgang mit den Daten bergen bestimmte Organisationsformen das Risiko unberechtigter Zugriffe: Etwa die Beschäftigung von Sozialhilfeempfängern mit Tätigkeiten, bei denen diese ihrerseits Sozialdaten zur Kenntnis nehmen können, oder das immer stärker eingesetzte „Outsourcing" bei der Verarbeitung sensibler Daten, das am Beispiel der Vergabe der Krankenaktenarchivierung eines ganzen Klinikums an ein Privatunternehmen diskutiert wurde.

Neben dem Schutz vor unbefugter Kenntnisnahme ist der Schutz der Bürgerinnen und Bürger vor der Verwertung veralteter Daten ein zentrales Ziel des Datenschutzes: Das Recht einer jeden Person auf Rehabilitation und Neuanfang muss abgesichert werden durch die fristgerechte Löschung von Daten über Verfehlungen, vergleichbar mit der menschlichen Tugend des Vergessens und Vergebens. Dies den Ordnungsbehörden immer wieder nahe zu legen, ist eine unserer wichtigsten Aufgaben. Parlamentarischer Unterstützung bedurfte es bei der Umsetzung neuer Vorschriften im Straßenverkehrsrecht, die die von dem Datenschutzbeauftragten seit vielen Jahren geforderte Bereinigung der Führerscheinakten von weit zurückliegenden Straftaten zur gesetzlichen Pflicht machen, oder bei der Frage, wie lange längst veraltete Bundeszentralregisterauskünfte in den Gewerbeakten aufbewahrt werden dürfen.

Das Bundesverfassungsgericht hat dem Datenschutz in der Form des informationellen Selbstbestimmungsrechtes Grundrechtscharakter verliehen; daraus folgt, dass - soweit möglich - die ohne Zwang ausgesprochene Einwilligung der Betroffenen in die Verarbeitung ihrer Daten oberster Grundsatz sein sollte. Gerade die Nutzung neuer Informationstechnik, die mit großen Risiken verbunden ist, bedarf grundsätzlich der freien Entscheidung der Betroffenen. Die Veröffentlichung von Personaldaten im Internet oder die Veröffentlichung von Daten über Mitarbeiterinnen und Mitarbeiter der Verwaltung, die im Rahmen des „Ideenmanagements" Vorschläge für die Verbesserung von Arbeitsabläufen machen, sind Beispiele hierfür.

Die Gesetzgebung auf dem Gebiet des Datenschutzes wird häufig sehr kritisch betrachtet, im vergangenen Herbst etwa in den Diskussionen des Deutschen Juristentags in Bremen. Der Vorwurf der Überregulierung ist jedoch unberechtigt. An manchen Stellen mag der Gesetzgeber zwar über das gebotene Maß an Regulierung hinausgeschossen sein. In der Regel geschah dies aber gerade nicht, um Bürgerrechte zu schützen, sondern um immer weitergehende Eingriffe in die informationelle Selbstbestimmung zu ermöglichen. Demgegenüber gibt es noch immer Bereiche, in denen konkrete Datenschutzregelungen, die dem Bürger Rechte in die Hand geben, fast ganz fehlen oder die diese Rechte nicht hinreichend klar berücksichtigten. So verschafft das Steuerrecht dem Staat zwar außer Geld den Zugang zu einer Vielzahl sensibelster Daten, enthält aber nach wie vor den Steuerzahlern das in anderen Gebieten selbstverständliche Recht auf Auskunft über seine Daten vor. Die Beschlussempfehlung der Senat solle sich für die Aufnahme datenschutzrechtlicher Bestimmungen in die Abgabenordnung einsetzen, zielt auf die Schließung einer der letzten großen Lücken der Datenschutzgesetzgebung. Andere Bereiche, wie z. B. das Melderecht, warten seit Jahren auf datenschutzrechtliche Korrekturen.

Das Bundesverfassungsgericht hat die Existenz der Datenschutzbeauftragten als eine unabdingbare Voraussetzung des rechtmäßigen Umgangs mit personenbezogenen Daten angesehen, Voraussetzung hierfür ist der unbeschränkte und bedingungslose Zugang des Datenschutzbeauftragten zu den Daten sowie den Unterlagen über ihre Verarbeitung. Vor diesem Hintergrund verwundert es, dass es eines Beschlusses dieses Hauses bedarf, um die Innenverwaltung anzumahnen, den Datenschutzbeauftragten auch rechtzeitig über datenschutzrelevante Vorhaben des Bundes zu informieren, die für die Verarbeitung von Daten in den Ländern von großer Bedeutung sind. Überhaupt ist in einigen Bereichen die Bereitschaft der Verwaltung, mit dem Datenschutzbeauftragten zu kooperieren, in den letzten Jahren deutlich gesunken, so dass in jüngster Zeit sogar der Eindruck entstand, der Datenschutz solle aus politischen Diskussionen herausgehalten werden.

Weltweit wird heute unter dem Schlagwort „Privacy Enhancing Technologies" die Forderung diskutiert, dass Datenschutz nicht nur als lästiges Anhängsel von Automationsvorhaben, sondern als Strukturmerkmal informationstechnischer Verfahren betrachtet wird. In den Beschlussentwürfen, die Ihnen zur Einführung von Informations-, Kommunikations- und Mediendiensten durch öffentliche Wohnungsbaugesellschaften, zu der Neugestaltung des polizeilichen Informationssystems oder zur Landesinitiative „Der Berliner Weg in die Informationsgesellschaft" vorliegen, macht sich dieses Haus die Forderung nach datenschutzfreundlichen Technologien zu eigen. Es sollte Ziel Berliner Politik sein, diese Stadt nicht nur zu einem hervorragenden Standort für Informations- und Kommunikationstechnik zu machen, sondern auch Vorbild zu geben für die menschengerechte Gestaltung dieser Techniken. Dass dabei Grenzen des Einsatzes der Informationstechnik ins Blickfeld geraten, zeigen die in Berlin wohl inzwischen fallengelassenen Pläne zur Einführung einer Elektronischen Fußfessel, die den Strafvollzug durch einen virtuellen elektronischen Käfig ersetzt.

Der Jahresbericht 1998 zeigt erneut, dass die Informationstechnik und damit die daraus resultierenden Datenschutzprobleme für die Menschen immer undurchschaubarer werden. Um so unverständlicher ist es, dass der Datenschutz zu denjenigen Gebieten gehört, die man (angesichts organisatorischer und haushaltsmäßiger Zwänge) am ehesten vernachlässigen zu können glaubt - unsere Untersuchung zu Stellung und Unterstützung behördlicher Datenschutzbeauftragter in der Berliner Verwaltung macht dies deutlich. ◆

# Hochschulbibliothek der FHVR Berlin: Retro-Konversionsprojekt erfolgreich abgeschlossen



Die Hochschulbibliothek der Fachhochschule für Verwaltung und Rechtspflege Berlin, Serviceeinheit für Informations- und Medienmanagement, befindet sich seit längerer Zeit im Prozeß der Automatisierung, um ihre im Berliner Hochschulgesetz bestimmten Aufgaben zur Sammlung, Erschließung und Nutzungsbereitstellung von Literatur und anderen Informationsträgern noch effizienter zu erfüllen; dies gilt besonders in Anbetracht der Aktivitäten zur Verwaltungsreform und vor dem Hintergrund knapper Personalressourcen und Sachmittel.

Eingesetzt wird das DV-gestützte Bibliotheksmanagementsystem der Firma SISIS GmbH, das nach dem Prinzip der Client-Server-Architektur arbeitet. Grundlage für das UNIX-Systemmodell ist ein Server mit der Gerätebezeichnung RM 400-430, dessen zentrale Komponente (CPU) ein Motherboard mit einem RISC-Prozessor R4400SC darstellt. Das Betriebssystem SINIX basiert auf UNIX (SystemV-kompatibel), die Datenbankgrundlage bildet Informix-ONL mit SQL.

Das Bibliotheksmanagementsystem SISIS besteht aus mehreren Modulen, die, vereinfacht formuliert, einzelne arbeitsorganisatorische Bereiche einer Bibliothek abbilden: Katalogisierung (SIKIS), Erwerbung (SIERRA) und Benutzung (SIAS), unterstützt von einem Modul für die Fremddatenübernahme (SIKMASS) und, last but not least, dem elektronischen Benutzer- oder Publikumskatalog (OPAC). Alle Module sind korrespondierend miteinander verzahnt – man spricht in diesem Kontext auch von einem *integrierten* Bibliothekssystem, dem die Idee zugrunde liegt, Daten, die zu einer Medieneinheit gehören, einmalig zu erfassen und danach immer wieder zu verwenden; dadurch tritt eine „ganzheitliche arbeitsprozeßorientierte Ablauforganisation" in den Vordergrund, verbunden mit Erfordernissen zur Reorganisation des Dienstleistungs- und Produktionsbetriebes Bibliothek.

Ein wichtiger erster Schritt für eine automatisierte Bibliotheksverwaltung stellte das von der Hochschulbibliothek der FHVR Berlin in Zusammenarbeit mit der Kommtreff Qualifizierungs- und Beschäftigungesellschaft mbH durchgeführte Projekt zur Retro-Konversion des gesamten Bibliotheksbestandes dar.

Die Kommtreff QG, zu deren Spektrum die Erhebung und Verarbeitung von Massendaten gehört, führt im Auftrag des Arbeitsamtes auch Projekte zur Retro-Konversion in Bibliotheken durch. Im Rahmen des Projektes an der FHVR Berlin erfaßten rund zehn Projektmitarbeiter (die Zahl der Mitarbeiter schwankte während der Dauer des Einsatzes geringfügig) die einzelnen Medien rückwirkend digital, das heißt, die über die Zettelkataloge der Bibliothek konventionell vorhandenen bibliographischen Daten wurden anhand der vorliegenden Medien (Autopsie!) durch manuelle Eingabe in die elektronische Datenbank überführt. Nach dem Abspeichern der SIKIS-Katalogaufnahme mußten die für eine spätere Ausleihe benötigten Angaben, wie Mediennummer, Sonderstandorte (Lesesaal usw.), Medientyp (Präsenz-, Ausleihexemplar usw.), Beilagen oder Hinweise auf etwaige Beschädigungen, eingetragen werden, die sogenannte SIAS-Datenerfassung. Der Input einer für jede physikalische Einheit individuellen Mediennummer erfolgte durch Einscannen (Handscanner) eines eigens generierten Barcodes.

Grundsätzlich möglich sind auch andere Vorgehensweisen zum Zwecke der Retro-Konversion – prioritär zu nennen wären: die Übernahme fertiger Titelaufnahmen aus fremden Datenbanken, beispielsweise dem Datenpool (Deutsche Nationalbibliographie) der Deutschen Bibliothek (online respektive off-line von der CD-ROM-Ausgabe) oder dem Kooperativen Bibliotheksverbund Berlin-Brandenburg (KOBV, vormals BBVB), sowie als optisches Mittel das Einscannen der eigenen Katalogisate, um übernommene Titelstrukturen nicht um die Spezifika der FHVR-Hochschulbibliothek ergänzen zu müssen. Diese Modi erfordern gewisse Voraussetzungen und Funktionalitäten – nicht nur technischer Art, die für die Hochschulbibliothek nicht ohne weiteres gegeben waren, so daß das von der Kommtreff QG relativ kurzfristig angebotene Verfahren, überdies bestätigt durch namhafte Referenzen, eindeutig präferiert wurde.

Vor Projektbeginn (November 1997) mußten eine Vielzahl von zeit- und arbeitsintensiven vorbereitenden Arbeiten bewältigt werden, um das gesamte Vorhaben sachgerecht durchführen zu können. Dazu war es leider unumgänglich, das Leistungsangebot der Hochschulbibliothek vorübergehend zu reduzieren. Die Hochschulbibliothek entwickelte Raumkonzepte zur Unterbringung der Projektmitarbeiter und stellte Arbeitsplätze mit entsprechender Hardwareausstattung zur Verfügung. Das neu beschaffte Modul für die Katalogisierung wurde durch Parametrierungen für die laufenden Erfassungsarbeiten angepaßt und zugleich auf die Bedürfnisse des Projektes zugeschnitten. Komplexe Arbeitsabläufe und –verfahren, konzipiert für das Retro-Projekt, wirkten sich, was es zu berücksichtigen galt, schließlich auch in einem erheblichen Maße auf die Organisation der Hochschulbibliothek aus. Die Einschränkungen für die Kunden mußten darüber hinaus so gering wie möglich gehalten werden; trotzdem ließ es sich nicht gänzlich vermeiden, die sich jeweils in Bearbeitung befindlichen Medien eines bestimmten Sachgebiets aus dem Freihandbestand und die Äquivalente des systematischen Kataloges dem Zugang durch die Nutzer kurzzeitig zu entziehen. ➔

← Die Grundeinweisungen: Einführung in die Grundlagen der Datenverarbeitung und in die bibliothekarische Arbeitsweise (Aufbau von wissenschaftlichen Bibliotheken, Titelaufnahme etc.), fanden bei der Kommtreff QG statt. Daneben vermittelten Beschäftigte der Hochschulbibliothek - im Team-Teaching - in einer hausinternen, zunächst anderthalb Wochen umfassenden Schulungsmaßnahme das erforderliche Know-how im Umgang mit dem an der FHVR Berlin eingesetzten integrierten Bibliotheksmanagementsystem SISIS und über die beabsichtigten verfahrenstechnischen Abläufe sowie spezielle Kenntnisse über die Struktur und die Besonderheiten der über fast 25 Jahre hinweg entstandenen, vorhandenen Katalogisate; denn Dateneingabe darf hier keineswegs mit „blindem Eintippen" verwechselt werden. Dafür implementierte die DV-Systembetreuung im Seminarraum der Hochschulbibiothek ein eigenes Schulungsnetz.

Die auf diese Weise qualifizierten und für die konkrete Aufgabenerledigung eingearbeiteten Projektmitarbeiter, die ja bisher in bibliotheksfremden Berufen tätig waren, erhielten darüber hinaus in regelmäßigen Abständen oder aus aktuellem Anlaß geeignete Nachschulungen (Vortrag mit praktischen Übungen). Das entband allerdings nicht von der Notwendigkeit, täglich die Projektmitarbeiter durch Fachpersonal zu betreuen: Mitarbeiter der Hochschulbibliothek klärten offene Fragen und in der Bearbeitung schwierige Fälle. Unabhängig davon, sichtete und kontrollierte ein Bibliotheksmitarbeiter täglich die Arbeitsergebnisse von rund zehn Projektmitarbeitern und veranlaßte gegebenenfalls Korrekturen bei fehlerhaften Dateneingaben. Hinzu kamen Steuerungs- und Koordinationsaufgaben, erleichtert dadurch, daß seitens der Kommtreff QG eine kompetente Projektleiterin vor Ort als Ansprechpartnerin zur Verfügung stand. Dennoch führte die Bindung von Bibliothekspersonalressourcen für Sonderaufgaben in ihrer Folge zu Rückständen in der laufenden Arbeit. Abhilfe schaffte später die Einstellung eines Diplom-Bibliothekars über einen Werkvertrag für die Dauer des Projektes. Das Arbeitsamt bewilligte die Projektmittel aufgrund der Regelungen für eine Lohnkostenzuschuß-Maßnahme (LKZ) nach § 249 h des Arbeitsförderungsgesetzes für nur sechs Monate. Bei der Planung, Vorbereitung und sogar während des Projektes aber ging die Hochschulbibliothek, Zusagen der Beteiligten zufolge, von einer Laufzeit von einem Jahr aus und hat diesbezüglich ihre Organisation und Arbeitsverfahren ausgerichtet. Erst nach konsequenter Intervention der FHVR Berlin und der Kommtreff QG erfolgte nach Ablauf des bereits genehmigten halben Jahres eine Umwandlung in eine AB-Maßnahme, damit einhergehend eine Verlängerung für ein weiteres Jahr mit überwiegend demselben – eingearbeiteten! – Mitarbeiterkreis.

Kostenneutral für die FHVR Berlin, wie gelegentlich zu hören, war das Retro-Projekt sicherlich nicht. Zwar finanzierte das Arbeitsamt die Personalkosten für die Projektmitarbeiter – der wesentlichste Faktor, zweifelsohne –, auch wurden zusätzlich benötigte Arbeitsmittel und Hardware (z.B. Scanner) durch die Kommtreff QG bereitgestellt, doch die Personal- und Sachmittelaufwendungen, die in der Hochschulbibliothek für vielfältigste Vorbereitungen, Schulungen, Betreuungsleistungen, einen Werkvertrag, beschaffte Arbeitsplatzrechner (natürlich unter dem Vorbehalt einer sinnhaften Verwendung nach Beendigung des Projektes) und anderes mehr entstanden sind, schlagen im Sinne der Kostenrechnung zu Buche. Der Nutzen aber ist unbestritten größer. Parallel zur laufenden Katalogisierung wäre die digitale retrospektive Erfassung des gesamten Bibliotheksbestandes mit der derzeitigen Personalausstattung, personelle Engpässe dabei unberücksichtigt gelassen, selbst langfristig kaum möglich.

Nach nunmehr anderthalb Jahren, Ende April 1999, fand das Retro-Konversionsprojekt seinen überaus erfolgreichen Abschluß; die Qualität der Arbeitsergebnisse ist etwaigen Vorbehalten zum Trotz beachtlich gut. Im Ergebnis sind alle Freihandbestände einschließlich der Lehrbuchsammlung im elektronischen Benutzerkatalog (OPAC, Online Public Access Catalogue) suchbar. Der Prozeß der Einführung eines integrierten Bibliotheksmanagementsystems konnte damit ein wesentliches Stück vorangetrieben werden: Im Rahmen der Erfassungsarbeiten wurden zugleich sämtliche Medieneinheiten mit einem selbstklebenden Barcodeetikett versehen, eine wichtige Voraussetzung für die vorgesehene Automatisierung der Ausleihverbuchung, die das Serviceangebot der Hochschulbibliothek qualitativ verbessern und erweitern wird. Eine Umsetzung im Echtbetrieb der Konzeptionen für die DV-gestützte Ausleihverwaltung erfolgt voraussichtlich im Laufe des kommenden Wintersemesters.

Der OPAC, der alle Vorteile einer Datenbank bietet, ermöglicht den Bibliotheksbenutzern, Informationen bequemer , schneller - computerschnell! - und effizienter zu finden; selbst nur fragmentarisch vorliegende Angaben führen jetzt in der Regel zu einem positiven Suchergebnis (immer vorausgesetzt, das recherchierte Medium ist grundsätzlich im Katalogbestand der FHVR-Hochschulbibliothek nachgewiesen). Zeitgleich mit dem Abschluß des Retro-Konversionsprojektes ersetzte der neue JAVA-OPAC den bisherigen WIN-OPAC: Die vorliegende Programmversion bietet erweiterte Funktionen an, ist komfortabler in ihrer Bedienung (Softwareergonomie), plattformunabhängig und überdies intra- und internetfähig. Weil sich die praxiserprobte Funktionalität der SISIS-Module mit einer javabasierten Oberfläche vereint, spricht man vom JAVA-OPAC. Damit ist endlich die Grundlage für einen vollständigen Abbruch und eine Auflösung des alphabetischen Zettelkataloges geschaffen. Der Zettelkatalog: ein durch erzielte Fortschritte überholtes und nicht mehr übliches Literaturerschließungsinstrument - eben ein Anachronismus.

*FRANK WEHRAND*

FHVR Berlin, SE Hochschulbibliothek,
Tel. 9021 (intern 921) - 4200, Fax - 4217,
frank.wehrand@fhv.verwalt.berlin.de ◆

# Solum Star



Anläßlich der Einführung des papierlosen Grundbuchs SOLUM STAR im Familiengericht Tempelhof/Kreuzberg am 8. Juli 1999 führte Berlins Justizsenator Dr. Ehrhart Körting unter anderem aus:

„Welche Neuerungen sind mit dem maschinell geführten Grundbuch verbunden? Bislang ging ein Antrag auf Eintragung bei der Geschäftsstelle des Grundbuchamtes ein und wurde dem Rechtspfleger vorgelegt. Dessen Verfügung ging erneut zur Geschäftsstelle und von dort zur Eintragerin, die die erfolgte Eintragung noch einmal mit dem Rechtspfleger gegenlas. Anschließend wurde der Vorgang über die Geschäftsstelle zur Kanzlei gegeben, um die Eintragungsbenachrichtigung zu fertigen.

Ganz anders im elektronischen System: Auch hier kommt der Eintragungsantrag zwar über die Geschäftsstelle zum Rechtspfleger; doch dieser gibt die Eintragungsverfügung sofort am Bildschirm ein und schließt den Vorgang durch seine elektronische Unterschrift ab. Damit veranlaßt er, daß die Daten im Archivsystem der Grundbuchdatenzentrale abgespeichert werden. Mit dieser Abspeicherung ist die Eintragung rechtswirksam. Anschließend erteilt die Geschäftsstelle die Eintragungsmitteilung. Statt vier sind also nur noch zwei Personen an der Eintragung beteiligt, der zeitliche, bürokratische und organisatorische Aufwand wird minimiert.

Die elektronische Speicherung ist künftig auch das alleinige Original des Grundbuchs. Deshalb müssen die rund 500.000 Berliner Grundbuchblätter nach und nach auf das neue System umgestellt werden. Dies geschieht zum größten Teil - nämlich bei etwa 80% der Blätterdurch Scannen der Altdaten, daneben müssen vor allem Folianten von Hand erfaßt werden. Die Altdatenerfassung läuft seit März dieses Jahres und soll bis Ende 2000 abgeschlossen sein. Den aktuellen Fortschritt werden wir jeweils auf einer Internet-Seite dokumentieren, deren Adresse in Kürze bekanntgegeben wird.

Der Umstieg auf das elektronische Grundbuch bringt allen Beteiligten wesentliche Vorteile. Das gilt zunächst für diejenigen, die ein Recht eintragen lassen möchten. Dies war bislang oft mit langen Wartezeiten verbunden. Verzögerungen bei der Baudarlehensgewährung und beim Baubeginn sowie zusätzliche Kosten waren die Folge. Durch die maschinelle Bearbeitung hingegen wird sich das Eintragungsverfahren erheblich - als Anhaltswert: 50% - beschleunigen; denn es entfällt die Zeitspanne zwischen der Verfügung des Rechtspflegers und der tatsächlichen Eintragung durch die Schreibkraft.

Externe Nutzer wie Notare und Kreditinstitute profitieren von dem schnelleren uns leichteren Online-Zugriff. Sie können künftig vom eigenen Büro aus über eine ISDN-Verbindung alle Grundbuchdaten abrufen und ausdrukken, sogar wenn gerade andere ebenfalls Einblick in dieses Grundbuch nehmen. Zugleich informiert eine sogenannte Fallübersicht über den aktuellen Stand des Bearbeitungsverfahrens. Damit können Notare ihre Mandanten schon im Beratungsgespräch über die gegenwärtigen Verhältnisse unterrichten, können Kreditinstitute ihre Darlehensentscheidungen zügiger treffen. Zum Vergleich: Bislang mußten beglaubigte und meist selbst einfache Abschriften beantragt werden, ihre Herstellung und Versendung wurde verfügt, und erst nach einigen Tagen lagen sie dem Notar vor.

Ermöglicht wird der Umstieg auf das elektronische Grundbuch durch die Software SOLUM STAR. Der Name setzt sich aus dem lateinischen Wort für Boden sowie der Abkürzung für „System für Textverarbeitung, Archivierung und Recherche“ zusammen. Die Software wird bereits von den Ländern Bayern, Bremen, Hamburg, Sachsen und Sachsen-Anhalt eingesetzt, weitere Länder wollen nachziehen. Berlin gehört damit bundesweit zu den Vorreitern des elektronischen Grundbuches - vor allem hinsichtlich der Erfassung von Altvorgängen, die wir als drittes Bundesland nach Hamburg und Bremen abschließen werden.

Bei der Hardware sind ebenfalls intensive Vorarbeiten zu leisten. Alle Grundbuchämter werden mit neuen geeigneten Computern ausgestattet, alle Amtsgerichte werden im Zuge dieses Projektes miteinander vernetzt. Wir arbeiten dabei eng mit dem Landesbetrieb für Informationstechnik - dem LIT - zusammen. Dort wird auch die vorhin erwähnte Grundbuchdatenzentrale untergebracht sein.

Angesichts all dieser erheblichen Investitionen wäre das Projekt SOLUM STAR aus öffentlichen Mitteln kaum zu verwirklichen. Wir freuen uns deshalb, daß wir dafür einen starken und erfahrenen Partner gewinnen konnten, die Siemens AG. Sie übernimmt die Finanzierung der Hard- und Software, sichert die Betriebsbereitschaft der Anlage und sorgt in zwei Zyklen für die erforderlichen Innovationen. Der Finanzierungsvertrag mit einem Volumen von über 20 Mio. DM und einer Laufzeit von mindestens zehn Jahren bringt gegenseitigen Nutzen. Wir entlasten den Steuerzahler, indem eine Verwaltungsaufgabe durch Privatfinanzierung erfüllt und das wirtschaftliche Risiko von unserem Partner übernommen wird. Und dieser refinanziert seine Investition aus den bundesweit geltenden Abrufgebühren, die private Nutzer im Online-Verkehr zahlen müssen.

Mit einer solchen „public-private-partnership“ gehen wir jene neuen Wege, die die Bürgerinnen und Bürger zu Recht von einer modernen Verwaltung erwarten. Ebenso berechtigt erwarten die Bürgerinnen und Bürger aber, daß mit ihren Daten sorgfältig umgegangen wird. Deshalb setzt die Teilnahme am automatisierten Abrufverfahren eine behördliche Zulassung voraus, die der Präsident des Amtsgerichts voraussichtlich ab September erteilen wird. Ein Kontrollverfahren schützt davor, daß Unberechtigte Grundbuchdaten manipulieren; dazu gehören mehrfache digitale Signaturen, Anzeigen von Manipulationsversuchen und verschlüsselte Datenübertragungen. Und vor unbeabsichtigten Löschungen oder Abstürzen schützen Sicherungskopien, die räumlich getrennt vom Originalarchiv eingerichtet werden.“ ◆

# Aktuelle Projekte aus dem Deutschen Insitut für Urbanistik

**Telematikgestützte Regionale Netze (TRN)**



Derzeit sind in Europa diverse Initiativen zum Aufbau lokaler oder regionaler Informations- und Kommunikationsinfrastrukturen zu beobachten. Ein besonderer Fall sind die telematikgestützten regionalen Netze (TRN), mit denen vorhandene regionale Netzwerkstrukturen zwischen Unternehmen bzw. Unternehmen und anderen Akteuren in der Region gestärkt oder neue geschaffen werden sollen. Mit ihrem Aufbau werden eine Reihe von spezifischen Zielen für die Stadt- und Regionalentwicklung verbunden.

Ziele der Untersuchung waren eine Bestandsaufnahme vorhandener TRN in Deutschland und Europa, die Ermittlung von Nutzungsmustern, die Darstellung der Inhalte mit Relevanz für die Regionalentwicklung und die Analyse von Auswirkungen auf die Regionalentwicklung. Ausgangsthesen waren, daß

- entsprechende telematik-gestützte Netze die Innovationsfähigkeit und -tätigkeit von Unternehmen, speziell von KMU fördern,
- kooperative Zusammenarbeit in Netzen forcieren und
- eher vorhandene Netzwerkstrukturen stärken als neue erzeugen.

Auswahlkriterien für die zu untersuchenden TRN waren u.a. ein eindeutiger Regionsbezug, die Eigeninitiative von Unternehmen oder anderen Akteuren der Region, ein wirkliches Netzwerk der Kooperationsbeziehungen (mehr als ein Knoten) und eine mindestens einjä hrige Kooperation.

Den Kriterien weitgehend entsprechende Projektideen bzw. Projekte in der Aufbauphase konnten in Großbritannien, in Belgien und den Niederlanden, aber auch in Deutschland in unterschiedlichen Branchen nachgewiesen werden; allerdings ließen sich aufgrund der frühen Phase noch keine Erfahrungen ableiten. So ließen sich trotz umfangreicher Recherchen nur drei Projekte identifizieren, die weitestgehend alle o.a. Voraussetzungen erfüllten:

- das Virtuelle Softwarehaus Berlin-Brandenburg,
- die Online-Hanse,
- das schwedische Netzwerkprojekt Föreningen-Träindustri.

Die Untersuchung der Projekte durch qualitative Befragungen, schriftliche und Online-Erhebungen brachte ernüchternde Ergebnisse. Die Nutzenpotentiale des Internet zur Stärkung der Kooperationsbeziehungen und der Wettbewerbsfähigkeit wurden nur sehr unzureichend ausgeschöpft.

Die Thesen ließen sich durch nur geringe Zahl zu identifizierender TRN weder falsifizieren noch verifizieren. Es deutet aber einiges daraufhin, daß nur die dritte These, nämlich die Stärkung bestehender Netzwerkstrukturen (im Gegensatz zum Aufbau neuer) Bestand hat. Effekte im Hinblick auf ein verbessertes Innovationsverhalten ließen sich kaum feststellen.

Es ist zu vermuten, daß die Fragestellung noch etwas „zu früh“ kam. Inzwischen gibt es eine Vielzahl weiterer Ansätze (u.a. mit Unterstü tzung aus Mitteln des Europäischen Sozialfonds durchgeführte Projekte), die mit gewissem Abstand eine erfolgreichere Evaluationen zulassen wü rden. Veröffentlichung in Vorbereitung: Steffi Bütow, Britta Oertel, Henning Marten, Telematikgestützte Regionale Netze, Berlin 1999.

**Forum Telematische Städte - KOMM!**

Das Projekt „KOMM! - Forum Telematische Städte“ ist eine gemeinschaftliche Initiative des Deutschen Instituts für Urbanistik (Difu), des Sekretariats für Zukunftsforschung (SFZ) und des Forschungszentrums für Informationstechnik, Institut für Systementwurfstechnik (GMD-SET). Ziel ist es, für die Kommunen ein bundesweites, interaktives Forum zum gegenseitigen Erfahrungsaustausch, zur Projektentwicklung und Kooperation auf den Feldern der Informations-und Kommunikationstechnologien und neuen Medien zu schaffen. Unterstü tzend soll ein ergänzendes, bundesweites Netzwerk mit themenbezogenen „Kompetenzknoten“ aufgebaut werden.

Das Forum soll im wesentlichen aus zwei Bausteinen bestehen: Einem Online-Forum im Internet und einem Forum zum persönlichen, „materiellen“ Austausch; der Schwerpunkt der Aktivitäten liegt auf der Entwicklung der Online-Plattform. Mit KOMM! sollen sowohl übergreifende Themenstellungen (z.B. die Konzeption einer schlüssigen kommunalen IuK-Politik, die Auswirkungen der Telematik auf die Städte) wie auch Einzelaspekte (z.B. kommunale Netzinfrastruktur, Stadtinformationssysteme, Verkehrstelematik, Telearbeit, Digitale Signatur und interaktive Verwaltung) behandelt werden. Es ist angestrebt, KOMM! auch als Plattform für den kommunalen Erfahrungsaustausch im Rahmen des BMBF-Stä dtewettbewerbs Multimedia „MEDIA@Komm“ auszubauen.

Eine Pilotphase hat das Ziel, einen Prototypen der Online-Plattform zu entwickeln und dabei thematische Teilaspekte beispielhaft aufzubereiten. Gleichzeitig wird die Vorgehensweise für die weiteren Projektphasen spezifiziert. In der Ausbau- und Konsolidierungsphase werden die Themenfelder schrittweise erweitert, das Netzwerk von Kompetenzknoten aufgebaut und begleitende Maßnahmen (z.B. Marketing, Ausbau von Dienstleistungen) intensiviert. Mit der Pilotphase wird im Sommer 1999 begonnen. Finanziert und mitgetragen wird das Projekt zu großen Teilen von der Deutschen Bank, der Deutschen Telekom, IBM Deutschland und dem BMWi. Die Kommunikations- und Kooperationsplattform von MEDIA@Komm wird auf KOMM! aufsetzen.

(Informationen aus den Internet-Seiten unter: difu.de/projektforen/laufende Projekt) ◆

# „Die virtuelle Zukunft der öffentlichen Verwaltung - und wo bleibt der Mensch?“

*„Die virtuelle Zukunft der öffentlichen Verwaltung - und wo bleibt der Mensch?“ fragt Dr. Ulrich Kampffmeyer, Leiter der Project Consult Unternehmensberatung GmbH Hamburg. Die interessanten und ausführlichen Antworten auf diese Frage können die SPLITTER-Leser in einer fünfteiligen Serie ab dieser Ausgabe lesen. Teil I führt in das Thema ein, Teil II gibt Antworten auf die Frage, warum viele DMS-Projekte scheitern. Der dritte Teil steht unter der Überschrift „Zwischen Unter- und Überforderung“, während sich der vierte Teil dann mit dem „Homo Buerocraticus“ beschäftigen wird. Die letzte Folge behandelt das Thema „Wissen und Knowledge Management“.*

## Einführung

Dokumentenmanagement-Technologie wird heute als die Möglichkeit betrachtet, Verwaltungsabläufe und Informationsbereitstellung zu optimieren. Wenn ich heute von Technologie im Sinne des Titelthemas spreche, meine ich hier natürlich nicht nur die eingegrenzte Dokumentenmanagement-Technologie im engeren Sinn. Im weiteren Sinn betrifft dieselbe Entwicklung auch Workflow, Archivierung und andere Themen, die jetzt durch die Internettechnologie hinzugekommen sind. Wenn ich über den Menschen in der Arbeitswelt von heute spreche, möchte ich mich auf einige Aspekte beschränken, die die Auswirkung der Technologie auf die Anwender solcher Systeme betreffen.

Dieses Thema ist sehr vielfältig. Daher möchte mich heute eigentlich nur auf fünf wesentliche Aspekte beschränken. Dies sind - nach einer kleinen Einführung in die Thematik „Dokumentenmanagement„ - die Themen:

- warum viele DMS-Projekte scheitern,
- der Mensch zwischen Über- und Unterforderung,
- der „Homo buerocraticus“,
- das Management von Wissen: Knowledge Management.

## Trends im Dokumentenmanagement

Dokumentenmanagement ist heute ein sehr weit gefaßter Begriff, der sich längst von den Ursprüngen des „Document Imaging„ und „Optical Filing„ entfernt hat. Es wird heute zwischen Dokumentenmanagement „im engeren Sinn„ und „im weiteren Sinn„ unterschieden:

### Dokumentenmanagement im engeren Sinn

Ursprünglich waren die verschiedenen Dokumentenmanagement-Technologien eher monolithische Anwendungen mit speziellen Clienten für die jeweiligen Applikationen ohne die Berücksichtigung von Integrationsaspekten. Klassisches Dokumentenmanagement in diesem Sinn dient der dynamischen Verwaltung von elektronischen Dokumenten und Dateien in Netzwerken mit Funktionalitäten wie:

- Check-in/Check-out
- Versionsmanagement
- Zugriffsschutz
- Bildung von Dokumentengruppen (Containern)
- Selbstbeschreibende Informationsobjekte

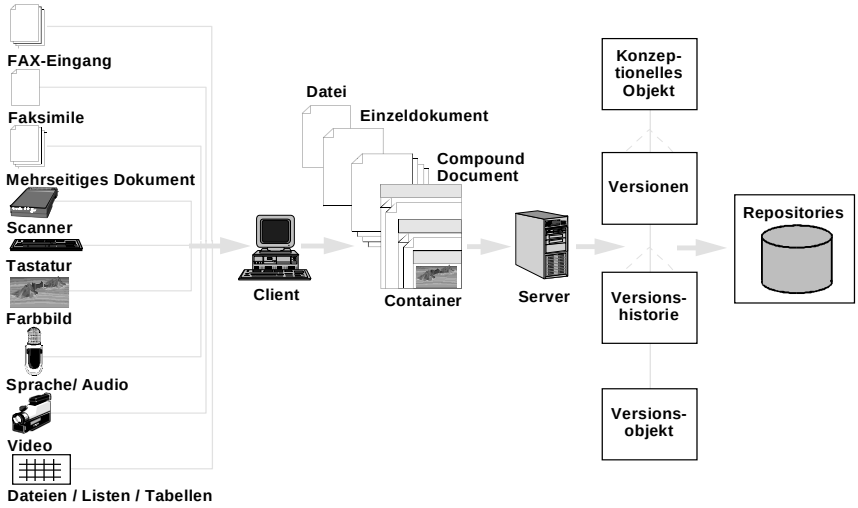



*Abbildung 1 Dokumentenmanagement im engeren Sinn*

### Dokumentenmanagement im weiteren Sinn

In Anbetracht einer zunehmenden Überschneidung und Integration der verschiedenen Dokumentenmanagement-Technologien werden unter Dokumentenmanagement im weiteren Sinn abgesehen von dem klassischen Dokumentenmanagement weitere Systeme und deren Zusammenspiel subsumiert: ➔

- **Bürokommunikation / Office-Pakete**
  Einzelne Module wie Textverarbeitung, Kalkulation, Grafik, Datenbank, Kalender, Mail oder Fax, aktive Steuerung durch den Anwender
- **Document Imaging**
  Scannen, Anzeigen, Drucken und Verwalten von Faksimile-Dokumenten
- **Elektronische Archivierung**
  Speicherung von Daten, Images und/oder Listen, datenbankgestützter Zugriff, Auslagerung, Revisionssicherheit
- **E-Forms**
  Elektronische Formulare für die Eingabe, Anzeige, Ausgabe und Verwaltung variabler Informationen
- **Output-Management**
  Erstellung, Verwaltung und Druckausgabe bei professionellen Druckerstraßen
- **Groupware**
  Kooperatives Arbeiten, datenbankgestützte Verwaltung von Daten und Dateien, Replikation, Gruppenfunktionen wie Kalender oder Mail, Verknüpfung und Integration einzelner Komponenten
- **Workflow**
  Strukturierte Abläufe, Status- und Aktionsüberwachung, regelbasierte Steuerung, Verarbeitung von CI- und NCI-Dokumenten, kontrollierte Weiterleitung von Dokumenten und Vorgängen

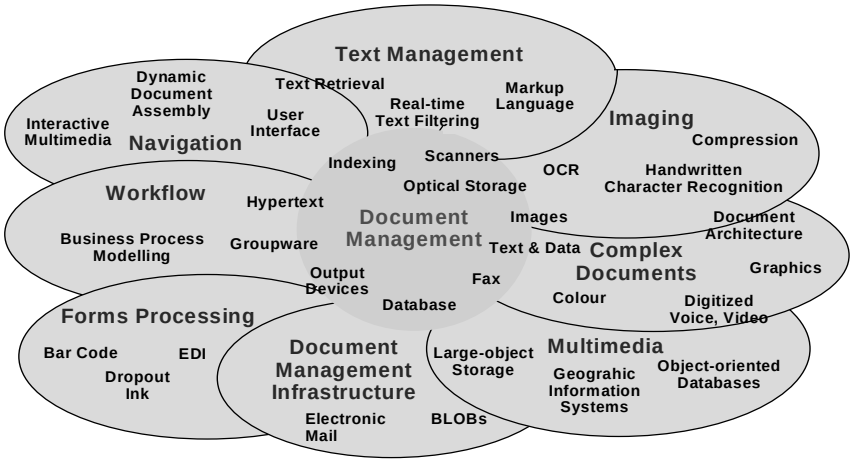



***Abbildung 2 Komponenten des Dokumentenmanagements***

Heute lassen sich sieben Haupttrends im Dokumentenmanagement im weiteren Sinn ausmachen:

- die Rezentralisierung von großen Dokumentenbeständen auf Intranet- und Internet-Sites mit Archiv-„Outsourcing„ und „Pay-per-view„,
- Pattern Recognition zur Erkennung von Zusammenhängen in unstrukturierten Datenbeständen und zur Analyse von Bildinhalten,
- der vollständigen Integration von Dokumentenmanagement in Betriebssysteme und Anwendungslösungen,
- der Konsolidierung der Anbieterlandschaft,
- der Erschließung von neuen Anwendergruppen im Home-, Home-Office- und „Virtual-Company„-Umfeld ,
- der Trennung des Angebots in individuelle „High-end„/„Production„-Lösungen, „Tool-sets„ und „Componentware„ sowie „Low-cost„/„Off-the-shelf„-Produkte – und nicht zuletzt -
- Knowledge Management.

## *Convergence of Technologies*

Einer der erwähnten wichtigen Trends ist das Zusammenwachsen der verschiedenen Dokumentenmanagement-Technologien. Das bedeutet, daß eine Trennung zwischen Workflow, Groupware, Archivierung, klassischem Dokumentenmanagement, COLD-Systemen und anderen Lösungen kaum mehr möglich ist. Künftige Entscheidungskriterien für Produkte orientieren sich nicht mehr an Funktionen, sondern an Schnittstellen, Standards sowie Plattformunabhängigkeit, verteilten Lösungen und Modularität.

Die Broschüren der Anbieter sind inzwischen mit Angeboten zu Modulen, Zusatzfunktionalitäten und Optionen prall gefüllt. Die Unterschiede zwischen den Produkten und Dienstleistungen sind heute kaum mehr greifbar, da sich die Angebote vom Funktionsumfang immer mehr ähneln. Damit werden die Selektion eines Realisierungspartners und dessen Erfahrungen, also „weiche Entscheidungskriterien“, zunehmend wichtiger. Die Zukunftssicherheit, Modularität, Migrationssicherheit und einfache Handhabung der Produkte ist maßgeblich für den langfristigen Erfolg.

Doch warum treiben selbst die Hersteller die Convergence of Technologies voran? Dies hat zwei Gründe:

- Zum einen versuchen die Unternehmen, die solche Lösungen anbieten, um sich natürlich durch neue Funktionalitäten und Erweiterungen vom Wettbewerb abzusetzen. Dieser Trend ist häufig nicht von Anwenderanforderungen bestimmt, sondern dient hauptsächlich Wettbewerbsvorteilen, Unterscheidungsmerkmalen und einer besseren Positionierung von Systemen, die bisher als Einzellösungen in der Landschaft standen.

- Der zweite Grund ist eher anwendergetrieben, das heißt, ➔

← daß die Anwender sich nicht mehr damit zufrieden geben, eine einzelne Lösung neben anderen Fachanwendungsprodukten wie ein Archivsystem mit einem eigenen Klienten zu akzeptieren. Sie erwarten vielmehr, daß diese Funktionalitäten in ihrer Anwendungsumgebung, in der sie täglich arbeiten, zur Verfügung gestellt werden.

Wenn wir also heute von Dokumentenmanagement-Technologien reden, meinen wir weniger die bisherigen Systemlösungen, die für sich ein Archiv- oder Workflowsystem dargestellt haben, sondern Funktionalitäten, die in reinen Fachanwendungen als Hintergrunddienst zur Verfügung gestellt werden.

### *DOMEA : Lösungen für die öffentliche Verwaltung*

Die öffentliche Verwaltung hat unter Federführung der KBSt im Rahmen von DOMEA eine Infrastruktur für Archiv-, Dokumentenmanagement- und Workflow-Lösungen definiert. Wenn wir vor dem zuvor genannten Hintergrund - der Integration von Dokumentenmanagement in Fachanwendungen - das Projekt DOMEA betrachten, so haben diese neuen Anforderungen mehrere Auswirkungen:

- Zum einen wird DOMEA bisher meistens nur technisch gesehen, häufig nur als eine Archiv- oder Workflow-Anwendung verstanden. Die Umsetzung in Fachanwendungen wird diese Betrachtungsweise ändern.

- Zum zweiten hat DOMEA eine sehr starke organisatorische Komponente. Denn die Systemlösungen, die im Laufe des DOMEA-Projekts definiert worden sind und jetzt zum Einsatz kommen, erfordern natürlich eine angepaßte Organisation. Das bedeutet, daß es die Inhalte, Strukturen, Schlüsselsystematiken und andere Merkmale sind, die aus einem Tool erst eine echte Fachanwendung machen.

- Zum dritten – und das ist ein wesentliches Thema meines Vortrags – ist natürlich, das Zusammenwirken dieser Softwarelösungen mit dem Benutzer zu sehen. Häufig gewinnt man doch den Eindruck, besonders bei Mammutprojekten - und DOMEA ist hier keine Ausnahme - daß zwar Organisation und technische Lösungen im Vordergrund stehen, aber daß die Anwender als eigentliche Nutzer dafür mehr und mehr in den Hintergrund treten.

### *Das automatisierte Büro bleibt Fiktion*

Hintergrund der Einführung von Dokumentenmanagement-Technologien ist die lange propagierte Idee des „papierlosen„ oder zumindest des „papierarmen Büros„ gewesen. Man erhoffte sich davon Verbesserungen, analog zur Einführung von Automatisierungsverfahren in Industrieprozessen, um die Arbeit mit Informationen, Dokumenten und Daten einfacher und schneller zu gestalten.

Wir wissen heute, daß das automatisierte Büro weitgehend eine Fiktion ist - insbesondere dann, wenn man Tätigkeiten unterstützen muß, die nicht vorhersehbar sind, die einen stark individuellen Charakter haben, die menschliches Einwirken auf das Ergebnis eines Prozesses notwendig machen. Vielmehr müßte man statt einem automatisierten Büro von Hilfsmitteln sprechen, die den Sachbearbeiter oder anderen Nutzer bei ihrer täglichen Arbeit unterstützen sollen.

Das Risiko solcher Begriffe wie „automatisiertes Büro„ oder „papierarmes Büro„ liegt darin, daß mit diesem Begriff häufig Ängste erzeugt werden - nach dem Motto: „Wozu werde ich als Mitarbeiter eigentlich dann noch gebraucht?„ Zum anderen werden jedoch auch übertriebene Erwartungen erzeugt, nämlich: „Ich kann soviel automatisieren, soviel erleichtern, daß alles wie von selber geht!„ Und zwischen diesen beiden Polen, einerseits der Angst um den Arbeitsplatz und andererseits einer übersteigerten Erwartungshaltung, befindet sich der Anwender heute.

Es ist richtig, daß in Registraturen und Archiven Personal eingespart werden kann. Im Vordergrund steht jedoch immer die Verbesserung der Informationsbereitstellung, die Beschleunigung von Arbeitsprozessen, die Übernahme von unnötigen, durch papiergebundene Organisation bedingten Routinetätigkeiten, die Schaffung von neuen Dienstleistungsangeboten, die Sicherung der Wettbewerbsfähigkeit und damit auch die Sicherung von Arbeitsplätzen.

Bisherige Erfahrungen haben gezeigt, daß zahlreiche Einführungsprojekte auch neue Arbeitsplätze geschaffen haben. Ich glaube außerdem, daß die Unternehmen heute keine Wahl mehr haben, ob sie solche Systeme einführen. In zahlreichen Branchen hängt die Überlebensfähigkeit der Unternehmen vom Einsatz von Archiv- und Workflowlösungen ab. Beispielsweise der gesamte Dienstleistungs- und Servicebereich bei Banken, Versicherungen, Telekommunikationsunternehmen, Handel usw. Es werden hier also eher Arbeitsplätze vernichtet, wenn die neuen Technologien ungenutzt bleiben.

Bestimmte neue Tätigkeitsprofile, neue Geschäfte und neue Dienstleistungen werden durch Technologien wie Workflow und Internet sogar erst möglich. Hier entstehen zahlreiche neuartige Arbeitsplätze, für die wir uns heute noch nicht einmal geeignete Berufsbezeichnungen ausgedacht haben. Bedingt durch den Boom der DMS-Branche werden auch von den Anbietern und Systemintegratoren neue Arbeitsplätze geschaffen. Der Bedarf an →

← qualifizierten System- und Organisationsberatern läßt sich derzeit gar nicht befriedigen. Letztlich sind diese neuen Arbeitsplätze bei den DMS-Anbietern natürlich nicht mit den hohen Arbeitslosenzahlen in Relation zu setzen. Hinsichtlich des Themas „soziale Verantwortung„ sind meines Erachtens aber heute eher die Politik, Verwaltung, Gewerkschaften und Unternehmen gefragt - nicht die vergleichsweise kleine DMS-Branche.

### *Die DMS-Industrie hält ihre Versprechen nicht ein*

In Hochglanzprospekten von Dokumentenmanagement-Herstellern und –dienstleistern wird seit Jahren versprochen, daß die Vision des „papierlosen Büros„ durch den Einsatz von Softwareprodukten wie Workflow, Dokumentenmanagement, elektronische Archivierung heute schon Realität ist. Dabei wird aber vergessen, daß die Anbieter sich häufig auf die reine Funktionalität konzentriert haben und nicht auf das, was die Anwendung im eigentlichen Sinne darstellt:

- Funktionalität heißt beispielsweise, daß ein System Dokumente scannen, indizieren und speichern kann, so daß der Benutzer sie wiederfinden kann.

- Anwendung heißt dagegen, daß bestimmte Indizes vergeben werden, die vorher definiert sein müssen, um wirklich alle Informationen wiederfinden zu können. Es müssen ergonomische Benutzungsoberflächen entwikkelt werden, die dem Anwender überhaupt die Arbeit mit diesem System ermöglichen.

Diese Kluft zwischen reinen Softwaretools und Anforderungen von Organisationen an eine Fachanwendung wurde bisher individuell überbrückt. Das heißt, daß die Tools für verschiedene Anwendungen so konfiguriert, adaptiert oder ergänzt wurden, daß die Fachfunktionalität möglichst vollständig abbildet wird.

Der Nachteil dieser Arbeitsweise ist, daß man jegliche Veränderung der Abläufe und der Organisation ebenfalls wiederum in dieser Software abbilden muß und, daß die Anwender dieser Produkte häufig nicht über das nötige Branchenwissen verfügen, um vorgefertigte Lösungen bereitzustellen.

Der Trend im Markt für Dokumentenmanagement-Lösungen geht dahin, daß die Anbieterschaft sich aufspaltet:

- Der erste Ansatz dabei ist, daß die Hersteller von reinen Produkten – im Server-Bereich „Engines„ genannt, auf dem Clienten „Enabling„ - die Basisfunktionalitäten zur Verfügung stellen.

- Beim zweiten Ansatz erstellen die Integratoren mit Hilfe dieser Produkte Lösungen. Hier wird zunächst immer ein „leeres„ Werkzeug mitgeliefert. Dieses Werkzeug wird durch den Einsatz von Integratoren und Beratern aufwendig mit Struktur und Inhalt und Ordnung gefüllt, bevor es überhaupt zum Einsatz kommen kann.

- Der dritte Ansatzpunkt ist, daß die Systemintegratoren individuelle Lösungen entwickelt haben, die genau auf eine Anwendung oder einen Anwender zugeschnitten sind.

Bei diesen verschiedenen Ansatzpunkten überwiegen heute noch die individuell für eine Branche oder für ein Unternehmen erstellten Lösungen. Erst durch die Standardisierung bei Projekten wie DOMEA wird die Möglichkeit geschaffen, einheitliche Lösungen zu erstellen, die multiplizierbar sind, damit natürlich auch kostengünstiger und einfacher einzuführen.

Wird fortgesetzt. ◆

***Das Bundesministerium für Verkehr, Bau- und Wohnungswesen auf der Datenautobahn***

## Mit elektronischer Aktenführung zu schnellen Entscheidungen

Die elektronische Akte weist den Weg in die Zukunft: Mitarbeiterinnen und Mitarbeiter im Bundesministerium für Verkehr, Bau- und Wohnungswesen (BMVBW) erfahren seit kurzem eine effektive Zusammenarbeit zwischen den Dienststellen in Berlin und Bonn. Möglich wird dies mit Einführung von DORIS, eines auf MIRES basierenden integrierten Dokumentenmanagement-Systems einschließlich einer IT-gestützten Registratur mit vollständiger elektronischer Aktenführung.

Mit einer ausschließlich papiergebundenen Registratur und Vorgangsbearbeitung konnte das Flexibilisierungs- und Rationalisierungspotential der bestehenden IT-Vollausstattung im BMVBW nicht hinreichend genutzt werden. Mit DORIS werden alle Dokumente elektronisch erfaßt, und der Dokumentenzugriff steht ortsungebunden, schnell und effizient im Sinne einer schlanken Verwaltung jedem zugriffsberechtigten Mitarbeiter zur Verfügung.

Grundlage der Planung und Entwicklung von DORIS war das Konzept „Papierarmes Büro„ der Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung (KBSt).

Dieses Konzept war vor dem Hintergrund des Umzugs der Bundesregierung nach Berlin sehr bedeutsam, da Teile der Ministerien in Bonn verblieben sind. Deshalb ist ein →

← benutzerfreundliches System gefragt, das den Transport von Akten und Dokumenten auf ein Minimum reduziert, komfortable Recherchefunktionen bietet und jedem Bearbeiter Volltextsuche ermöglicht. Das Produkt DORIS stand in Bonn und Berlin rechtzeitig vor dem Umzug des BMVBW zur Verfügung.

Damit setzt das BMVBW die Dokumentenmanagement-Lösung DORIS als erstes Bundesministerium standortübergreifend ein.

Mit DORIS wird eine ganzheitliche Bearbeitung von elektronischen Dokumenten und Papierdokumenten ohne Medienbruch angestrebt. Gravierende Nachteile des Mediums Papier, wie fehlende Datensicherheit und eingeschränkter ortsgebundener Zugriff auf einmalig vorhandene Papierdokumente, werden vermieden. Die flexible elektronische Dokumentenbearbeitung hilft, Entscheidungsprozesse zu beschleunigen.

Zur Realisierung von DORIS wurde zunächst eine Projektgruppe in heterogener Zusammensetzung mit Expertenkenntnissen in Sachbearbeitung, Registratur, Organisation und Informationstechnik gebildet. Erste Aufgabe der Projektgruppe war die Spezifikation der organisatorischen, fachlichen und technischen Anforderungen an eine IT-gestützte Dokumentenorganisation im BMVBW. So war z.B. die aufgabenbezogene Neugestaltung der Aktenstruktur unabdingbar. Ebenso waren Neuregelungen im Bereich der Ablauforganisation (Geschäftsgang) erforderlich.

Die DORIS-Konzeption aus dem Jahr 1997 berücksichtigt die seit 1996 von der KBSt entwickelte und im Band 34 der KBSt-Schriftenreihe dokumentierte Konzeption DOMEA „Aufbau eines Pilotsystems für Dokumentenmanagement und elektronische Archivierung im IT-gestützten Geschäftsgang„. Seit 1998 wird das Konzept der KBSt unter dem Namen „Papierarmes Büro„ weiterentwickelt.

Die Arbeiten der Projektgruppe DORIS umfassen die Konzeptmodule „Schriftgutmanagement„ inklusive „Archiv„ und „Dokumentenbearbeitung„. Der Bereich „Vorgangsbearbeitung„ wurde zunächst zurückgestellt und wird zunächst im BMVBW durch Integration des hausweit eingeführten E-Mail-Systems Novell-GroupWise abgebildet. Dies entspricht den Stufen 1 und 2 der von der KBSt empfohlenen Einführungsstrategie (DOMEA-Telegramm 3), erweitert um wesentliche Funktionen zur Weiterleitung der Dokumente im Geschäftsgang per E-Mail sowie zur Dokumentation der Bearbeitungsschritte und -stationen.

Die verschiedenen Mitarbeitergruppen des Ministeriums wurden bereits in der Entwurfsphase einbezogen:

- Die Sachbearbeitung erstellt, bearbeitet Dokumententwürfe und Dokumente, leitet sie weiter und legt sie ab.
- Die Leitungsebene bearbeitet Dokumente im Mitzeichnungs- und Entscheidungsprozeß und leitet sie weiter.
- Der Registratur obliegt die Organisation des Aktenplans und der Ablagestruktur, die Ablage und die Archivierung von Dokumenten.

Das Lösungskonzept wurde bereits in der Entwurfsphase mit der Mitarbeitervertretung (Personalrat) abgestimmt.

Aus strategischen Gesichtspunkten wurde die Entscheidung zum Einsatz des bereits im Ministerium eingeführten Volltextrecherche- und Dokumentenmanagement-Systems MIRES der Firma Haessler frühzeitig getroffen. Dabei stand die Zielsetzung im Vordergrund, eine einheitliche Systemarchitektur für die hausweite Dokumentenablage zu erhalten. An die Firma Haessler wurde der Auftrag erteilt, das Standardprodukt MIRES auf die spezifischen Dokumentenmanagement-Anforderungen des Ministeriums anzupassen. Ergebnis dieser Anpassungen ist das IT-System DORIS.

Ein Prototyp von DORIS wurde bereits zu einem frühen Zeitpunkt im BMVBW eingeführt und einem ausführlichen, mehrmonatigen Test an ca. 50 Arbeitsplätzen unter Praxisbedingungen in verschiedenen Organisationseinheiten in Bonn und Berlin unterzogen.

Nach Auswertung der Testergebnisse und zahlreicher Anregungen der Beteiligten wurde die Weiterentwicklung des Produkts DORIS zur Herstellung des Wirkbetriebs initiiert.

**Welche entscheidenden Vorteile bietet DORIS ?**

DORIS reduziert den Transport von Akten auf ein Minimum und bietet jedem Sachbearbeiter eine komfortable Recherchefunktionen unter Verwendung umfangreicher und kombinierbarer Suchkriterien (inklusive Volltextrecherche). Informationen aus integrierten Quellen wie Fax, E-Mail und Online-Diensten können mitgespeichert und recherchiert werden.

Der Papier-Posteingang wird unmittelbar nach Eingang in der Registratur erfaßt und elektronisch gescannt („frühe Erfassung„). Anschließend wird das Dokument direkt per E-Mail an den Posteingangsempfänger versandt. Es besteht dann ein sofortiger elektronischer Zugriff auf den Posteingang und auf den Aktenbestand.

Die Dokumente werden unmittelbar nach der Speicherung in unterschiedliche Formate gewandelt. So wird z.B. aus einem eingescannten Dokument der Volltext extrahiert. Textdokumente (z.B. aus WinWord) hingegen werden zur Sicherung einer Langzeitarchivierung zusätzlich im Rasterbild-Format (standardisiertes TIF-Format) abgespeichert.

**Erzielter Nutzen:**

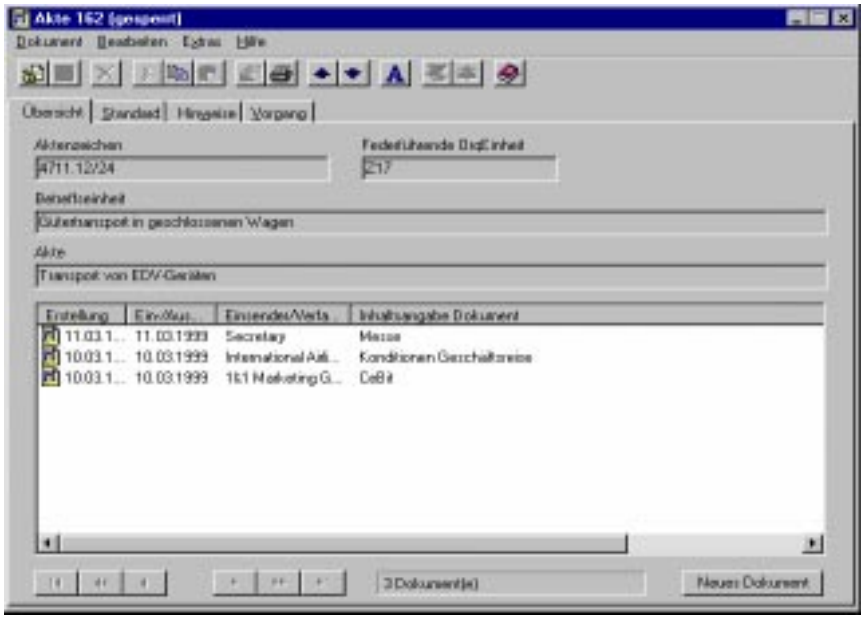
- DORIS reduziert die Transport- und Liegezeiten der Akten, →

➔ was zu massiven Einsparungen in der Bearbeitungszeit führt.

- Die Bearbeiter erhalten direkten Zugriff auf den Posteingang und auf den Aktenbestand. Somit können Wartezeiten vermieden werden.
- Komfortable Suchfunktionen unterstützen bei der Recherche nach Vorgängen. Besonders hilfreich ist die Volltextrecherche.
- Komplexe Recherchen können an ausgebildete Registratoren weitergegeben werden.
- Das Dokumentenmanagement-System erlaubt den Mitarbeitern, elektronische Dokumente selbst zu speichern (z.B. Entwürfe, Vermerke, Internet-Informationen). Eine Abgabe an die Registratur in Papierform ist nicht mehr notwendig.
- Eine klar gegliederte und leicht vermittelbare Benutzeroberläche und Bedienung vereinfacht die Arbeit mit dem System.
- Schutz- und Kontrollmechanismen gewährleisten den Datenschutz.
- Die Portabilität und die leichte Anpassbarkeit von DORIS garantiert niedrige Investitionskosten.




***Die Akten und Dokumente werden mittels eines Aktenplans verwaltet, der auch auf anderen Plattformen oder Datenbanken außerhalb von DORIS angelegt sein kann. Die nachstehende Abbildung zeigt eine „Akte".***



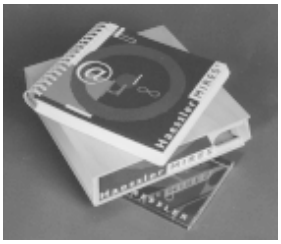

DORIS arbeitet auf Basis von MIRES. Die Grundbausteine von MIRES sind der MIRES Client für die Datenerfassung und Recherchen und der MIRES Server, der die Datenbasis bereitstellt.

DORIS ist modular aufgebaut und kann den Bedürfnissen entsprechend individuell zusammengestellt werden. Es kann in vorhandene Systeme integriert werden, besitzt Schnittstellen zu allen gängigen Standard-Dokumenten und ist plattformübergreifend verfügbar (auf UNIX und NT).

Die ersten Erfahrungen im BMVBW lassen erkennen, daß beim Einsatz von DORIS - gerade in verteilten Organisationen - erhebliche Effizienzsteigerungen erzielbar sind. Die vielseitigen Recherchemöglichkeiten im Schriftgut finden hohe Akzeptanz. Damit kann eine ganzheitliche Bearbeitung, unabhängig von der Verfügbarkeit der Papierdokumente in der Registratur, erreicht werden.

Die Überführung der bestehenden Testarbeitsplätze in den Wirkbetrieb ist abgeschlossen. Die Anzahl der in den Wirkbetrieb einbezogenen Arbeitsplätze wird sukzessive erhöht. Alle von der Bonn-Berlin-Aufteilung besonders betroffenen Organisationseinheiten sollen schnellstmöglich einbezogen werden.

Das Projektteam im BMVBW ermutigt auch andere Ministerial- und Verwaltungsbehörden, sich mit der Thematik intensiv auseinanderzusetzen, und steht diesbezüglich für einen Erfahrungsaustausch oder weiterführende Kooperation zur Verfügung.



Weitere Informationen: HAESSLER INFORMATION GmbH, Mühlstrasse 58, 75328 Schömberg, Telefon: 72 35 97 09 0, Fax: 72 35 97 09 80, Internet: http://www.haesseler.com/ ◆

# Neues aus dem Hause Microsoft

### *Windows 98: Zweite Ausgabe liegt vor*

Der „Nachfolger“ von Windows 98 bringt das Betriebssystem auf den jüngsten Stand der PC-Technik. Die Zweite Ausgabe bringt mehr Bedienerkomfort, nützliche Systemerweiterungen, schnellere und einfachere Installation von USB-Geräten und noch mehr Internet-Integration. Damit ist laut Microsoft Windows 98 zuverlässiger und schneller geworden und benötigt noch weniger Einarbeitungszeit als sein Vorgänger.

Im Vordergrund steht der Internet Explorer 5.0, der sich nun durch bessere Geschwindigkeit, Benutzerfreundlichkeit und Flexibilität auszeichnet. Darüber hinaus erlaubt das Internet Connection Sharing (ICS) das gleichzeitige Nutzen einer Internet-Verbindung (z.B. ein ISDN-Zugang zu einem Provider) von mehreren über ein LAN verbundenen PCs. Auf diese Weise lassen sich Kleinst-Netze wie in Agenturen, Arztpraxen oder auch im Heimbereich kostengünstig an das Internet anschließen. Interessant für Spiele-Freaks dürfte sein, dass ICS die Beteiligung mehrerer Spieler aus einem Heimnetzwerk an einem Online-Spiel - und dies bei nur einer Internetverbindung ermöglicht.

Für den Gedankenaustausch mit Kunden, Kollegen oder Freunden steht Windows NetMeeting 3.0 bereit. „Bild im Bild“-Funktion, 24 Bit Echtfarben sowie Internet-Telefonie in hoher Sprachqualität prädestinieren diese Anwendung für jede Art von Kommunikation.

Selbstverständlich wartet Windows 98 Zweite Ausgabe mit einer im Vergleich zur Vorgängerversion erweiterten Hardware-Unterstützung auf. Diese betreffen unter anderem den Wechsel eines Geräts im laufenden Betrieb (z.B. bei einer Universal Serial Bus-Komponente oder einem Device Bay-Modul wie einem DVD-Laufwerk). Anwender von Bildschnittsystemen profitieren von den hohen Datentransferraten über den IEEE 1394-(„FireWire“-) Bus – so lassen sich die großen Datenmengen von Multimedia bewältigen. Die zweite Ausgabe ist voll kompatibel zu Intel Pentium III Prozessoren und unterstützt erweiterte 3D- und Video-Funktionen.

Notebook-Besitzer können sich über eine erweiterte ACPI-Implementation freuen, die ein genaues Abstimmen von Stromsparfunktionen auf die Fähigkeiten des Geräts und die Erfordernisse des Anwenders gestattet.

Nicht zuletzt enthält Windows 98 Zweite Ausgabe das Windows 98 Service Pack. Dieses auch separat seitens Microsoft kostenfrei über das Internet abrufbare Service Pack enthält unter anderem optimierte Funktionen im Hinblick auf das Jahr 2000 sowie nützliche Systemerweiterungen.

Windows 98 Zweite Ausgabe ist im Handel erhältlich. Das Vollprodukt kostet zirka 400 Mark, ein Update von Windows 95 oder früheren Windows-Versionen rund 200 Mark. Windows 98 Zweite Ausgabe wird bei neuen PC bereits von vielen Herstellern vorinstalliert und löst darüber hinaus das bisherige Windows 98 in den Regalen des Fachhandels ab.

Kunden, die bereits den Vorgänger Windows 98 besitzen, können die Zweite Ausgabe mittels einer über Microsoft Direkt (Tel.: 0180 / 525 11 99, Fax: 0180/ 525 11 91) beziehbaren Windows 98 Zweite Ausgabe Updates CD für 24 Euro (DM 46,94) nachrüsten. Diese kann auch online bestellt werden über: http://www.microsoft.com/germany/windows98

### *Kreative Fotowerkstatt*

Mit der neuen Version des erfolgreichen Bildbearbeitungsprogramms hat Microsoft zusätzliche Funktionen eingebaut. Picture It! 2000 macht aus unterbelichteten Schnappschüssen klare Bilder in guter Qualität. Das Programm zeichnet sich durch einfache Bedienung dank intelligenten Werkzeugen und Bildbearbeitungsmöglichkeiten wie dem Verfremden aus.

Oft bedauert der Amateur-Fotograf rote Augen, unbekannte Menschen, Grünstiche oder triste Hintergründe auf seinen Schnappschüssen. Picture It! 2000 behebt diese Schönheitsfehler, bastelt Collagen, entfernt Falten und verschönert Körper. Darüber hinaus kann der Anwender Einladungen entwerfen und Motive verzerren.

Die vierte Version von Picture It! 2000 bietet eine Palette neuer Möglichkeiten, die die Bildbearbeitung am PC zu Hause schneller, leichter und effektvoller machen. Eine Neuerung sind die Toolbars, die um nützliche Befehle erweitert wurden. Von nun an ist es möglich, eine Mehrfachauswahl an Anweisungen zu geben und damit viele Arbeitsprozesse zu beschleunigen. Befehle wie „Rückgängig„ und „Wiederherstellen„ ermöglichen es, einzelne Schritte zu verfolgen.

Die grosse Auswahl an Vorlagen stellt eine Reihe von ClipArts, Hintergründen, Fotoecken und Webvorlagen zur Verfügung. Der Benutzer erstellt damit seine eigenen Fotogrußkarten, Bildschirmschoner, Fotoalben, Zertifikate oder Diashows. Er veröffentlicht seine Bilder mit Hilfe des Web-Assistenten einfach im Internet oder frischt seine Homepage mit eigenen Fotoanimationen und Daumenkino-Effekten auf.

Die Lieblingsaufnahme kann zu Hause ausgedruckt werden oder der Anwender nutzt die Dienste von Fotofachfirmen wie Fuji. So erhält er eine optimale Ausbelichtung seines Fotos. ➔

← Zusätzliche Hardware ist nicht nötig. Die Fotos werden direkt von einer digitalen Kamera, dem Scanner oder aus dem Internet heruntergeladen, oder die Labors entwickeln die Fotos auf CD-ROM. Die neue Version von Picture It! 2000 ermöglicht beidseitiges Drucken, was sich für Einladungen und Karten besonders gut eignet.

Das Minilabor von Picture It! 2000 verbessert mehrere Fotos gleichzeitig. Einzelne Bildteile können ausgeschnitten, gedreht und der Helligkeit, dem Kontrast und Farbstich angepasst werden. Risse und Löcher werden retuschiert und ausgefüllt. Die Archivierung gestaltet sich ebenso einfach. Der Anwender katalogisiert seine Bilder nach Datum, Namen oder Untertitel.

Das aktualisierte und erweiterte Picture It! 2000 bietet eine große Auswahl an Nachbearbeitungsmöglichkeiten. Eine „Rote-Augen-Korrektur„ entfernt den unerwünschten Effekt. Kratzer, Staub oder unbekannte Personen werden aus den Bildern retuschiert.

Das Highlight von Picture It! 2000 mit dem zugleich größten Spassfaktor ist das Verfremden. Der Anwender tauscht seinen Kopf oder Körper mit denen der Stars und Publikumslieblinge. Der Falten-Entferner glättet Falten und verjüngt auf Mausklick.

Eigene Briefmarken können erstellt und Bilder mit Farbe dekoriert werden. Der Benutzer kann seine Unterschrift unter besonders gelungene Aufnahmen setzen und mit Pinsel-Funktionen überraschende Effekte zaubern. Kunstliebhaber verwandeln ihre Fotos in impressionistische Bilder, Aquarelle oder Mosaike. Intelligente Werkzeuge weisen den Weg zu jedem Spezialeffekt. Visuelle Menüs erleichtern es Anfängern und Spezialisten, ihrer Kreativität freien Lauf zu lassen.

**Systemanforderungen:** Windows 95, Windows 98, Windows NT Workstation Version 4.0, Service Pack oder höher. Multimedia-PC mit 166 MHz-Pentium- oder höher Prozessor 32 MB RAM, SVGA-Grafikkarte, 1MB VRAM Quatro-Speed CD-ROM-Laufwerk oder schneller 270 MB freier Festplattenspeicher, Microsoft Mouse oder kompatibles Zeigegerät, Microsoft Internet Explorer 5.0 (auf der CD enthalten) oder höher. Nach der Installation kann der Benutzer seinen Standardbrowser weiterverwenden. Optional: Soundkarte mit Kopfhörer oder Lautsprecher, Internetzugang mit MAPI-fähigem Email-Client

Microsoft Picture It! 2000 ist ab Oktober 1999 zum Preis von 99 Mark im Fachhandel erhältlich.

## *Microsoft nimmt europäisches Jahr-2000-Informationszentrum in Betrieb*

Im Juli 1999 kündigten Microsoft Europa, Middle East und Africa (EMEA) die Eröffnung ihres Jahr-2000-Informationszentrums an. Damit will sich Microsoft für Kunden als Ansprechpartner zur Verfügung stellen, die sich über die Jahr-2000-Computerumstellung im Zusammenhang mit Microsoft-Produkten Gedanken machen. Dieses Engagement, das dem Informationsbedürfnis von Verbrauchern sowie kleinen und mittleren Unternehmen ohne Internetzugang nachkommt, ist bislang einzigartig in Europa. Das neue Informationszentrum ergänzt mit seinem für Anrufer aus ganz Europa kostenlosen Jahr-2000-Produkt-Informationsservice (Ressource CD) das bereits bestehende, Web-basierende Serviceangebot von Microsoft. Das Informationszentrum ist von Montag bis Freitag von 9:00 bis 18:00 Uhr geöffnet.

Mit der heutigen, offiziellen Eröffnung steht der kostenlose Informationsservice europaweit in den Sprachen Deutsch, Französisch und Englisch zur Verfügung. Schritt für Schritt werden die Services ausgebaut, bis die meisten Sprachen Europas und des mittleren Ostens abgedeckt werden können. Ab sofort können damit folgende Leistungen in Anspruch genommen werden:

- Teilnahme an einem kostenlosen CD-ROM Subskriptions-Programm
- Informationen über die Jahr-2000-Fähigkeit von Microsoft-Produkten per Fax oder Briefpost
- Informationen über andere nützliche Services, wie zum Beispiel Microsoft Kundenservice-Nummern und lokale Produkt-Support Dienstleistungen

Nach der Anmeldung für das Subskriptions-Programm bekommt der Anrufer regelmäßig die neuesten Produktinformationen und Werkzeuge auf einer CD-ROM zugeschickt. Diese enthält Informationen, wie sich Kunden auf verschiedenste Aspekte der Jahr-2000-Computerproblematik einstellen können, wie zum Beispiel Hardware, Betriebssysteme, Anwendungsprogramme, Dokumente, Individualprogramme und deren Schnittstellen zu den Daten. Als Teil der Subskription erhält der Anwender die neuesten Software-Upgrades zu Microsoft Produkten mit bekannten Jahr-2000-Problemen und eine ausführliche Dokumentation zur Installation dieser Komponenten.

„Mit diesem Service reagieren wir auf einen dramatisch wachsenden Informationsbedarf von Privatkunden und kleinen und mittleren Unternehmen. Für die etwa 70 Prozent der Kunden in Europa, im mittleren Osten und in Afrika, die keinen Zugang zum Internet besitzen, ist dieser Dienst von unschätzbarem Wert. Wir sind davon überzeugt, mit dieser Art von Kundenservice in der Softwareindustrie einen neuen Maßstab gesetzt zu haben“, so Michel Lacombe, Präsident von Microsoft EMEA.

Diese Kampagne wird auch von Empfehlungen der Europäischen Kommision getragen, die in ihrem Bericht „How the European Union is tackling the Year 2000 →

← Computer problem“ zu „...weiterführenden Maßnahmen aller beteiligten Bereiche zur Informationsbereitstellung ... und zur Offenlegung von Informationen über die Jahr-2000-Fähigkeit von Produkten und Dienstleistungen...“ ermuntert. „Informationszentrum und Produkt Support Service werden solange aufrechterhalten, solange unsere Kunden dies brauchen“, so Lacombe weiter. „Wir werden regelmäßig den Grad der Kundenzufriedenheit messen, um sicherzustellen, daß dieser Dienst die Erwartungen auch weiterhin erfüllt.“

In den vergangenen 18 Monaten hat Microsoft 2.054 seiner Produkte im Hinblick auf die Jahr-2000-Compliance evaluiert und über 93 Prozent für bereit befunden, fehlerfrei beim Kunden zu funktionieren.

Die Nummer des Microsoft Jahr-2000-Informationszentrums ist:

0800 - 183 36 54

Informationen zur Jahr-2000-Fähigkeit von Microsoft-Produkten gibt es auch unter http://www.eu.microsoft.com/year2000 und in deutscher Sprache unter http://www.eu.microsoft.com/germany/jahr2000 ◆

## Sicherheitslücken bei der Jahr-2000-Umstellung

Der AXENT Enterprise Security Manager (ESM) schließt Lücken, die bei der Jahr-2000-Umstellung (Y2K) in internen Netzen entstehen können. Die Sicherheitsmanagement-Lösung überprüft Unternehmensnetze beliebiger Größe laufend nach potentiellen Risiken, selbst wenn zehntausende von Einzelsystemen daran angeschlossen sind. Der Einsatz des ESM garantiert, dass die vorhandenen Sicherheitsanforderungen während des Umstellungsprozesses ebenso erfüllt werden wie nach Abschluss der Y2K-Maßnahmen. Die Verbindung zum Internet muss dabei nicht unterbrochen werden – die Integrität sensibler Daten bleibt trotzdem vollständig gewahrt.

Eine noch unveröffentlichte Studie der Gartner Group geht davon aus, dass Schwierigkeiten bei der Y2K-Systemumstellung den massivsten Datendiebstahl in der Computergeschichte zur Folge haben werden – der Verlust wird mehr als eine Milliarde US Dollar betragen. Wenn Mitarbeiter ihre Systeme upgraden, können dabei unabsichtlich Lücken entstehen: Das erlaubt Hackern oder nicht autorisierten internen Anwendern, unternehmenskritische e-Business-Transaktionen zu stören oder zu manipulieren. Vielfach werden Systeme auch während der Umstellungsphase komplett „eingefroren“. Dabei ist nicht immer gewährleistet, dass alle installierten Sicherheitskomponenten bei der Wiederinbetriebnahme auf dem neuesten Stand sind.

Das enorme Ausmaß der Jahr-2000-Umstellungen zwingt Unternehmen dazu, nach dem Upgrade jedes einzelne System auf sicherheitsrelevante Mängel hin zu überprüfen.

„Angesichts der enormen Umstellungsmaßnahmen, die in kürzester Zeit umgesetzt werden müssen, kann es leicht passieren, dass ein IT-Verantwortlicher die Installation des allerneuesten Security Patch verpasst. In manchen Fällen wird auch absichtlich ein ‚Hintertürchen‘ zum Netz offen gehalten, beispielsweise zur Feinabstimmung der Upgrades - auch dadurch kann sich jemand einen unerlaubten Zugriff verschaffen“, erklärt Tami Stein, Produktmanager bei AXENT. „Mit jedem Upgrade für Software oder Hardware - vor allem bei so massiven Eingriffen wie bei der Jahr-2000-Umstellung - müssen Unternehmen laufend prüfen, ob ihre neue Infrastruktur noch den vorhandenen Sicherheitsanforderungen entspricht. Potentielle Bedrohungen für sensible Daten im Netz müssen schnellstmöglich erkannt und bekämpft werden, besonders wenn viele Einzelsysteme mit dem offenen Internet verbunden sind.“

Weltweit profitieren AXENT-Kunden vom Enterprise Security Manager (ESM): Die Sicherheitsmanagement-Lösung überwacht die Netzwerksicherheit und managt die installierten Schutzmaßnahmen im gesamten Unternehmen automatisch, einschließlich aller Workstations, Server und anderen Schlüsselkomponenten für den Zugang zum Internet – selbst wenn zehntausende von Einzelsystemen an das Netzwerk angeschlossen sind. ESM ist die erste Sicherheitsmanagement-Lösung mit einer zentralen Managementkonsole und umfangreichen Reporting-Funktionen.

AXENT empfiehlt Unternehmen dringend, die Jahr-2000-Umstellungen ihrer Systeme mit Sicherheitsmanagement zu verbinden. Nur so lassen sich alle Systeme schützen, die aufgrund ihrer direkten Verbindung zum Internet besonders gefährdet sind.

In Kombination mit einer stringenten Security Policy ist ESM das ideale Werkzeug, um sicherzustellen, dass anfällige Systeme während des Upgrades oder beim „Einfrieren“ keinen unkontrollierten Bedrohungen ausgesetzt werden.

Die größten Sicherheitsrisiken im Zusammenhang mit Y2K-Umstellungen sind laut AXENT: fehlende Security Patches im Betriebssystem, nicht korrekt installierte Applikationen, die „Hintertüren“ offen lassen, nicht passende Dateischutzmechanismen, schlecht konfigurierte Netzwerkeinstellungen sowie durch Y2K-Spezialisten hinterlassene Sicherheitslücken wie leicht durchschaubare Passwörter, temporäre Accounts oder Administratorrechte, die nach Abschluss der Umstellungsmaßnahmen nicht gelöscht werden.

Weitere Informationen: E-Mail info@axent.com oder im Internet unter http://www.axent.com/ . ◆

SIEMENS

Siemens Business Services: Wir verbessern durch den Einsatz neuester Informations- und Kommunikationstechnik die Prozesse unserer Kunden und Partner in der öffentlichen Verwaltung. Wir sind Ihr Lösungs- und Dienstleistungsanbieter. Wir beraten, realisieren, trainieren, betreiben - zu Ihrem Nutzen auch als Generalunternehmer.

Geschäftsgebiet Öffentliche Auftraggeber Berlin
Rufen Sie uns einfach an: 030 / 386-27471



# Kurzmeldungen

### *Novedia wird AG*



Das junge Berliner Software- und Systemhaus wurde in eine AG umgewandeit. Dieser Schritt ist die logische Folge einer rasanten Unternehmensentwickiung und bildet die strukturellen Rahmenbedingungen für ein anhaltend starkes Wachstum. Novedia wurde 1997 von Absolventen der TU Berlin gegründet. Das Unternehmen beschäftigt derzeit 50 Mitarbeiter, die im Zuge der Umwandlung am Unternehmen beteiligt werden. Der Umsatz betrugt 1998 rund 4 Millionen Mark, für 1999 wird mindestens eine Umsatzverdoppelung erwartet. Dabei wurden ohne nennenswerte Fremdfinanzierung immer Gewinne erwirtschaftet. Das Unternehmen ist ausschließlich im Business-to-Business-Bereich tätig, wo es sich auf Großkunden konzentriert. Novedia entwickelt kundenspezifische Intra-/Extranet-Lösungen, ist Entwicklungspartner für Telekommunikations-Systeme (Network Management, Intelligent Network) und bietet Consulting in den Bereichen Netzkonzeption und Netzadministration. Durch das junge Team - das durchschnittsalter beträgt 28 Jahre - und den engen Kontakt zu Lehr- und Forschungseinrichtungen wird eine frühe Adaption neuer Technologien sichergestellt. Novedia ist im Web unter http://www.novedia.de/ präsent. ◆

### *Die besten Bildbearbeitungsprogramme für unter 350 Mark*

Digitale Kameras und Bildbearbeitungssoftware ersetzen immer stärker herkömmliche Fotolabors. Die Software macht das Ausbügeln von Fehler in den Fotos so einfach, dass auch Heimanwender schnell zurecht kommen. In einem Test hat das Einsteigermagazin Computer easy acht aktuelle Programme bis 350 Mark unter die Lupe genommen. Testsieger wurde das 350 Mark teure Programm Photo Impact 4.2 von Ulead. Es überzeugte durch den größten Funktionsumfang, die komfortablen Korrekturfunktionen und seine einfache Bedienung. Zum Preis-Leistungs-Sieger wurde das 80 Mark teure Picture-It 99 von Microsoft gekürt, an dem die Tester die vorbildliche Benutzerführung loben. ◆

### *Linux für Einsteiger*

Linux steht immer noch als Synonym für komplizierte Tastaturbefehle und eine aufwendige Installation. Aber nicht mehr lange: Die Distribution »Easy Linux« der Konstanzer Firma EIT bringt das komplexe Betriebssystem ebenso einfach auf die Platte wie man das von Microsoft Windows gewohnt ist – so die Computerzeitschrift PC-ONLiNE über das 90 Mark teure Easy Linux. Nach der Installation landet man direkt in der grafischen Oberfläche K-Desktop und kann dann mit Hilfe von Assistenten die Konfiguration abschließen. Mit dem Star Office 5 ist auch ein Büropaket für den Privatanwender im Lieferumfang enthalten. ◆

### *Y2K: Verschiebung aus Haushaltsgründen*

"Schließlich wird **mit der Umstellung auf Windows NT** auch **die Jahr-2000-Problematik** in Teilbereichen **gelöst** werden können, da das neue Betriebssystem die Jahreszahl 2000 (und folgende) bereits beinhaltet und entsprechende Prozesse problemlos verarbeitet.

Die Umstellung auf Windows NT vollzieht sich in der Landesverwaltung einerseits anhand des Grades fachlicher Unabweisbarkeit ... und andererseits **mit Blick auf die angespannte Haushaltslage** des Landes, die ein schrittweises Vorgehen unumgänglich macht. Gleichwohl soll die Umstellung **bis zum Jahr 2002** im wesentlichen **abgeschlossen** sein" (Zitat aus dem IT-Gesamtplan eines Bundeslandes) ◆

### *K7 läuft Pentium III davon*

Ein Wettrennen besonderer Art veranstaltete die Computerzeitschrift CHIP. Der neue Prozessor Athlon (K7) von AMD trat gegen den schnellsten Intel-Chip an. Und der K7 übertrumpfte seinen Pentium-III/600 Konkurrenten deutlich. Vor allem bei grafikintensiven Anwendungen und modernen Spielen ist der K7 rund 30% schneller, aber auch andere Anwendungen profitieren von der neuen AMD-CPU.

Da sich laut CHIP die nächste Intel-CPU-Generation weiter verspätet, hat AMD mit den K7-Chips aus Dresden gute Chancen. ◆

# Amt für Logistik und Informationstechnik im BA Lichtenberg 1998



Am 01.08.1997 wurde das Amt für Logistik und Informationstechnik gebildet. Das Amt umfasst die Bereiche Einkauf-Service, Transport- und Kopierservice sowie den IT-Service.

Ziel des Amtes war die konsequente kundenorientierte Ausrichtung auf Basis der weitgehenden Fach- und Ressourcenverantwortung. In diesem Zusammenhang wurde dem Amt für Logistik und Informationstechnik Auftragswirtschaft für 51 Kapitel des Bezirksplanes Lichtenberg erteilt. Das Amt für Logistik und Informationstechnik bewirtschaftet neben 29 eigenen Ausgabetiteln 275 Ausgabetitel anderer Kapitel in Auftragswirtschaft.
...

Zu Beginn des Jahres stand der IT-Service vor einer Vielzahl von Aufgaben. Es galt, schnell ein Konzept zu entwickeln und umzusetzen, welches den Betrieb des vorhandenen Daten- und Telekommunikationsnetzes unter den gegebenen Bedingungen sicherstellt und gleichzeitig dringend ➔

← notwendige Maßnahmen für die Fortentwicklung und den Ausbau der daten- und telekommunikationstechnischen Infrastruktur im Bezirk vorantreibt. Nur unter diesen Voraussetzungen ist die eigentliche Aufgabenstellung, einen leistungsfähigen und umfassenden Service für Telefon und Computer allen Mitarbeitern des Bezirksamtes anzubieten, realisierbar.

Der Ausstattungsgrad aller Abteilungen mit Arbeitsplatzcomputern (APC) hat sich 1998 weiter verbessert, derzeit werden 867 PC-Gerätekonfigurationen im Bezirk betrieben. In den Bereichen BVV und Bezirksbürgermeister sowie den Abteilungen Bau- und Wohnungswesen und Wirtschaft, Umwelt, Bürgerdienste ist inzwischen der Bedarf an PC-Arbeitsstationen gedeckt. Nachholbedarf besteht dagegen nach wie vor in den Abt. Jugend und Bildung (Versorgungsgrad 84 %) bzw. Gesundheit und Soziales (60 %).

Die Anzahl der Erstausstattung von Arbeitsplätzen ist nunmehr insgesamt rückläufig, dagegen nimmt der Aufwand für den notwendigen Austausch veralteter PC-Gerätekonfigurationen und Systemsoftware zu. Verantwortlich dafür sind nicht nur die geltenden und in vielen Fällen überschrittenen Betriebs- oder Abschreibungsfristen oder die nach wie vor hohen Innovationszyklen, zusätzlicher Handlungsbedarf entsteht im Zusammenhang mit der Jahrtausendwende, der Euro-Einführung, aber auch aufgrund von Strukturveränderungen (bspw. Bezirksfusion).

Da ein effizienter Einsatz von IuK-Technik erst in Verbindung mit einem leistungsfähigen Datennetz und modernen Fachanwendungen zu erreichen ist, lagen weitere wichtige Aufgabenstellungen des IT-Services im Ausbau und Aufbau einer einheitlichen Netzinfrastruktur im Bezirk, in der Einbindung der APCs in das Netz, der Einführung von neuen Fachanwendungen und Verwaltungsverfahren in den Fachämtern sowie das Bereitstellen von mehr Funktionalität, Leistung und Service für IT-Anwender.

Für die Entwicklung der Netzinfrastruktur wurden nach einer entsprechenden Analyse und Schwerpunktsetzung, Planungsunterlagen und Projekte initiiert bzw. in eigener Regie realisiert. Zielstellung war und ist ein modernes wirtschaftliches Daten- und Telekommunikationsnetz, welches den hohen Anforderungen der Zukunft gewachsen ist und sich harmonisch in die IT-Landschaft des Landes Berlin einpasst.

Eine Vielzahl von Infrastruktureinführungsmaßnahmen für das Kommunikationsnetz des Bezirkes konnten im letzten Jahr realisiert werden. Standorte wie die Frankfurter Allee 187, Möllendorffstraße 6 und 53 oder Magdalenenstraße 17 - 19 wurden mit moderner, leistungsfähiger Übertragungstechnik für Kommunikationsnetze ausgestattet, weitere Standorte wurden informationstechnisch erschlossen und die Leistungsfähigkeit der wichtigsten MAN-Zugänge erhöht. Mit der neuen Technik können nun zusätzliche Dienstmerkmale und Funktionalitäten dem IT-Anwender zur Verfügung gestellt werden. So wurden mit der Inbetriebnahme eines zentralen E-Mail-Servers eines PC-Faxservers neue Kommunikationsmöglichkeiten erschlossen. Die Inbetriebnahme des Lichtenberger Intranetservers, der neben einem stets aktuellen Telefonverzeichnis, schnellen Zugriff auf umfassende Informationen und Daten des Bezirkes sowie anderer Verwaltungseinheiten, Lehreinrichtungen oder politischer Institutionen des Landes Berlin ermöglicht. Für Spezielle Fachanforderungen wurde weiterhin ein gesicherter Zugang zum Internet realisiert.

Mit der Inbetriebnahme eines zentralen Datensicherungssystems (Backupserver), der Realisierung eines zentralen Virenschutzes auf den Kommunikationsservern und die Installation von Virenschutzsoftware auf potentiell gefährdeten Rechnern, wurden neben administrativen Maßnahmen wie das Erarbeiten einer Virenschutz- und PC-Onlinerichtlinie für Anwender erste dringend erforderliche Schritte zur Durchsetzung einer hohen Daten- und Betriebssicherheit im Netzverbund durchgeführt. Größtes Hemmnis für eine planmäßige Fortführung der dringend erforderlichen Maßnahmen sind die nur begrenzt zur Verfügung stehenden finanziellen Mittel.

Auch das Telekommunikationsnetz wurde weiter ausgebaut. Der Telefonanlagenverbund des Bezirksamtes wurde um mehrere Anlagenteile erweitert, neue Anlagen wurden in Betrieb genommen, zu einem Netzverbund zusammengeschlossen und die Jahr 2000-Fähigkeit hergestellt. Zusätzlich in den Anlagenverbund integrierte D1- und D2-Koppelmodule zum Mobilfunknetz erhöhen die Funktionalität. Dadurch wurden Gebühreneinsparungen von bis zu 150 % erzielt. Auch bei den Fernmeldegebühren im Festnetz konnten durch geeignete administrative und infrastrukturelle Maßnahmen, wie die Aufnahme des Querleitungsbetriebes über das Landesnetz, Modernisierungen (ISDN) oder durch Inanspruchnahme günstigerer Tarifanbieter (Call by Call) Einsparungen für das Bezirksamt im vergangenen Jahr von insgesamt rund 160.000 DM realisiert werden.

Im Bereich der Infrastrukturbetreuung galt es im vergangenen Jahr wieder verstärkt, aktive Unterstützung bei der Einführung neuer DV-Fachverfahren bzw. der Implementierung neuer Anwendungsmodule in vorhandene Verfahren (Profiskal, BO) zu leisten. Mit Unterstützung des IT-Services wurden so unter anderem das Verfahren Diwo 96 im Wohnungsamt, die Liegenschaftsmanagementanwendung „Kolibri“ im Grundstücksamt, FIS/ALK-Anwendungen im Stadtplanungsamt oder GAIA im Naturschutz- und Grünflächenamt neu eingeführt. Für weitere Großverfahren wie IPV, Basis, Wahlen und EWW-neu wurden Vorbereitungen getroffen bzw. Teil- und Testinstallationen durchgeführt.

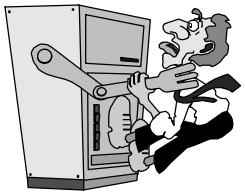
Insgesamt betreuen die Mitarbeiter der IT-Stelle derzeit rund 30 zentrale →

← und dezentrale Serverkonfigurationen für Datenbanken, Anwendungen und Kommunikation. Wichtigste Aufgabe ist neben der Gewährleistung einer hohen Betriebs- und Ausfallsicherheit dieser Systeme die weitere NT-Migration der APC in den Netzverbund. Die entsprechenden technischen und strukturellen Voraussetzungen wurden an den wichtigsten Dienst- und Bürogebäudestandorten geschaffen: technisches Know-how, Fachkompetenz und praktische Erfahrungen im IT-Service wurden aufgebaut. Derzeit sind erst rund 100 PC's in das Kommunikationsnetz eingebunden, für das laufende Jahr wurden aber schon viele Fortsetzungsprojekte vereinbart.

Bei der Benutzerbetreuung wurde im vergangenen Jahr verstärkt Wert auf einen kundenfreundlichen, schnellen und leistungsfähigen IT-Service gelegt. Immerhin sind überschläglich mindestens 1.000 IT-Anwender zu beraten. So können zum Beispiel alle NT-Arbeitsplatzrechner im Netzverbund zentral von einem Servicecomputer der IT-Stelle gewartet, Störungen analysiert, Maßnahmen zur Fehlerbeseitigung eingeleitet der notwendige Softwareupdates verteilt und eingespielt werden, ohne dass wie bisher ein Mitarbeiter der IT-Stelle sich zum betreffenden Standort begeben muss. Auch die Ferninstallation und Konfigurierung neuer APCs sind möglich.

(Aus: Jahresbericht 1998 des Bezirksamtes Lichtenberg von Berlin, Seite 86-88) ◆

**PROBLEME ?**



Rufen Sie an :

HOTLINE

USER HELP DESK

90 12 (912) 70 22

## Stadtpläne online

Für den nächsten Besuch in einer deutschen Großstadt können Internet-User häufig auf die Anschaffung eines gedruckten Stadtplans verzichten: Wie die Computerzeitschrift PC-ONLiNE berichtet, steht unter www.stadtplandienst.de aktuelles Kartenmaterial für Berlin, Hamburg, München und Düsseldorf zur Verfügung. Ein großes Plus ist die Standort-Suche: Statt eine Straße mühsam per Koordinaten zu lokalisieren, findet man sie schnell über die Suchfunktion. ◆




## Kurz-Info zum Intranet-Angebot der Senatsverwaltung für Inneres

Das Zentrale IT-Management stellt nunmehr auch Informationen der AG "IT-Dienstleistungen" bereit. Diese Arbeitsgruppe beschäftigt sich mit Konzepten zur Vergabe von IT-Dienstleistungen an Externe und den LIT; die IT-Stellen der Verwaltung sollen durch die Auslagerung geeigneter Aufgaben entlastet werden. Es bestehen enge Kontakte zum Bundesland Baden-Württemberg, wo diese Idee bereits erfolgreich umgesetzt wurde. Den dort geschlossenen Rahmenvertrag haben wir ebenfalls bereitgestellt.

Die Informationen zum IT-Koordinierungsausschuss für Berlin (IT-KAB) werden noch überarbeitet; wir planen, ca. ab Oktober 1999 weitere Gremien, wie z.B. die AG "Verfahrensübergreifende IT-Koordination" (AG VITKo), in das Intranet aufzunehmen, so dass auch die dort angesprochenen Themenbereiche allen Mitarbeitern zur Kenntnis gelangen.

Wir möchten Sie bei dieser Gelegenheit herzlichst um ein Feedback zu unserem Angebot bitten; auch wenn sich evtl. nicht alle Wünsche umsetzen lassen, →

← würden wir uns über Anregungen und Kritik sehr freuen. Sobald alle organisatorischen und technischen Hürden beseitigt sind, werden wir die interessantesten Informationen auch im Internet unter *http://www.berlin.de* bereitstellen.

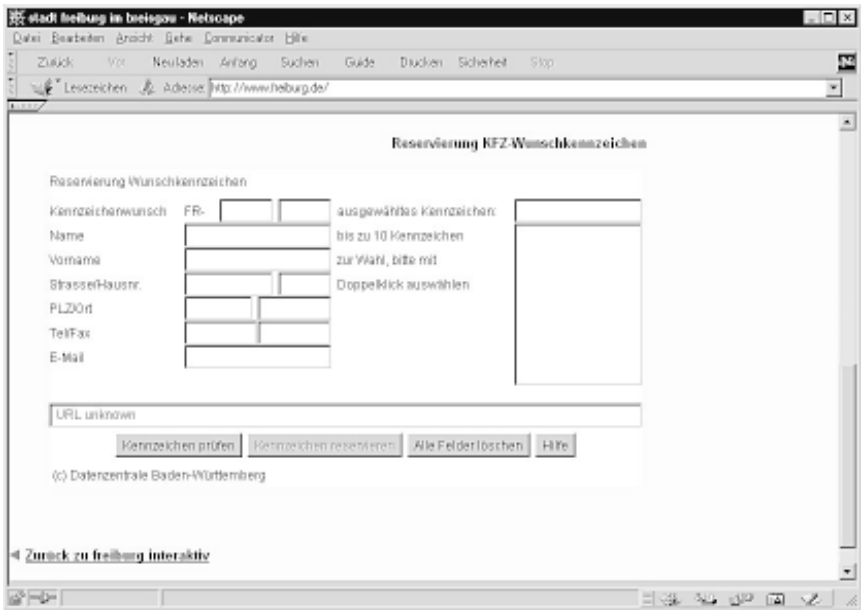
Unsere Intranet-Adresse: http://www.seninn.verwalt-berlin.de/LAZ/vc4/. Ansprechpartner für unser Intranet-Angebot: Hr. Wiegand - wiegand@seninn.verwalt-berlin.de

*MICHAEL WIEGAND* ◆

## Kfz-Wunschkennzeichen reservieren!

Die Stadt Freiburg bietet einen interessanten online Service für ihre PKW-Besitzer an: man kann sich sein Kfz-Wunschkennzeichen per Internet reservieren lassen.
Eine Reservierung kann nur erfolgen, wenn:

- Java im Browser (Netscape oder Microsoft ab Version 4.x) aktiviert ist
- das Wunschkennzeichen komplett eingegeben (2 Buchstaben, 3 Ziffern) wird
- das Wunschkennzeichen innerhalb der Kennzeichengruppe AA- bis JZ liegt und die Buchstaben B, F und G in keiner Kombination vorkommt
- die persönlichen Daten (inkl. Tel.Nr.) vollständig sind.




War die Reservierung des Kfz-Wunschkennzeichens erfolgreich, so wird dieses Kennzeichen für 14 Tage in der Kfz-Zulassungsstelle der Stadt Freiburg bereitgehalten. Danach verfällt die Reservierung. Das Wunschkennzeichen kostet 25.- Mark und ist bei Inanspruchnahme in der Zulassungsstelle zu bezahlen. ◆

## Lokale Agenda 21 online

Das Internet-Informationsangebot der Senatsverwaltung für Stadtentwicklung, Umweitschutz und Technologie wurde um das politisch aktuelle Thema "Lokale Agenda 21 - Berlin" erweitert. Auf der Homepage http://www.sensut.berlin.de finden Interessierte unter dem Button "StadtAgenda 21" alles Wissenswerte zu diesem Thema. Informiert wird über die Aktivitäten von mehr als 150 Agenda-Akteuren der Stadt aus Wirtschaft, Wissenschaft, NGOs (Non Governmental Organizations) sowie über Schulen und den Bildungsbereich, über das Abgeordnetenhaus, über bezirkliche Gruppen und die Bezirke sowie über die Senatsverwaltungen. Mit dem Angebot wird allen Agenda 21-Akteuren kostenlos die Möglichkeit eröffnet, sich auf dieser neuen Web-Site zu präsentieren. Der interessierten Öffentlichkeit wird die Chance geboten, sich über diese Web-Site komfortabel und umfassend zu informieren.

Darüber hinaus wird auch der gesamtstädtische Konsultationsprozeß gefördert. Dazu wurde ein spezielles Diskussionsforum eingerichtet, das die Möglichkeit bietet, eigene Meinungen ins Netz zu bringen und mit anderen Interessierten virtuell zu diskutieren. Außerdem ist es auch möglich, per Mausklick Fragen zum Thema Lokale Agenda 21 an die Verwaltung zu stellen.

Das neue Informationsangebot wird abgerundet durch Informationen über die Geschichte des Agenda 21-Prozesses (UN-Konferenz 1992 in Rio de Janeiro), mit Link- und Literaturlisten, dem Zugang zu einem Terminkalender zu Agenda-Aktivitäten in Berlin, der von der Grünen Liga aktualisiert wird sowie über internationale Aktivitäten der Senatsverwaltung für Stadtentwicklung, Umweltschutz und Technologie mit unmittelbarem Agenda-Bezug.

Für Akteure, die sich mit eigenen Beiträgen zur Agenda 21 im internet präsentieren möchten, stehen auf unserer Web-Site Anmeldeformulare zur Verfügung. Diese sind jeweils unter dem Button "Angaben hinzufügen oder korrigieren" zu finden und befinden sich an mehreren Stellen der Web-Site, z.B. unter dem Button "öffentlicher Arbeitskreis". Das Anmeldeformular für den Zugang zur Web-Site mit →

← eigenen Beiträgen kann auch unter Tel. 9025-2488 oder -2465 bzw. per E-Mail bei gisela.klindworth@sensut.verwalt-berlin.de angefordert werden. ◆

## Die besten Suchmaschinen im Internet



Wer im gigantischen Heuhaufen des Internet fündig werden will, braucht zuverlässige Suchdienste. Inzwischen gibt es im Web hunderte von Suchmaschinen. Das Computermagazin CHIP hat die wichtigsten davon getestet.

Die besten englischsprachigen Suchmaschinen sind der CHIP zufolge Hotbot (www.hotbot.com) und Northern Light (www.northernlight.com). Hotbot hat nach eigenen Angaben rund 110 Millionen Web-Seiten indiziert, so daß diese bei Suchanfragen durchforstet werden können; Northern Light kennt sogar 150 Millionen Seiten. An Hotbot loben die Tester der CHIP die einfache Handhabung und die verschiedenen Spezialsuchfunktionen, beispielsweise die Möglichkeit, gezielt nach Audiodateien, Bildern oder Email-Adressen zu forschen. Northern Light wartet zwar nicht mit diesen Extras auf, wird im Test aber deutlich häufiger fündig als Hotbot und stellt die Suchergebnisse sehr übersichtlich dar.

Unter den deutschsprachigen Suchmaschinen erhalten Altavista (www.altavista.de) und Fireball (www.fireball.de) die Empfehlung der CHIP. In Altavista sind rund 8 Millionen deutsche Web-Seiten verzeichnet, in Fireball 6,5 Millionen. Altavista überzeugt durch seinen komplexen Datenbestand und die umfangreichen Suchmöglichkeiten. Fireball glänzt durch die höchste Trefferzahl bei den deutschen Angeboten und durch eine Reihe von Filtern, mit denen man nicht relevante Seiten ausblendet. ◆

## Internet-Cafés in der Jugendarbeit



In Räumen der Kinder- und Jugendeinrichtung Wichertstraße 24 in Prenzlauer Berg entstand vor einigen Monaten Berlins 7. Internet-Café in einer Jugendfreizeitstätte. Das neue Freizeitangebot entstand im Rahmen des Projektes „Internet Cafés in der Jugendarbeit" das Bestandteil der ressortübergreifenden Initiative „Projekt Zukunft - Der Berliner Weg in die Informationsgesellschaft" ist.

Das Café wird von der Jugend- und Familienstiftung des Landes Berlin gemeinsam mit der Mannesmann o.tel.o GmbH, den Trägern, der Werkstatt neue Technologien und Kultur e.V. (WeTeK), der Pfefferwerk GmbH und dem Bezirksamt finanziert. Öffnungszeiten: dienstags bis sonnabends von 15 bis 21 Uhr.

Im Rahmen der Vereinbarung des Landes Berlin und o.tel.o fördern die Senatsverwaltung für Schule, Jugend und Sport, die Jugend- und Familienstiftung des Landes Berlin und die Mannesmann o.tel.o GmbH darüber hinaus die im letzten Jahr eingerichteten Internet Cafes, so dass deren Existenz gesichert ist.

Weitere vier Internet-Cafés sind in Jugendfreizeitstätten in Kreuzberg, Marzahn, Spandau und Zehlendorf geplant. Sie sollen alle in diesem Jahr eingerichtet und eröffnet werden. ◆

## debitel akquiriert die "erste Adresse" Deutschlands im Internet



Zum 1. Juli hatte debitel die Vorzeigeadresse Deutschlands im Internet, berlin.de übernommen. debitel erschließt damit einen der künftig bedeutsamsten Teile der Wertschöpfungskette auf dem Telekommunikationsmarkt: qualitativ hochwertige Inhalte und Transaktionssysteme. Dr. Joachim Dreyer, der Vorstandsvorsitzende der debitel AG, kommentierte den Erwerb: "Mit diesem neuen Dienst sichert sich debitel Deutschlands "erste Internet-Adresse", einen Zugang zum Content Providing und damit einen bemerkenswerten Wettbewerbsvorsprung." Am 9. Juli wurde dann bekannt, dass debitel mit der Swisscom einen neuen Mehrheitsaktionar gefunden hat, mit dem der weitere Ausbau der Geschäftsfelder im Mobilfunk, im Festnetz und im Internet gemeinsam vorangetrieben werden soll.

Der Münchner Branchenexperte Mathias Plica prognostiziert, daß sich deren Schwerpunkt bis zum Jahr 2001 vom Internet-Access in Richtung Inhalt, Service und Anwendungen verlagern wird. Werden gegenwärtig noch 85 Prozent der Werte im Bereich Internet-Zugang generiert, wird sich dieser Anteil bis 2001 auf 40 Prozent reduzieren. Der Beitrag von Dienstleistungen, Inhalten und Anwendungen zur Wertschöpfung wird dagegen von heute zehn auf dann über 40 Prozent steigen.

Mit berlin.de verfügt die größte netzunabhängige Telefongesellschaft Europas über die international attraktivste deutsche Domaine. Pro Monat werden rund 2,5 Millionen Seitenabrufe verzeichnet. Das junge regionale Online-System hat bereits mehr als 20.000 registrierte Nutzerund bietet über 20.000 Seiten Inhalte an.

Eine weitere Besonderheit von berlin.de ist das Betreibermodell. Die Domaine wird als Public-Private-Partnership betrieben. Berlin stellt kostenlos Namen, qualitativ hochwertigeInhalte der öffentlichen Hand sowie die Autorisierung als offizielles Stadtinformationssystem, die privaten Betreiber tragen im Gegenzug die erforderlichen Investitionen für den Ausbau. ◆

akademie·de
<die internet-akademie>

**Die SPLITTER-Leser können künftig von den „Tips & Tricks“, einem Angebot von akademie.de, die Internet-Akademie, mit täglich aktuellen Tips zu Internet, Kommunikation, E-Commerce und Marketing, profitieren. Tips & Tricks sind auch im Internet unter http://www.tips-tricks.de zu finden.**

## Link in einem neuen Fenster öffnen

Wenn Sie Informationen suchen, ist es sehr nützlich, mehrere Browserfenser geöffnet zu haben. Gerade bei Abfragen von Suchmaschinen muß man erst die Seite öffnen, um zu entscheiden, ob die gesuchten Informationen enthalten sind. Sind sie nicht auf der Seite, muß man über den Zurück-Button wieder zur Suchmachinen-Seite und einen anderen Link wählen.

Wenn Sie dagegen mehrere Fenster verwenden, werden die Seiten bereits im Hintergrund geladen. Sie sparen also erhebliche Ladezeit der Seiten ein. Nur das Öffnen der Links in einem neuen Fenster ist meist umständlich.

Wenn Sie Links anklicken, erscheint die Seite aber üblicherweise im selben Fenster. Sie müssen den Link also umständlich über das Kontextmenü in einem neuen Fenster anzeigen lassen.

Es geht aber auch einfacher. Tastenkombinationen zu drücken ist in jedem Fall schneller. Wir wollen Ihnen in diesem Artikel die Tastenkombinationen der verschiedenen Browser vorstellen.

**Netscape Navigator**

Für den Navigator gibt es keine besonderen Tastenkombinationen für das Öffnen in einem neuen Fenster. Genauer betrachtet braucht man das auch nicht. Im Kontextmenü befindet sich der Eintrag „In einem neuen Fenster öffnen“ gleich an Position 1. Dadurch ist er weitaus schneller zu erreichen als derselbe Eintrag im IE.

**Microsoft Internet Explorer**

Im IE ab Version 3 können Sie durch Drücken der Shift-Taste (Umschalt) einen Link in einem neuen Fenster anzeigen lassen. Halten Sie also die Umschalt-Taste gedrückt, und klicken Sie gleichzeitig mit der Maus auf den Link.

Bei den Favoriten funktioniert das nicht. Aber auch da bewirkt die Umschalt-Taste Nützliches. Wollen Sie mehrere Favoriteneinträge nacheinander anzeigen, drücken Sie die Umschalt-Taste. Dadurch wird das Favoritenmenü nach dem Klick auf den Favoriten nicht geschlossen. Sie können also einen weiteren Favoriten anklicken. Dieser wird dann allerdings im selben Fenster geöffnet.

**Opera**

Im norwegischen Browser Opera gilt ebenfalls die Tastenkombination „Umschalt + Klicken“. Dadurch wird auch in Opera ein neues Fenster mit dem Link geöffnet. Aber es gibt noch eine viel interessantere Variante.

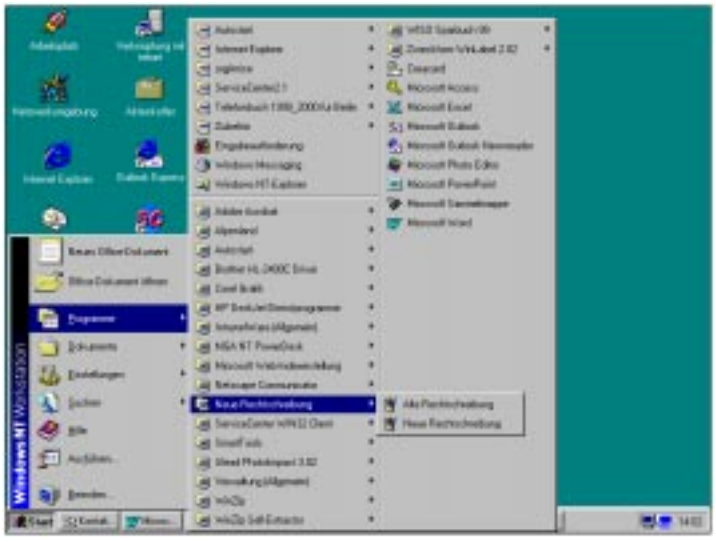
Durch Drücken der Kombination „Strg + Umschalt + Klicken“ starten Sie ebenfalls den Link in einem neuen Fenster, aber dieses Fenster wird automatisch in den Hintergrund versetzt, so das Sie sofort in der ersten Seite weiterlesen können. Sie können sie sich dann später anzeigen lassen, wenn die Seite vollständig geladen ist.

Fenster schließen

Sind es dann doch zu viele Fenster geworden, können Sie das jeweils aktuelle wieder durch eine Tastenkombination schließen. Drücken Sie dazu „Strg + w“. Dieser Hot-Key funktioniert in allen Browsern. Wenigstens da konnten sich die Browserprogrammierer einigen. ◆

## Hier spricht das Testlabor

Eine neue Nachricht für die geplagten Nutzer zur deutschen Rechtschreibüberprüfung. Mit diesem Zusatz können die Anwender von Microsoft Office 95 und Office 97 nun entscheiden, ob sie ihre Texte nach den alten oder den neuen Rechtschreibregeln überprüfen lassen wollen. ➔



*Alt und Neu*

← Dieses Tool ersetzt die bisher verfügbare überarbeitete Rechtschreibprüfung, die gleichzeitig alte und neue Rechtschreibung akzeptiert hat.

Nach der Installation finden sie im Startmenü unter Programme - Neue Rechtschreibung die Möglichkeit zwischen alten und neuen Rechtschreibregeln umzuschalten. Dieser Zusatz lässt sich mit Office 95 und Office 97 unter Windows 95, Windows 98, Windows NT 3.51 und Windows NT 4.0 einsetzen.

Möchten Sie dieses Tool einsetzen, setzen Sie sich mit mir in Verbindung. Tel.: 9012(912)-60 68.

*JÜRGEN ZIMMERMANN* ◆

# Copyright im Internet - Teil III -

## *DOI - Digital Object Identifier*



Zum wirkungsvollen Schutz gegen Missbrauch von digitalen Informationen in Netzwerken sowie zum kommerziellen elektronischen Publizieren bedarf es einer einheitlichen Identifizierungsmethode für alle Objekte. Ein solches Copyright-System ist der Digital Object Identifier (DOI). Darüber hinaus bietet das DOI-System die Möglichkeit, eine Verbindung zwischen den Benutzern von Informationen und den Rechteinhabern herzustellen und erleichtert so den automatisierten Handel mit digitalen Inhalten. Das Projekt zur Konzeption des DOI wurde 1995 von der American Association of Publishers (AAP) aufgesetzt. In Washington wurde basierend auf dem erarbeiteten Konzept im Februar 1997 ein erster Prototyp vorgestellt. Seit Juli 1997 wird das DOI-System von US-amerikanischen und europäischen Verlagshäusern in einem Pilotprogramm eingesetzt.

**Aufbau des DOI**

Der DOI besteht aus einem Präfix zur Definition der Orte, wo Informationen erhältlich sind, und einem Suffix zur eindeutigen Identifizierung eines bestimmten Objektes. Das Präfix setzt sich wiederum aus einer Directory-Nummer und einer Verlagsidentifizierungsnummer zusammen. Als Suffix folgt eine Object-ID, deren Aufbau und Länge nicht vorgeschrieben sind. Ein DOI sieht z.B. folgendermaßen aus:

| **Präfix** | **Suffix** |
|---|---|
| 10.1001/ | [ISBN] 3-409-87940-4 |

Die Directory-Nummer wird einem Verlag vom Directory-Manager zugeteilt. Directory-Manager kann es für jedes Land oder jede Branche geben. Im Rahmen des Pilotprogrammes gibt es nur einen Directory Manager und alle Präfixe beginnen mit den Ziffern 10. Danach folgt eine vierstellige Ziffer, die den Verlag identifiziert. Das dem Schrägstrich folgende Suffix wird individuell vom Verlag vergeben. Das Suffix kann Objekten jeder Größe (Buch, Artikel, Abbildung etc.) und allen Dateiarten (Text, Audio, Video, Grafik, Software etc.) zugewiesen werden. Ein Buch kann beispielsweise eine DOI-Nummer besitzen und eine Komponente innerhalb des Buches (z.B. ein Kapitel) kann eine weitere DOI-Nummer haben. Der Verlag muß die kompletten DOIs einschließlich der Links zu den entsprechenden Objekten an den Directory-Manager melden.

**Nutzung des DOI-Systems**

Das DOI-System stellt Werkzeuge zur Verfügung, die Verlage und Unternehmen sowohl für die interne Verwaltung ihrer Inhalte als auch für den digitalen Vertrieb dieser Inhalte nutzen können. Ein Nutzer, z.B. Kunden, Studenten oder Wissenschaftler, startet mit Hilfe einer DOI-Nummer eine Anfrage beim Directory-Manager. Im allgemeinen braucht der Nutzer die DOI-Nummer dabei nicht zu kennen. Alle identifizierbaren Objekte werden am Bildschirm mit einem Icon markiert, und das eigentliche System läuft im Hintergrund. Klickt ein Nutzer auf die DOI-Nummer eines Objektes, wird eine Nachricht an das zentrale Directory geschickt, in dem die Web-Adresse des Objektes gespeichert ist. Diese Adresse wird zusammen mit einer Anweisung, die entsprechende Internetadresse aufzusuchen, zum Browser des Nutzers gesendet. Nach kurzer Zeit sieht der Nutzer eine Web-Seite, auf der der jeweilige Verlag den Inhalt des Objektes entweder direkt zeigt oder weitere Informationen über das Objekt und darüber, wie das Objekt oder auch verwandte Informationen zu erhalten sind, anbietet.

**Unterstützung und Akzeptanz des DOI in Europa**

Von den am Prototyp teilnehmenden Verlagen wurden bereits im November 1997 über 200.000 DOIs vergeben. Nach anfänglichen Schwierigkeiten findet die Initiative der Association of American Publishers auch in Europa großen Anklang. An der ersten europäischen Demonstration des DOI-Systems auf der Frankfurter Buchmesse im vergangenen Jahr nahmen Elsevier Science, Academic Press und der Springer-Verlag teil. Hier wurden Applikationen präsentiert, bei denen ein Benutzer in einer Liste einen DOI-Button anklicken konnte, um auf einen bestimmten Artikel zuzugreifen. In einer weiteren Anwendung wurden die Leser über ein Inhaltsverzeichnis zu den entsprechenden Abstracts und Artikeln einer Zeitschrift geführt. Management und Vermarktung des DOI-Systems werden mittlerweile von der internationalen DOI-Foundation in Washington und Genf übernommen.

## *Offene Fronten beim Schutz von digitalen Werken*

Abgesehen von den technischen Problemen der Implementierung und Nutzung von MMRCS und DOI ergeben sich eine Vielzahl von organisatorischen Fragen: ➔

← Wie vollzieht sich der Übergang von Rechten, muss dann dem Objekt ein neuer DOI zugeteilt werden, was geschieht mit Kopien, die mit dem alten DOI noch im digitalen Umlauf sind ?

Wie sind multiple oder von der Nutzung her differenzierte Rechte, zusammengesetzte oder „virtuelle", nur temporär bestehende Objekte, Verlagsgemeinschaften, Autorengemeinschaften, die Verbindung von originären analogen und abgeleiteten digitalen Werken und andere Fälle durch den DOI zu handhaben - hat ein Werk zukünftig eine Historie, eine Sequenz von DOIs mit unterschiedlicher Bedeutung ?

Ist die vorgesehene Struktur und Größe des DOI überhaupt ausreichend dimensioniert? Reichen sechs Stellen zur weltweiten Identifikation von Verlagen, wenn jeder Autor seinen eigenen Kleinverlag gründet, da er für die digitale Veröffentlichung keine herkömmlichen Verlage mehr benötigt? Wird die ISBN, die sich am herkömmlichen Druckwerk orientiert, dem Charakter von zusammengesetzten multimedialen Objekten gerecht?

Werden Autoren und Künstler als Urheber das Verfahren akzeptieren? Eine einfache, unkomplizierte Handhabung wurde bereits von Künstlerverbänden angemahnt?

Sind europäische Projekte und das Verfassen von Gesetzen der richtige Weg, oder werden solche Initiativen einfach vom internationalen Softwaremarkt überrollt?

Wie sollen DOIs international online überprüft werden? Sind hier neue Regulierungsbehörden notwendig? Wie erfolgt eine Prüfung von DOIs, die offline mit Datenträgern verteilt werden? Wer hindert jemanden z.B., sich selbst einen DOI auszudenken, bei einem Werk den Titel und zwei Worte zu ändern, das Werk ins Internet zu stellen und Nutzungsgebühren unter einem Pseudonym auf einer Cybercash-Bank auf den Bahamas einzusammeln?

Welche Rolle werden zukünftig die Verwertungsgesellschaften wie z.B. VG Wort und andere spielen? Müssen sie digital aufrüsten, um DOIs zu verwalten und im Internet nach der Nutzung von Werken aktiv zu recherchieren, oder erübrigt sich das Tätigkeitsfeld, wenn jeder Verlag oder Künstler selbst die Nutzungsgebühren im Netz eintreibt?

Die MMRCS-Initiative der Europäischen Gemeinschaft ist sicher ein Weg, um die Entwicklung von Sicherheitsstandards voranzutreiben, obwohl man auch hier den Eindruck hat, dass Teile der Probleme bereits in anderen von der EU gesponsorten Projekten behandelt oder sogar gelöst wurden. Vorhandene oder vor der Verabschiedung stehende Gesetze im Kommunikations- und Multimedia-Umfeld müssen bei den Überlegungen berücksichtigt oder zumindest kritisch hinterfragt werden. Eine Beschränkung auf die Thematik des Copyright wird dem generellen Problem nicht gerecht. Auch andere Bestrebungen, wie zum Beispiel die digitale Signatur können ihren Beitrag zur Absicherung von Rechten leisten.

## *Die digitale Signatur*

Die digitale Signatur hat nichts mit einer gescannten oder einer über Passwort oder Login kontrollierten elektronischen Unterschrift zu tun, sondern dient zur Authentifizierung des Erstellers und des Inhalts eines elektronischen Dokumentes. Eine digitale Signatur wird durch die Kombination eines öffentlichen Schlüssels (Public Key), der von Zertifizierungsstellen vergeben wird, und eines geheimen privaten Schlüssels (Private Key) generiert und an ein elektronisches Dokument angehängt. In Deutschland ist das Verfahren im Signaturgesetz (SigG) festgelegt.

Die digitale Signatur ist eine der wesentlichen Voraussetzungen für den Abschluss von Geschäften bei Electronic Commerce und im Internet und zielt im wesentlichen auf den Austausch von Geschäftsdokumenten zwischen nicht bekannten Partnern. Zum Zeitpunkt der Übermittlung digital signierter Dokumente besteht noch kein Vertrag zwischen Absender und Empfänger. Der Identifizierung des Absenders und der rechtlichen Relevanz der übermittelten Nachricht kommen daher eine große Bedeutung zu. Die digitale Signatur soll hier den gleichen rechtlichen Charakter gewinnen wie die eigenhändige Unterschrift. Die Bundesnotarkammer sieht außerdem auch Anwendungsgebiete, bei denen die digitale Signatur bei der Erstellung und Versendung von Urkunden im Rechtsverkehr zum Einsatz kommt.

Die Grenzen zwischen der reinen Nutzung von Informationen und dem kostenpflichtigen Bezug von Dienstleistungen, bei denen es auch zu elektronischen vertraglichen Vereinbarungen kommt, verschieben sich zunehmend. Das kann dazu führen, dass die digitale Signatur auch im Umfeld der Verbreitung von Nachrichten und der Nutzung von Informationspools im Internet an Bedeutung gewinnt. Auch zur Absicherung von Urheberrechten und des Copyright im Internet könnte die digitale Signatur künftig beitragen.

## *Ausblick*

Die Bedeutung des Problems und einer schnellen Lösung zeigt sich auch in anderen Bereichen. Unternehmen, die sich in der Vergangenheit hauptsächlich mit der Erstellung von Programmen oder DV-Dienstleistungen beschäftigt haben, versuchen zunehmend auch die Inhalte unter ihre Kontrolle zu bringen. Gute Beispiele hierfür sind z.B. Beteiligungen an Fernsehsendern oder der Aufkauf kompletter Sammlungen und deren Digitalisierung für die Nutzung im Internet. Die sich in Jahrhunderten herausgeprägte Interessengemeinschaft von Urhebern und Publizisten beginnt sich aufzulösen. Autoren und Künstler beschreiten eigene Wege der Veröffentlichung →

← ihrer Werke - ohne Verlage, ohne Händler, ohne Galerien. Die moderne Informationsgesellschaft definiert die Rollen neu - auch die Unterschiede zwischen Urheber und Konsument verschwinden, neue Formen kooperativen Schaffens zeichnen sich ab.

Diese Veränderungen regulativ einzufangen wird durch die Verbreitung des Personal-Computers und der Internetnutzung immer schwieriger. Auch ausgefeilte Schutzmechanismen zur Codierung oder eindeutigen Identifizierung von Objekten werden immer schneller unterlaufen. Nationales Recht steht nahezu hilflos vor der internationalen Verbreitung und Nutzung von Information. Fragen, ob bei der Nutzung eines Werkes das Recht des Landes des Urhebers oder Copyright-Inhabers oder des Landes, in dem das Werk genutzt wird, gelten soll, führen sich bereits heute ad absurdum. Verlage agieren international, es kann nicht sichergestellt werden, dass der Empfänger eines Objektes identisch mit dem späteren Nutzer ist, Zeitpunkt und Form der Nutzung sind nach der ersten Bereitstellung nicht mehr zu kontrollieren usw. Internationale, allgemein anerkannte, durch Standard-Softwareprodukte unterstützte und einfache Regelungen sind gefordert.

Der sich stürmisch entwickelnde Markt wird von sich aus eigene normative Kraft entwickeln und manche gutgemeinte Initiative überholen. Dabei werden herkömmliche Geschäftsfelder unter Umständen auf der Strecke bleiben. Vielerorts wird das Copyright bereits nur als nachgeordnet angesehen, und die Urheberrechte, der Schutz desjenigen, der das Werk geschaffen hat, werden in den Vordergrund der Überlegungen gestellt. In einem Zeitalter, in dem jeder mit jedem kommunizieren kann, werden die Rechte von Mittlern von Informationen immer mehr unter Druck geraten.

Was in jedem Fall sichergestellt sein muss, ist, daß originäre Ideen und individuelles künstlerisches Schaffen auch im Zeitalter des Internet geschützt sind, dass jeder Autor und jeder Künstler die ihm zustehende Anerkennung seiner Leistung - ideell, persönlich und monetär - erhält. Auch in der modernen Informationsgesellschaft mit Technikverliebheit und den unbegrenzten Möglichkeiten des Internet, des Fernsehens und anderen Formen der Informationsverbreitung müssen die essentiellsten Grundsätze des Menschenrechts erhalten bleiben.

**Profil**

Dr. Ulrich Kampffmeyer, Jahrgang 1952, ist Geschäftsführer der Unternehmensberatung PROJECT CONSULT GmbH, eine der führenden produkt- und herstellerneutralen Beratungsgesellschaften für Dokumenten-Management und Workflow in Deutschland.

PROJECT CONSULT GmbH, Büro Hamburg, Oderfelder Str. 17, D-20149 Hamburg, Tel.: 040 / 460 762 20, Fax: 040 / 460 762 29, E-Mail: PROJECT_CONSULT@CompuServe.COM◆

# Digitale Archive – ein neues Paradigma?

## *Internationales Kolloquium aus Anlaß des fünfzigjährigen Bestehens der Archivschule Marburg*



Die Archivschule Marburg nahm ihr fünfzigjähriges Bestehen zum Anlaß, ein internationales Kolloquium zum Thema „Digitale Archive – ein neues Paradigma?“ zu veranstalten, zu dem sich über 100 Teilnehmer aus dem In- und Ausland in Marburg am 22. und 23. Juni 1999 einfanden. Es war die Absicht der Archivschule, angesichts einer zunehmenden Informatisierung der Verwaltung die Frage nach den neuen Strukturen von Kommunikations- und Geschäftsabläufen in den Behörden und nach den Möglichkeiten ihrer Überlieferung in den Unterlagen auf die Tagesordnung zu setzen – eine Frage, die angesichts der zentralen Aufgabe der Archive, eine aussagekräftige und authentische Überlieferung zu bilden, für den Berufsstand von größter Wichtigkeit ist. Da das Kolloquiumsthema im Spannungsfeld von Archivwissenschaft, Verwaltungswissenschaft und Informationswissenschaft anzusiedeln ist, setzte sich der Kreis der Referentinnen und Referenten aus Vertretern aller drei Disziplinen zusammen, die den Teilnehmern der Veranstaltung umfassende Einblicke in die aktuellen Entwicklungen gaben.

In seinem Eröffnungsvortrag gab Heinrich Reinermann (Deutsche Hochschule für Verwaltungswissenschaften Speyer) einen allgemeinen Überblick über die zu erwartenden Auswirkungen der Informationstechnik auf die Reform der öffentlichen Verwaltung. Dabei unterstrich er, daß die neuen Technologien zur Umgestaltung sämtlicher gesellschaftlicher Bereiche und zum Wegfall bisheriger Determinanten für Strukturen und Abläufe führen. Für die Verwaltung bedeutet dies die Chance zu neuen Organisationsmodellen, wobei insbesondere horizontale Abstimmungen und Verbünde über Behördengrenzen hinweg hohe Produktivitätsreserven bieten.

Die Aufgabe der Verwaltung konzentriert sich dabei stärker auf die Gewährleistung anstelle der eigenen Erledigung von Aufgaben. Es ergeben sich auch neue Möglichkeiten für Beratungs- und Dienstleistungen, etwa ein zeitnahes, individuelles Verwaltungshandeln und ein bisher unbekanntes Maß an Verwaltungstransparenz. Angesichts dieser neuen Verwaltungswelt, die nicht nur von „electronic records“, sondern einem regelrechten „electronic government“ gekennzeichnet ist, ist aber auch eine neue Form des Wissensmanagement vonnöten, um die explosionsartig wachsende Menge digitaler Daten sinnvoll nutzen zu können. →

← Die Auswirkungen der neuen Verwaltungswelt auf die Archive war Gegenstand der ersten, von Hermann Rumschöttel (Gerneraldirektor der Staatlichen Archive Bayerns) geleiteten Arbeitssitzung. Hartmut Weber (Landesarchivdirektion Baden-Württemberg, Stuttgart) unterstrich in seinem Referat die Notwendigkeit, daß sich die Archive den neuen Technologien nicht verschließen dürften, sondern sich den neuen Wind, der in der Verwaltung wehe, für ihre eigenen archivischen Interessen nutzbar machen müßten. In der heutigen Zeit ist es nicht mehr das Wissen allein, das Macht bedeutet, sondern vor allem der Wissensvorsprung. Digitale Aufzeichnungen allerdings müssen immer im Kontext ihrer Systeme als ungestörtes Ensemble erhalten bleiben, um spätere Lesbarkeit und Interpretation zu gewährleisten. Das Konzept des Life-Cycle, das momentan in der Diskussion um die elektronischen Aufzeichnungen viel diskutiert wird, läuft dabei Gefahr, diese Kontexte zu übersehen, weil es die neue Zwecksetzung, die mit der Archivierung ermöglicht wird, nicht in den Blick nehmen kann. Archive sollten beim Nutzerbedarf ansetzen und neue Formen anbieten, wie etwa virtuelle Lesesäle oder ein digitales Praktikum für Studenten.

Der Bibliothekarsberuf ist von der Digitalisierung ebenfalls betroffen, wenn auch auf andere Art und Weise als das Archivwesen. Dies wurde in den Ausführungen von Hermann Leskien (Generaldirektor der Bayerischen Staatlichen Bibliotheken, München) deutlich. Auswirkungen stellte er vor allem in den Bereichen der Beschaffung mit dem Zuwachs an digitalen Dokumenten, der Nutzung bei der wachsenden Zahl an Online-Nutzungen und der Nutzerstruktur, die durch Verjüngung des Benutzerdurchschnitts nach Elektronisierung der Katalogsysteme geprägt ist, sowie in der steigenden Bedeutung von digitalen Bibliotheksverbünden fest. Die Retrodigitalisierung analoger Dokumente stellt die Bibliotheken allerdings vor enorme Kosten, weniger aufgrund der eingesetzten Technik, als vielmehr durch den erforderlichen Personaleinsatz. Ein wirtschaftlicher Einsatz dieser Technik ist aus diesem Grunde fragwürdig. Der Mehrwert liegt vermutlich vor allem in der Verfügbarmachung bisher schwer zugänglicher Primärquellen sowie in einer pragmatischen Zusammenstellung von Material für Lehre und Studium.

Rainer Kuhlen (Universität Konstanz) sprach über Informationsautonomie. Er stellte als Hilfsmittel für die Informationssuche die im Internet bereitstehenden Informationsassistenten vor, die gesuchte Informationen selbständig im Internet ermitteln. Diese Assistenten erlauben die automatische Suche nach einem vorgegebenen Profil und stellen selbständig neue Links her. Sie visualisieren, was sie gefunden haben, validieren den Inhalt, erstellen Exzerpte und nehmen schließlich selbständig Transaktionen vor. Die Möglichkeiten automatischer Beschaffung von Information erhöhen eher die Unsicherheiten, statt sie zu beseitigen. Deshalb ist eine Überschätzung der Potentiale der Informationsbeschaffung zu befürchten.

Christine Pétillat (Direktorin des Centre des Archives Contemporaines, Fontainebleau) erläuterte die Zusammenhänge zwischen den Verwaltungsreformbestrebungen der letzen 15 Jahre und der Einführung digitaler Informationstechniken in Frankreich. Durch die bereits in den achtziger Jahren eingeführte Minitel-Technologie hatte Frankreich zwar in den letzten anderthalb Jahrzehnten einen technologischen Vorsprung inne, unterlag jedoch der Gefahr, zu lange daran festzuhalten und den Anschluß an die neue, durch die Internet-Technologie geprägte Entwicklung zu verpassen. Im Zusammenhang der Verwaltungsdezentralisierung der letzten Jahre gab es deshalb forcierte Bestrebungen, die staatlichen Behörden ans Internet anzuschließen und damit sowohl im zwischenbehördlichen Verkehr wie auch im Kontakt zwischen Bürger und Verwaltung mehr Effizienz und Kundennähe zu gewährleisten. Angestrebt wird ein bürgernaher und offener Staat („un état proche et ouvert"), in dem die neuen Transparenzregelungen auch im Archivwesen umgesetzt werden: eine Novellierung des Archivgesetzes, die die Sperrfristen radikal verkürzt, steht kurz vor der Verabschiedung.

Die zweite Arbeitssitzung, geleitet von Ingrid Grohmann (Staatsarchiv Leipzig), stand unter dem Leitthema „Die digitalisierte Verwaltung". Hier stellte zunächst Andreas Engel (Universität Koblenz-Landau) das Domea-Konzept zur Verwaltungsautomatisierung der Bundesministerien vor. Er erläuterte wie die bisherigen Verfügungen in elektronischer Form abgebildet werden sollen.

Die technischen Aspekte von elektronischen Geschäftsprozessen und Workflow-Managementsystemen beleuchtete Stefan Jablonski (Universität Erlangen-Nürnberg). Am Beispiel der Geschäftsabläufe einer Bank präsentierte er Workflows als Systeme, die je nach den konkreten Bedürfnissen und Rahmenbedingungen modelliert werden müssen. Hauptschwierigkeit ist die Definition von Prozessen. Sie kann nur bei stark strukturierten Vorgängen gelingen und muß auch dort einen hohen Grad an Flexibilität haben.

Nicole Bickhoff (Landesarchivdirektion Baden-Württemberg, Stuttgart) erläuterte am Beispiel des elektronischen Grundbuchs in Baden-Württemberg die neuen archivischen Anforderungen, die sich in einer digitalisierten Verwaltungswelt stellen. Bis 2006 sollen sämtliche Grundbücher des Landes in elektronischer Form vorliegen und die dann geschlossenen Grundbücher auf Papier den Staatsarchiven übergeben werden. Das Konzept des elektronischen Grundbuchs basiert auf dezentralen Produktionssystemen in den Grundbuchämtern, die mit einem zentralen Archivsystem verbunden sind, das als Grundbuch im rechtlichen Sinn fungiert. Dieses Archivsystem dient zugleich als Auskunftssystem für die →

← externe Nutzung über das Internet, wobei der Datenschutz durch Verschlüsselung und digitale Signaturen gewährleistet ist.

Die von der globalen Vernetzung der Informationssysteme aufgeworfene Frage nach internationalen Standards behandelte Nils Brübach (Archivschule Marburg) mit einer Vorstellung der aktuellen Planungen zur internationalen Normierung der Schriftgutverwaltung. Auf australische Anregung beschäftigt sich seit 1998 eine multinationale Arbeitsgruppe mit dieser Frage und hat sich als Ziel gesetzt, eine ISO-Norm zu erarbeiten. Als Grundproblem stellt sich dabei die unterschiedliche Funktion von Schriftgut insbesondere im deutschen und im angelsächsischen Raum heraus. Während die deutschen „Akten" als Instrument zur Steuerung von Verwaltungshandeln eingesetzt werden, haben die „records" vor allem eine inhaltliche Dokumentationsfunktion. Die daraus resultierenden Unterschiede in den Normungsvorschlägen konnten in der Aufteilung der geplanten Norm in einen Qualitätsstandard und einen Technischen Bericht aufgefangen werden, so daß für das Jahr 2001 mit einer Verabschiedung der ISO 15489 zu rechnen ist.

Die dritte, von Ottfried Dascher (Hauptstaatsarchiv Düsseldorf) geleitete Arbeitssitzung war dem Gedächtnis des Geschäftsprozesses gewidmet. Auch hier stand zunächst ein internationaler Vergleich im Mittelpunkt. Stefan Fisch (Deutsche Hochschule für Verwaltungswissenschaften Speyer) berichtete über seine Erfahrungen aus Forschungen zur elsässischen Geschichte in der Zwischenkriegszeit und insbesondere über die Veränderungen in der staatlichen und kommunalen Verwaltung nach der Rückgliederung des Elsaß nach Frankreich. Hier standen die Unterschiede der Formen von Schriftgutverwaltung im Mittelpunkt. Schon nach 1871 hatte die deutsche Verwaltung im eroberten Elsaß gegen die in Frankreich übliche Verbindung von Registratur und Archiv kritisiert. Während im erneut französischen Elsaß nach 1918 auf kommunaler Ebene deutsche Verwaltungstraditionen noch bis weit in die zwanziger Jahre fortwirkten, gab es auf der mittleren staatlichen Ebene des Departements einen deutlichen Bruch in der Organisation des Schriftguts, der dazu führte, daß die Akten nun – anders als zu deutscher Zeit – praktisch keine Bearbeitervermerke mehr enthielten und jeder Bearbeiter seine eigene Ablagemethode anwandte - durchaus mit Sinn, machte er sich doch dadurch im streng hierarchisch-monokratischen System weniger ungewollt von oben kontrollierbar.

Einen ebenfalls historischen Vortrag hielt Rainer Polley (Archivschule Marburg). Er widmete sich der Protokollierung in kollegialen Gremien der Spätphase des Ancien Régime. Anhand anschaulicher Beispiele illustrierte er, wie sehr das mit der Ausbildung des frühneuzeitlichen Behördenstaats entstandene Kollegialitätsprinzip im Zeichen der Aufklärung immer mehr in Frage gestellt wurde. Insbesondere die aufwendigen Protokollierungsverfahren und die Mündlichkeit des Geschäftsgangs stießen immer wieder auf Kritik, blieben jedoch in manchen Bereichen bis weit ins 19. Jahrhundert hinein vorherrschend.

Peter J. Horsman (Niederländische Archivschule, Amsterdam) sprach über die archivische Bewertung elektronischer Aufzeichnungen und behandelte in seinem Referat die Frage, wie in Zeiten einer zunehmend durch E-Mail und Internet geprägten Kommunikation überhaupt noch „Spuren im Sand der Zeit" gesichert werden könnten. Da sich durch den Einsatz von elektronischer Kommunikation die Funktion von Schriftlichkeit innerhalb von Behörden und Organisationen verändere, müssten die Archivare ihr Bewertungsmethoden, -kriterien und -ziele revidieren.

Angelika Menne-Haritz (Archivschule Marburg) befaßte sich mit dem Thema des Prozeßgedächnisses und der Funktionen, die Erinnern und Vergessen in seiner Konstruktion haben. In ihrem Vortrag entwarf sie eine Typologie der offenen Entscheidungsprozesse und stellte dabei mündliche, schriftliche und elektronische Prozesse einander gegenüber. Gemeinsame Merkmale bestehen in einer nach Abschließung nach außen, in selbstorganisierter Prozeßhaftigkeit sowie im Bedarf an Steuerungsinstrumenten, wobei alle diese Merkmale in einer auf dem Vergessen oder Vermeiden von Texten beruhenden Kommunikation begründet liegen. Bei elektronischen Prozessen stellen sich jedoch besondere Probleme, da elektronische Aufzeichnungen pure Texte ohne äußerliche Merkmale und Kennzeichen sind. Von archivischer Seite müssen deshalb neue Strategien entwickelt werden, bei denen das bestmögliche Funktionieren der selbstorganisierter Prozesse in der Verwaltung im Zentrum steht. Als Gesamtbilanz der Tagung kann festgehalten werden, daß einmal mehr deutlich wurde, in welch hohem Maße es für die Archive im Zeitalter der elektronischen Aufzeichnungen eine unverzichtbare Notwendigkeit ist, sich bereits vor der Übernahme mit der im Vergleich zu herkömmlichem Schriftgut neuartigen Struktur der aktuellen Verwaltungsunterlagen auseinanderzusetzen. Hierzu hat das Kolloquium der Archivschule Marburg einen wichtigen Beitrag geleistet.

*Andreas Metzing* ◆

Die ganze Welt...



...des Internet:

KISS

LIT Berlin:
(030) 90 12 60 01

# Neue Medien stellen neue Herausforderungen

## *Fachkongress „Lernen und Arbeiten im Netz“ tagte in Berlin*

In Berlin fand Anfang Juli der Fachkongress „Lernen und Arbeiten im Netz“ statt. Mit diesem Kongress setzte die Senatsverwaltung für Arbeit, Berufliche Bildung und Frauen ihre Aktivitäten fort, die gesellschaftlichen und arbeitsmarktpolitischen Konsequenzen des Übergangs von der Industrie- zur Informationsgesellschaft mit Expertinnen und Experten aus verschiedenen Lebens- und Arbeitsbereichen zu diskutieren.

Die Senatorin für Arbeit, Berufliche Bildung und Frauen, Gabriele Schöttler, erklärte zum Kongress: „Die Industriegesellschaft befindet sich auf dem Weg zur Informationsgesellschaft. Die Arbeitswelt wandelt sich tiefgreifend. Vor diesem Hintergrund besteht die große Zukunftsaufgabe darin, die neuen Technologien und Medien für die Sicherung bestehender und die Schaffung neuer Arbeitsplätze produktiv zu machen. Die IT-Branche zählt zu den Spitzenbranchen der deutschen Wirtschaft. Die Wachstumsraten liegen im zweistelligen Bereich. Heute sind hier bundesweit bereits mehr als 1,8 Millionen Beschäftigte tätig. Gleichzeitig können in Deutschland derzeit rund 100.000 Stellen in der Informations-, Kommunikations- und Medientechnik nicht besetzt werden, weil Fachkräfte fehlen. Ausbildung, Qualifizierung und Fortbildung im Bereich der neuen Informationstechnologien, in den Multimedia-Anwendungen und den interaktiven Diensten kommt daher eine Schlüsselrolle zu. Gerade auch in der Region Berlin-Brandenburg lassen sich so vorhandene Beschäftigungspotentiale erschließen.

Mit den neuen Medien verbinden sich neue Qualifikationsanforderungen. Es geht nicht allein um formale Abschlüsse. Im Vordergrund stehen vielmehr soziale Kompetenzen, wie Teamfähigkeit, vernetztes Denken, Eigeninitiative und Interdisziplinarität. Um den Bedarf an qualifiziertem Fachpersonal zu decken, brauchen wir eine Qualifizierungsoffensive, die diesen Erfordernissen Rechnung trägt. Flexibel und unbürokratisch müssen wir Wege finden, um Beschäftigte für den speziellen Bedarf der Praxis aus- und weiterzubilden. Das Angebot bei Ausbildung, Weiterbildung und Schulung ist so zu gestalten, dass es je nach Bedarf in Anspruch genommen werden kann.“



***Foto: Hahn***

Als Beispiele führte Senatorin Schöttler das Konzept „Training on the Job“ an. Hier werde die Qualifizierung in einem dualen System mit Praxisprojekten in der Wirtschaft und öffentlichen Einrichtungen erworben. Mit dem Konzept „Instruction on demand“ werde berufsbegleitend in jenen Praxisprojekten qualifiziert, wo der jeweilige Bedarf für die Qualifizierung entsteht.

Um die Defizite des Berliner Standorts in den Bereichen Medien, Kommunikation und Bildung abzubauen, soll die Zusammenarbeit von Senat und Wirtschaft noch intensiver werden. Dazu dient auch das Leitprojekt „Anpassung und Erweiterung von Medien- und Kommunikationsqualifikationen im Dialog mit regionalen Akteuren aus Wirtschaft und Bildung“. So soll ein Kompetenzzentrum Berlin für die Medien- und Kommunikationsberufe aufgebaut werden, um die Maßnahmen zu initiieren, zu koordinieren und umzusetzen. Die Hauptaufgabe besteht darin, dem Mangel an Fachkräften im Medien- und Kommunikationsbereich durch entsprechende Maßnahmen entgegenzuwirken.

Senatorin Schöttler: „Das Kompetenzzentrum Berlin für die Medien- und Kommunikationsberufe soll die Kommunikation zwischen Unternehmen, Verbänden, Personaldienstleistern, Arbeitsämtern, Bildungsinstitutionen, Verwaltung und Politik anregen und deren Aktivitäten abstimmen. Es soll die Strukturen und Entwicklungen auf den Märkten für berufliche Qualifikation in Medien- und Kommunikationsberufen analysieren, aber auch die Angebote an Aus-, Fort- und Weiterbildung. Aufgabe des Kompetenzzentrums ist es außerdem, die Verbundausbildung zu fördern, da viele kleine und mittlere Unternehmen alleine nicht ausbilden können.

Ein weiteres Aufgabenfeld wird sein, ein tagesaktuelles ➔

← Kommunikationskonzept auf der Basis von Internet-Technologie zu erstellen und umzusetzen. Dies soll die nötige Markttransparenz auf der Angebots- und Nachfrageseite ermöglichen und für die nötigen quantitativen und qualifikatorischen Anpassungen sorgen. Ganz besonders wichtig ist mir dabei das Vorhaben, dem Zentrum eine Innovationsleitstelle zur Förderung der Frauen in den IT-Berufen anzugliedern. Obwohl gerade Frauen Stärken in den sozialen Kompetenzen haben, gilt der IT-Beruf noch als eine Domäne der Männer. Deshalb ist es mir wichtig, gerade im Zusammenhang mit diesem Kongress mein besonderes Anliegen zu unterstreichen, Mädchen einen besseren Zugang in diese Berufe zu verschaffen." ◆

## CeBIT 2000 im EXPO-Jahr bereits im Februar



Im Frühjahr 2000 heißt es wieder: It's CeBIT Time - diesmal schon im Februar. Das hannoversche Messegelände wird mit seinem Angebot an Informationstechnik, Software, Büroautomation und Telekommunikation erneut zum Treffpunkt für die IuK-Industrie aus aller Welt. Aufgrund der Weltausstellung EXPO 2000 in Hannover (01.06. - 31.10.2000) findet die CeBIT im kommenden Jahr bereits vom 24. Februar bis zum 01. März statt - und nicht, wie sonst, Mitte oder Ende März. Zur CeBIT 2000 wartet das Messegelände mit einer verbesserten Infrastruktur auf, die Ausstellern und Besuchern gleichermaßen zugute kommt.

Zu Beginn des neuen Jahrtausends kann die CeBIT Hannover auf eine dreißigjährige erfolgreiche Geschichte zurückblicken. 1970 startete sie als ein Schwerpunkt der Hannover Messe, der kontinuierlich an Bedeutung gewann. Seit 1986 wird die CeBIT als eigenständige Messe veranstaltet, die sich innerhalb weniger Jahre zur Leitmesse der internationalen Informations- und Telekommunikationstechnik sowie zur größten Messe der Welt entwickelte.

Zur CeBIT 2000 erwartet die Deutsche Messe AG rund 7.400 Aussteller (1.999: 7.412), die eine Netto-Ausstellungsfläche von rund 390.000 m2 (398.913 m2) in 26 Hallen belegen. Die Angebotsschwerpunkte der CeBIT 2000 sind "Informationstechnik", "Network Computing", "Entwicklung, Konstruktion, Fertigung, Planung", "Automatische Datenerfassung", "Software, Beratung, Dienstleistungen", "Telekommunikation", "Office Automation", "Bank- und Sparkassentechnik", "Kartentechnik/Sicherheitstechnik" sowie "Forschung und Technologietransfer".

Der Schwerpunkt "Telekommunikation" präsentiert sich zur CeBIT 2000 internationaler denn je. Zahlreiche international operierende Carrier nutzen die Messe, um ihr Angebot den CeBIT-Besuchern aus aller Welt vorzustellen. Erstmals gibt es eine eigene Halle für Distributoren. Neue Anlaufstelle vor allem für die Händler von I+K-Technik ist die Halle 10 im Süden des Messegeländes. Ein Teil der Halle 10 steht darüber hinaus den Anbietern von Netzwerktechnik zur Verfügung.

Um einzelne Inhalte der CeBIT 2000 gezielt und konzentriert vorzustellen, werden themenspezifische Gemeinschaftspräsentationen veranstaltet: Software-Zentrum Mittelstand" in der Halle 4, "Internet-Park" in der Halle 6, " Network Information Center - NIC" in der Halle 11, "Bank-Finanz-Systeme" "im Erdgeschoß der Halle 18, "AIM International (Automatic Identification Manufacturers) " in der Halle 19, "CeflS - Centrum für InformationsSicherheit" in der Halle 23 und "Satellite Business" in der Halle 26. Das "Europäische Anwender-Centrum Kommune, Staat und Wirtschaft ENAC" präsentiert sich auf erweiterter Fläche in allen vier Pavillons an der Nordseite der Halle 11. Neu im Themenkatalog von ENAC ist der Bereich "Geografische Informationssysteme". Erstmals wird innerhalb des CeBIT-Schwerpunktes "Telekommunikation" eine Gemeinschaftspräsentation zum Thema "Powerline - Kommunikation aus der Steckdose" durchgeführt. Tagungen, Forumsveranstaltungen und Firmenvorträge runden das Messeangebot ab.

Die CeBIT wartet im Februar 2000 mit einer weiter verbesserten Infrastruktur auf. Im Südosten des Messegeländes entstehen zusätzliche Parkplätze: Ein neues Parkhaus bietet Platz für 1.150 Pkws. Im Osten des Geländes auf dem Dach der Halle 8 wird ein neuer Eingang geschaffen. Von diesem Eingang "Ost 3" aus führt eine 30 Meter breite Brücke über den Messeschnellweg bis zur EXPO Plaza und zu den Parkplätzen im Osten des Messegeländes. An der EXPO Plaza wird eine Straßenbahnhaltestelle gebaut - die Endstation "Expo-Ost". Zur CeBIT 2000 nimmt diese Station ihren Testbetrieb auf. Hier hält die Stadtbahnlinie 11, die von der Nordstadt über die Innenstadt, Kirchrode und Bemerode sowie den Kronsberg bis zum EXPO-/Messegelände fährt.

Zusätzliche Hallenverbindungsbauten sorgen dafür, daß der CeBITBesucher seinen Rundgang über das Messegelände trockenen Fußes machen kann. Neu zur CeBIT 2000 sind die Übergänge zwischen den Hallen 1 und 2, 2 und 3 sowie 11 und 12. Ein architektonisches Highlight wird das EXPO-Dach auf dem Freigelände zwischen den Hallen 12 und 26. Die filigrane Konstruktion aus zehn Holzschirmen hat die Größe von zwei Fußballfeldern. Unter dem EXPO-Dach entstehen vier Pavillons, die erstmals zur CeBIT 2000 genutzt werden und den Ausstellern des Schwerpunktes "Telekommunikation" zur Verfügung stehen. ◆

CeBIT HANNOVER 24.2.–1.3. 2000

Berlin

# OPENNET 99

**Die Veranstaltung**



Vom 15.11.1999 bis zum 17.11.1999 findet in Bad Honnef bei Bonn die OPENNET'99 statt. Die OPENNET wird vom „German Chapter of the Internet Society" veranstaltet und informiert bereits seit 8 Jahren die Fachöffentlichkeit über neue Entwicklungen im Internet.

Die OPENNET'99 steht unter dem Leitthema: Internet - Technologie für eine neue Gesellschaft. Auch in diesem Jahr mischt die OPENNET Bewährtes und Neues. Wichtige Bestandteile der Konferenz sind:

- State-of-the-Art-Tutorials (Rechtsfragen, Internet-Technologie, Sicherheit, Zahlungsverkehr im Internet)
- Information über aktuelle Entwicklungen (Weiterentwicklung des WWW, Gefahren und Bedrohung im Internet)
- Hintergrundinformation und Zusammenhänge verdeutlichen (Kryptogesetze, Geistiges Eigentum und Internet, Datenschutz im Internet)
- Entscheidungshilfen (Übertragungstechnik, Sicherheitsmaßnahmen, WWW-Auftritt)
- Praxisnaher Erfahrungsaustausch wird im Konferenzteil „Meet the expert" geboten. Ihre Fragen werden von TOP-Experten beantwortet.

**Die Vortragenden**

Wer kann besser über eine Technologie informieren als die Erfinder? Viele der Internet Pioniere Deutschlands sind Mitglied in der Internet Society. Wie auch schon in den letzten beiden Jahren wird auch die OPENNET'99 wieder in Kooperation mit dem World Wide Web Consortium durchgeführt. Mit Robert Cailliau konnten wir bereits jetzt einen der beiden Erfinder des WWW als Redner gewinnen.

**Was bietet die OPENNET'99 für Sie?**

Die OPENNET bietet Informationen aus erster Hand. Die Referenten arbeiten an führender Stelle an der Weiterentwicklung des Internet und an der Schaffung der gesellschaftlichen und rechtlichen Grundlagen seiner Nutzung mit. Sie haben beruflich mit dem Internet zu tun? Dann finden Sie hier kompetente Gesprächspartner zu allen Fragen rund um das Internet.

Weitere Auskünfte auch zu Sponsoring erhalten Sie unter: OPENNET'99, c/o Christine Harms, GMD - Schloß Birlinghoven, 53754 Sankt Augustin, Mailto: Christine.Harms@gmd.de ◆

# SYSTEMS 99



Vom 18. - 22. Oktober täglich von 9:00 bis 18:00 Uhr hat die SYSTEMS 99 ihre Pforten geöffnet. Die letztjährige „Premiere" der SYSTEMS auf dem neuen Messegelände hat eindrucksvolle Rekorde aufgestellt, 1999 werden sie alle nochmals übertroffen werden. Ab September können Sie unter www.systems.de Ihre Eintrittskarten online bestellen. Das transparente Ordnungsprinzip der „Fachmessen in der Messe" hat überzeugt und kann als Kompetenzcenter zur optimalen Orientierung über den Markt genutzt werden.Die Ausstellungsfläche wird in diesem Jahr um eine Halle aufgestockt, weil bereits im Februar 80% der bisherigen Flä che fest gebucht war. Einzigartig auf der SYSTEMS: die Foren - der Infovorsprung durch SYSTEMS-Wissen. Hier präsentieren und diskutieren Top-Entscheider aus Wirtschaft, Politik, Medien und Industrie die aktuellen Trendthemen. Stellen Sie sich Ihr individuelles Systems-Foren-Programm zusammen. Buchen Sie rechtzeitig und online Ihre Anreise, Ihr Hotel und Ihr persö nliches Begleitprogramm zur Messe. ◆

# Jubiläums-IFA: Rekordbeteiligung mit 849 Aussteller aus 36 Ländern



Innovationen standen im Mittelpunkt der Internationalen Funkausstellung in Berlin. Sie ist die Leitmesse für die Unterhaltungselektronik und die privat genutzte Informations- und Kommunikationselektronik. Darüber hinaus ist die IFA ein Ereignis für die Fachwelt: Europas wichtigste Ordermesse. 849 Aussteller aus 36 Ländern (1997: 812 Aussteller aus 33 Ländern) präsentierten auf der vergrößerten Ausstellungsfläche von 160.000 Quadratmetern die neuesten Technologien, Produkte und Dienstleistungen der konvergierenden Branchen: vom Plasmabildschirm über den digitalen Camcorder-Winzling, von der exklusiven HiFi-Anlage bis hin zum Internet-Handy und „Organizer".

Die Funkausstellung, die in diesem Jahr ihr 75-jähriges Jubiläum feierte, stellte unter Beweis, daß sie sich nicht auf ihren Lorbeeren ausruht. Die Internationale Funkausstellung entwickelte sich von der weltgrößten Spezialmesse für Unterhaltungselektronik zur umfassenden Schau der Consumer Electronics. Sie präsentierte denn Besuchern das gesamte Spektrum der konvergierenden Technologien. Dabei spielte die Digitaltechnik die überragende Rolle. „Digitale Evolution" hieß auch das Motto der IFA '99.

Ob Fernsehen oder Hörfunk, Computer- oder Telekommunikationswelt, Übertragungs-, Empfangs- oder Speichertechnologien - sie alle profitieren von den Fortschritten der Digitaltechnik. Sie sorgt für eine bessere Ausnutzung der Frequenzen, für eine stark wachsende Speicherkapazität, neue Dienste und Serviceleistungen, für mehr Bedienkomfort, für Miniaturisierung und damit letztlich auch für Mobilität. Und dies sowohl in der ➔

← Unterhaltungselektronik als auch in der Computer- und Telekommunikationswelt.

Was vor 75 Jahren mit der Vorstellung von Detektorgeräten und erster Röhrenempfänger, Empfangskristallen und Kopfhörern begann, entwickelte sich sukzessive zur bedeutendsten Multimediamesse weltweit und heute zu einem Wegweiser in die Informationsgesellschaft.

Für das Fernsehen wurden auf der IFA gleich zwei wichtige Fortschritte präsentiert, zum einen die terrestrische Übertragung digitaler Signale (DVB-T), zum zweiten ein neuer Standard für Universalempfänger, der unverschlüsselte und Pay-TV-Signale aller Art erschließt, die sogenannte „Multimedia-Home-Platform" (MHP). Zur „neuen" Fernsehwelt gehören weiterhin Settop-Boxen, die digitale Satellitensignale aufarbeiten und darüber hinaus auch die Möglichkeiten des Internet-Surfens über TV-Geräte ermöglichen. Auch die Geräte selbst entwickelt sich weiter: Plasma-Flachbildschirme, TV-Geräte mit integriertem Internet-Empfangsteil, Audio-/Video-Kombinationen, 16:9/100 Hz-Geräte und natürlich vermehrt auch Dolby-Surround-Anlagen mit und ohne Schnur. ◆

## Broschüre „Arbeiten im Call Center"



Das Kooperationsbüro multimedia+arbeitswelt in Frankfurt am Main hat im April 1999 eine Broschüre mit dem Titel „Arbeiten im Call Center - Handlungshilfe für Betriebs- und Personalräte" veröffentlicht. Diese 46-seitige Broschüre stellt eine Zusammenfassung der Call-Center-Tagung dar, die im November 1998 in Bad Oeynhausen stattfand. Veranstaltet wurde die Tagung vom Kooperationsbüro multimedia + arbeitswelt, von DPG, HBV und IG Medien, der Technologieberatungsstelle des DGB Landesbezirks NRW und der Hans-Böckler-Stiftung in Zusammenarbeit mit der Zeitschrift Computer Fachwissen für Betriebs-und Personalräte. Inhaltlich wurden folgende Themen behandelt:

- Call Center Tagung - Betriebsräte stellen „ihr" Call Center vor.
- Analysen und Forderungen - Die sechs Fachforen der Tagung (Arbeitszeit und Personaleinsatzplanung, Arbeitsgestaltung im Call Center, Zwei Sekunden sind zuviel (Abhören), Betriebliche Vergütungssysteme, Qualifizierung, Arbeiten als Call-Center-Agent)
- Arbeitsbedingungen im Schraubstock - Call Center in der Kommunikationsbranche
- Zentralisieren und auslagern - Call Center in der Medienbranche
- Zwischen Kundenwunsch und Rationalisierung - Call Center bei Banken und Versicherungen
- Was wir wollen - Leitbilder für das Arbeiten im Call Center
- Handlungsanleitung - Hilfe für Betriebs- und Personalräte in Call Centern.

Am Ende der Darstellungen werden einige Fachbegriffe erklärt und weitere Informationsquellen aufgeführt.

Die Broschüre ist erhältlich von dem Kooperationsbüro multimedia + arbeitswelt, Rhonestraße 2, 60528 Frankfurt/Main, Telefon 069 - 66 95 32 01 oder Fax 069 66 95 32 32. ◆

## Statistik regional jetzt auch auf CD-ROM



Die von den Statistischen Ämtern des Bundes und der Länder bisher nur auf Disketten gemeinsam herausgegebene Datenbank Statistik regional ist ab sofort auch auf CD-ROM für Windows 95/98 oder NT 4.0 erhältlich. Mit dieser CD hat der Nutzer die Möglichkeit, wirtschaftliche und soziale Fakten aus der amtlichen Statistik für Kreise und kreisfreie Städte, Regierungsbezirke, Länder und das Bundesgebiet zu recherchieren und zu Tabellen zusammenzustellen.

Statistik regional bietet Daten zu folgenden Sachgebieten:

- Gebiet und Bevölkerung
- Gesundheitswesen
- Unterricht und Bildung
- Beschäftigung, Erwerbstätigkeit, Arbeitslosigkeit
- Land- und Forstwirtschaft
- Produzierendes Gewerbe
- Gebäude und Wohnungen, Bautätigkeit, Baulandverkäufe
- Fremdenverkehr (Gäste, Übernachtung)
- Verkehr (Unfälle, Kfz-Bestand)
- Sozialwesen (Jugendhilfe)
- Öffentliche Finanzen
- Volkswirtschaftliche Gesamtrechnungen
- Umwelt (Wasser, Abwasser, Abfall)
- Wahlen

Die CD-ROM Statistik regional enthält die Datenbank mit der zum Betrieb erforderlichen Software sowie eine Übersichtskarte zur administrativen Gliederung Deutschlands als PDF-Datei. Die Daten sind einfach und schnell abzurufen. Die Recherche erfordert keine Vorkenntnisse. Recherchierte Ergebnisse können nicht nur ausgedruckt, sondern auch im Text- oder im Excel-Format gespeichert und weiterverarbeitet werden.

Statistik regional erscheint jährlich (aktuelle Ausgabe 1998), enthält jetzt die Daten für zwei Berichtszeiträume (Jahre 1995 und 1996) und kostet als Einzelplatzversion DM 290,- / EUR 148,27 einschl. Versandkosten.

Eine Demo-Version von Statistik regional mit vollem Funktionsumfang und einigen Daten zur Bevölkerung kann für DM 10 - / EUR 5,11 erworben werden. Bestellungen sind zu richten an: Statistisches Landesamt Berlin Alt - Friedrichsfelde 60, 10315 Berlin, Telefon: 030 / 9021 3899 Telefax: 030 / 9021 3655 ◆

SPLITTER

Wenn sich Ihre Anschrift ändert,

wenden Sie sich bitte telefonisch oder schriftlich an die Redaktion des SPLITTER, Telefon 90 12 (912) 6080

Nr. 3 / 1999

Raum für Versandetikett

**Liebe Splitter-Leser,**

möchten Sie nicht einmal selber zur Feder greifen?

Der Splitter lebt von seinen Autoren und aktuellen Mitteilungen direkt aus den Verwaltungen.

Wir freuen uns jederzeit über Themenvorschläge und Artikel aus Ihren Reihen.

Die nächste Ausgabe erscheint im Dezember 1999. Der Redaktionsschluß ist am **15. Oktober 1999**.

Faxen Sie uns einfach Ihre Texte oder rufen Sie an:

| | |
|---|---|
| Frau Hahn | 90 12 (912) 6080 |
| Herr Brodersen | 90 12 (912) 6014 |
| Fax | 90 12 (912) 3908 |

**Ihre Splitterredaktion**

# Internetsucht

Du bist internetsüchtig, wenn ...

An diesen untrüglichen Zeichen kannst Du erkennen, dass Du internetsüchtig bist: Du bezeichnest den Gang zur Toilette als „downloading". Du kommst aus Deinem Zimmer, stellt fest, dass Deine Eltern ausgezogen sind, und Du hast nicht die geringste Ahnung, wann das passiert ist. Du brauchst eine Viertelstunde, um durch Deine Bookmarkdatei zu scrollen. Deine Alpträume sind in GIF und HTML. Du stellst Dein Modem ab und dieses grässliche Gefühl stellt sich ein, gerade so, als hättest Du bei einem geliebten Menschen den Stecker rausgezogen. Du beginnst, Dich als „Kurt @ Netz Punkt DE" vorzustellen. Dein Herz schlägt jedesmal höher und dreht Kapriolen, wenn Du im Fernsehen eine neue WWW-Adresse siehst. Deine Freundin drapiert eine blonde Peruecke über Deinen Monitor, um Dich daran zu erinnern, wie sie aussieht. Wenn Du auf eine Homepage schaust, die voll mit Links ist, erscheinen alle Links bereits in lila. Dein Haustier hat eine eigene Homepage. Du kannst Deine Mutter nicht anrufen - sie hat kein Modem. Deine Telefonrechnung ist so schwer wie ein Ziegelstein. Du schreibst Deine Hausaufgaben in HTML und gibst dem Lehrer die URL.

Agentur Harald Happe

Gefunden in der Online-Ausgabe von info CANARIAS - Ausgabe 433 vom 29. 7. 1999 - URL: http://www.infocanarias.com/ ◆

IMPRESSUM

Herausgeber: Landesbetrieb für Informationstechnik Berlin (LIT), Berliner Straße 112-115, 10713 Berlin
Telefon: 90 -0, intern (912), Fax: 90 12 (912) 31 12,
Internet: http://www.lit.berlin.de/ und im Intranet: http://www.lit.verwalt-berlin.de

Redaktion:
Michael Brodersen: (auch Grafik & Layout), Tel: 90 12 (912) 60 14,
E-Mail: Michael.Brodersen@lit.verwalt-berlin.de oder MBrodersen@t-online.de
Gabriele Hahn: Tel: 90 12 (912) 60 80, E-Mail: Gabriele.Hahn@lit.verwalt-berlin.de

Druck: LIT Berlin, Auflage: 2.350

Gastautoren: Guido Stepken
AG-Internet, Landeskriminalamt Berlin
Dr. Olaf Winkel, Institut für Politikwissenschaft der Universität Münster
Harald Seiffert, Von zur Mühlen 'sche Unternehmensberatung GmbH, Bonn
Frank Wehrand, Fachhochschule für Verwaltung und Rechtspflege Berlin
Dr. Ulrich Kampffmeyer, Project Consult GmbH, Hamburg
Michael Wiegand, Senatsverwaltung für Inneres, Berlin
Andreas Metzing

Namentlich gekennzeichnete Beiträge geben nicht unbedingt die Meinung der Redaktion bzw. des LIT wieder.
SPLITTER Nr. 4/99 erscheint voraussichtlich im Dezember 1999