Arbeitskreis Technik der Datenschutz-
beauftragten des Bundes und der Länder

Datenschutz bei der Nutzung von Internet und Intranet

Herausgeber:

Der Landesbeauftragte für den Datenschutz
Mecklenburg-Vorpommern
Schloss Schwerin
19053 Schwerin
Telefon: (03 85) 5 94 94-0
Telefax: (03 85) 5 94 94-58
E-Mail: datenschutz@mvnet.de
Internet: http://www.lfd.m-v.de

Verantwortlich: Dr. Werner Kessel

Redaktionsschluss: 15. Dezember 2000

Herstellung: CLUB WIEN und cw Obotritendruck GmbH, Schwerin

Vorwort

Das Internet wird im Zeitalter der Informationsgesellschaft zu einem immer wichtigeren Kommunikationsmittel. Auch die Verwaltungen nutzen im Zuge ihrer Modernisierung in zunehmendem Maße dieses weltweite Computernetz und die dort eingesetzten Technologien. Künftig sollen nicht nur Informationen zwischen den einzelnen Behörden ausgetauscht, sondern den Bürgerinnen und Bürgern auch Dienstleistungen "online" angeboten werden.

Der Anschluss von lokalen Netzen an das Internet ist jedoch mit erheblichen Risiken für den Datenschutz und die Datensicherheit verbunden. Die Rechner und Übertragungswege des Internet sind nur eingeschränkt kontrollierbar. Da bei der Entwicklung des Internet Sicherheitsfragen lange Zeit eine untergeordnete Rolle gespielt haben, wurden keine Maßnahmen getroffen, um die Risiken für Vertraulichkeit, Integrität und Zurechenbarkeit in angemessener Weise zu minimieren. Der erste Teil dieser Broschüre, die *Orientierungshilfe "Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet"*, die von den Arbeitskreisen Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erstellt wurde, beschreibt vorhandene Risiken und erläutert Maßnahmen, mit denen ihnen in angemessener Weise begegnet werden kann. Es werden verschiedene Firewallarchitekturen dargestellt und Strategien erläutert, mit denen das stets verbleibende Restrisiko minimiert werden kann.

Die zunehmende Nutzung neuer Kommunikationsformen, beispielsweise E-Mail, erfordert unter anderem auch eine neue Art der Verbreitung von Kommunikationsadressen. Hierzu werden elektronische Verzeichnisdienste eingesetzt. Der elektronische Zugriff auf die dort gespeicherten personenbezogenen Daten übersteigt die Möglichkeiten konventioneller Adress- und Telefonverzeichnisse erheblich und birgt ebenfalls neue Risiken für die Vertraulichkeit und die Integrität dieser Daten. Jede datenverarbeitende Stelle muss deshalb sorgfältig prüfen, welche Daten in derartige Verzeichnisse aufgenommen werden. Der zweite Teil der Broschüre, die *Orientierungshilfe "Datenschutzrechtliche Aspekte beim Einsatz von Verzeichnisdiensten"* des Arbeitskreises Technik, enthält Hinweise, wie mit elektronischen Verzeichnisdiensten umgegangen werden sollte, damit schutzwürdige Belange der ver-

zeichneten Personen nicht unangemessen beeinträchtigt werden. Obwohl hier nur Verzeichnisdienste in einer definierten Netzwerkumgebung (Intranet) der öffentlichen Verwaltung betrachtet werden, sind die Empfehlungen prinzipiell auch auf den erweiterten Bereich des Internet anwendbar.

Der dritte Abschnitt der Broschüre ist dem *Arbeitspapier "Vom Bürgerbüro zum Internet"* entnommen, das eine Arbeitsgruppe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder unter Leitung der Landesbeauftragten für den Datenschutz Nordrhein-Westfalen erstellt hat. Dieses Arbeitspapier befasst sich mit datenschutzrechtlichen Fragen bei der Modernisierung der Verwaltung. Die hier veröffentlichten Abschnitte "Informationsangebote öffentlicher Stellen" und "Interaktive Verwaltung" enthalten zwei weitere Aspekte der Internetnutzung öffentlicher Stellen aus datenschutzrechtlicher Sicht. Zum einen wird erläutert, welche datenschutzrechtlichen Anforderungen Behörden beachten müssen, wenn sie eigene Informationsangebote im Internet bereitstellen. Zum anderen werden Hinweise gegeben, wie die Verwaltung den Bürgerinnen und Bürgern interaktive Kommunikation anbieten und Verwaltungsvorgänge über das Internet abwickeln sollte, damit datenschutzrechtliche Vorschriften nicht verletzt werden.

Dr. Werner Kessel
Landesbeauftragter für den Datenschutz
Mecklenburg-Vorpommern

Inhaltsverzeichnis

Teil 1
Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet

Teil 2
Orientierungshilfe „Datenschutzrechtliche Aspekte beim Einsatz von Verzeichnisdiensten“

Teil 3
Internetnutzung durch öffentliche Stellen

Auszug aus dem Arbeitspapier “Vom Bürgerbüro zum Internet” der Arbeitsgruppe “Serviceorientierte Verwaltung” der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Teil 1

Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet

erstellt von den
Arbeitskreisen “Technik” und “Medien”
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder

Überarbeitete Fassung vom November 2000

1 Einleitung

Das Internet ist ein weltweites Computernetz, in dem hunderttausende größere Rechnerverbünde und somit Millionen einzelner Computer zusammengeschlossen sind. Das Internet hat sich zum weltgrößten und mächtigsten globalen Informations- und Kommunikationsmedium entwickelt. Der Internet-Boom hat auch vor den öffentlichen Verwaltungen nicht Halt gemacht. Seit geraumer Zeit wächst in öffentlichen Stellen der Wunsch nach einem Zugang zu globalen Datennetzen, insbesondere zu dem Internet. Die Netzanbindung soll sowohl zur Informationsgewinnung als auch zur Bereitstellung eigener Informationen für andere dienen (zur Beschreibung des Internet und der wichtigsten Internet-Dienste vgl. Anhang).

Dabei ist der Anschluss an das Internet mit erheblichen Gefährdungen des Datenschutzes und der Datensicherheit verbunden. Die Rechner und Übertragungswege dieses weltweiten Computernetzes sind nicht kontrollierbar. Welchen Weg eine Nachricht nimmt oder in welchem Vermittlungsrechner die Nachricht bearbeitet wird, ist nicht transparent. Denn das Internet wurde ursprünglich nur unter Verfügbarkeitsaspekten entwickelt – auch wenn neuere Entwicklungen versuchen, weiteren Sicherheitsbedürfnissen Rechnung zu tragen. Deshalb wird den Risiken für Vertraulichkeit, Integrität und Zurechenbarkeit vielfach nicht in der gebotenen Weise begegnet. Schwächen finden sich in den Protokollen für die Datenübertragung, in den Implementierungen und Installationen der Programme für die Internet-Dienste und in den angeschlossenen Rechnersystemen. Ohne besondere Schutzmaßnahmen kann sich ein Angreifer oft mit wenig Aufwand unter Ausnutzung der Sicherheitslücken unberechtigten Zugang zu fremden Rechnern verschaffen und dort Daten ausspähen oder sogar manipulieren oder zerstören. Dies ist besonders gravierend, weil angesichts von bereits weit mehr als 100 Millionen Internet-Teilnehmern auch die Zahl der potentiellen Angreifer, die diese Sicherheitslücken ausnützen und somit die am Internet angeschlossenen Verwaltungsrechner bedrohen, sehr groß ist.

Die vorliegende Orientierungshilfe wurde von den Arbeitskreisen „Technik“ und „Medien“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erstellt[1]. Sie soll den für den Betrieb von Netzen der öffentlichen Ver-

1 Aufgrund der Zuständigkeit der Mitglieder dieses Gremiums vor allem für den Datenschutz im öffentlichen Bereich richtet sich diese Orientierungshilfe in erster Linie an öffentliche Verwaltungen. Die Aussagen lassen sich aber im Allgemeinen auch auf andere Bereiche übertragen.

waltung Verantwortlichen deutlich machen, mit welchen Risiken für die Sicherheit der "internen" Netze bei einem Anschluss an das Internet zu rechnen ist und wie diese Risiken begrenzt werden können. Die Frage, in welchen Fällen und unter welchen Bedingungen es zulässig ist, dass Verwaltungen personenbezogene Daten mit Hilfe des Internet übertragen oder veröffentlichen, ist nicht Gegenstand der Orientierungshilfe und muss jeweils konkret untersucht werden.

Die hier entwickelten Strategien zur Risikobegrenzung bedürfen im Einzelfall einer weiteren Konkretisierung, wobei neben den beschriebenen Firewall-Architekturen ggf. weitere Maßnahmen zu ergreifen sind, um eine Gefährdung personenbezogener Daten zu vermeiden (etwa Einsatz von Verschlüsselungsverfahren). Angesichts einer sich ständig verändernden Gefährdungslage infolge der "Entdeckung" neuer unerwarteter Sicherheitsprobleme bleiben auch bei Einsatz von Firewall-Systemen erhebliche Restrisiken bestehen.

Der Anschluss an das Internet ist angesichts dieser Gefährdungslage aus Datenschutzsicht nur vertretbar, wenn zuvor eine eingehende Analyse und Bewertung der damit verbundenen Risiken erfolgt ist und die Gefahren durch technische und organisatorische Maßnahmen hinreichend beherrscht werden können.

2 Vorbereitung und Planung

Grundlage für eine datenschutzgerechte Nutzung des Internet ist eine genaue Planung der Internet-Aktivitäten einer Verwaltung. Je nach dem Informations- und Kommunikations-Bedarf ist eine der möglichen Nutzungsarten unter Berücksichtigung einer der Anschlussmöglichkeiten vorzusehen. Es bedarf einer genauen Analyse sowohl dieses Bedarfs als auch der mit der jeweiligen Anschlussart verbundenen Risiken.

2.1 Nutzungs- und Anschlussmöglichkeiten

2.1.1 Nutzungsarten

Grundsätzlich sind drei Konstellationen der Internet-Nutzung einer Behörde zu unterscheiden:

1. Eine Behörde nutzt einen Internet-Zugang nur, um Informationen im Internet suchen zu können, und/oder
2. eine Behörde stellt eigene Informationen im Internet zum (potentiell weltweiten) Abruf zur Verfügung (wobei im Internet von Informationsanbietern erwartet wird, dass sie auch per E-Mail erreichbar sind [siehe 3.]) oder
3. eine Behörde stellt eigene Informationen im Internet zum Abruf zur Verfügung **und** bietet zusätzlich die **Interaktion mit Bürgerinnen und Bürgern**, z. B. per E-Mail, an.

Diese drei Konstellationen können auf verschiedene Art und Weise technisch umgesetzt werden und verlangen unterschiedliche Maßnahmen, um den Datenschutz und die Datensicherheit zu gewährleisten.

2.1.2 Anschlussarten

Die Anschlussarten an das Internet können in drei verschiedene Szenarien unterteilt werden, die unterschiedliche Sicherheitsrisiken mit sich bringen:

2.1.2.1 Direktanschluss eines Rechners an das Internet

Hier wird ein einzelner, nicht lokal vernetzter Rechner per Modem und Telefonleitung über einen Provider (dies kann ein verwaltungsinterner oder ein externer sein) an das Internet angeschlossen (Abbildung 2.1). Diese Variante spielt besonders bei kleinen Behörden und im privaten Bereich eine große Rolle. Bei eventuellen Angriffen besteht ein Sicherheitsrisiko nur für den einzelnen Rechner. Es lässt sich durch entsprechende Maßnahmen reduzieren (z. B. ausschließliche Verwendung des Rechners für den Zugang zum Internet; sicherstellen, dass Ressourcen des Rechners – wie etwa Festplattenverzeichnisse – nicht für den Zugriff über das Netz freigegeben sind).

Abbildung 2.1: Direktanschluss eines Rechners an das Internet

2.1.2.2 Zentrale Kopplung eines lokalen Netzes an das Internet

Hier hat der Rechner (evtl. über ein LAN oder aber direkt per Modem oder ISDN) einen Zugang zum Intranet der Verwaltung. Von dort besteht ein einziger zentraler Zugang zum Internet (Abbildung 2.2). Eventuelle Angriffe aus dem Internet können bereits an der zentralen Übergangsstelle vom Internet zum Intranet zum großen Teil abgefangen werden. Der Rechner bzw. das LAN ist zusätzlich aus dem Intranet heraus angreifbar.

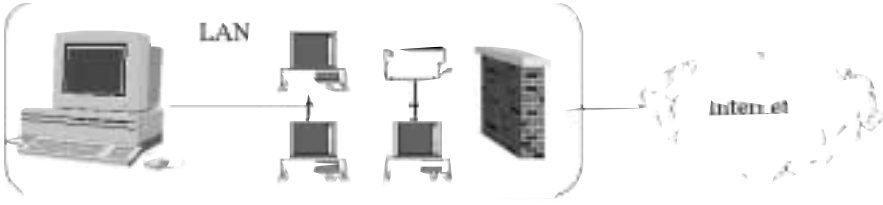


Abbildung 2.2: Zentrale Kopplung eines lokalen Netzes an das Internet

2.1.2.3 Dezentrale Zugänge zum Internet

Neben einem direkten Internet-Anschluss über einen Provider verfügt der Rechner gleichzeitig über eine Verbindung zu einem Intranet (Abbildung 2.3). Bei eventuellen Angriffen besteht nicht nur ein Sicherheitsrisiko für den an das Internet angeschlossenen Rechner, sondern auch für das LAN, in dem sich der Rechner befindet, und das Intranet. Daher ist von dieser Konstellation generell abzuraten.

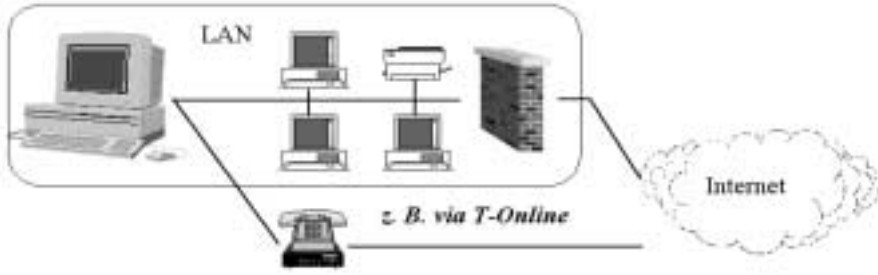


Abbildung 2.3: Dezentraler Anschluss eines lokal vernetzten Rechners an das Internet

2.2 Kommunikations- und Risikoanalyse

Vor einem Anschluss an das Internet ist eine Analyse des Kommunikationsbedarfs durchzuführen. Bei der Beurteilung der Erforderlichkeit eines Internet-Anschlusses ist ein strenger Maßstab anzulegen. Auch wenn die Erforderlichkeit bejaht wird, ist zu prüfen, ob der Verwendungszweck nicht schon durch den Anschluss eines isolierten Rechners erreicht werden kann.

Die Art des zu realisierenden Zugangs hängt wesentlich davon ab, welche Dienste des Internet genutzt werden müssen. Bei der Beurteilung der Erforderlichkeit ist ebenfalls ein strenger Maßstab anzulegen. Dabei ist zu unterscheiden zwischen Diensten, die von lokalen Benutzern im Internet abgerufen werden, und Diensten, die von lokalen Rechnern für Benutzer im Internet erbracht werden. Diese Kommunikationsanforderungen müssen aufgrund der unterschiedlichen Aufgaben sowohl für den zentralen Zugang zum Internet als auch für jeden einzelnen Rechner analysiert werden.

Ausgangspunkte einer derartigen Analyse sind der Schutzbedarf der zu verarbeitenden Daten und die Sicherheitsziele der öffentlichen Stelle sowie die Risiken der unterschiedlichen Dienste. In Anlehnung an die Empfehlungen des BSI-

Grundschutzhandbuchs sind im Rahmen einer Risikoanalyse zur Feststellung des Schutzbedarfs folgende Fragen zu beantworten:

- Welche Datenpakete dürfen auf der Grundlage welchen Protokolls bis zu welchem Rechner im Netz weitergeleitet werden?
- Welche Informationen sollen nicht nach außen gelangen?
- Wie können z. B. die interne Netzstruktur und Benutzernamen nach außen unsichtbar gemacht werden?
- Welche Authentisierungsverfahren sollen benutzt werden; sind benutzerspezifische Authentisierungsverfahren notwendig?
- Welche Zugänge werden benötigt (z. B. nur über einen Internet-Service-Provider)?
- Welche Datenmengen werden voraussichtlich übertragen?
- Welche Rechner mit welchen Daten befinden sich im Netz, die geschützt werden müssen?
- Welche Nutzer gibt es im Netz, und welche Dienste sollen dem einzelnen Nutzer zur Verfügung gestellt werden?
- Welche Aktivitäten im Netz sollen protokolliert werden? (Dabei werden ggf. Fragen des Arbeitnehmerdatenschutzes tangiert.)
- Welche Dienste sollen auf keinen Fall genutzt werden?
- Wird sichergestellt, dass nur die Dienste genutzt werden können, die ausdrücklich freigegeben worden sind (was nicht erlaubt ist, ist verboten)?
- Welcher Schaden kann im zu schützenden Netz verursacht werden, wenn Unberechtigte Zugang erhalten?
- Welche Restrisiken verbleiben, wenn die vorgesehenen Schutzmaßnahmen realisiert wurden?
- Welche Einschränkungen würden Benutzer durch den Einsatz von Schutzmaßnahmen akzeptieren?

Um im Rahmen der empfohlenen Kommunikationsanalyse beurteilen zu können, welche Dienste von welchem Nutzer an welchem Rechner tatsächlich benötigt werden, sollten die jeweiligen Stellen zunächst versuchen, genaue Kenntnisse über die Möglichkeiten und Gefährdungen der angebotenen Kommunikationsmöglichkeiten zu erlangen.

Verwaltungsnetze dürfen an das Internet nur angeschlossen werden, wenn und soweit dies erforderlich ist. Die Kommunikationsmöglichkeiten haben sich am Kommunikationsbedarf zu orientieren. Dabei ist auch zu prüfen, inwieweit das Behördennetz in anschließbare, nicht anschließbare und bedingt anschließbare Teile segmentiert werden muss und ob die Aufgabe mit einem nicht in das Verwaltungsnetz eingebundenen Rechner erfüllt werden kann. Bei einem unvertretbaren Restrisiko muss auf einen Anschluss des jeweiligen Netzes an das Internet verzichtet werden. Der Zugriff auf Internet-Dienste kann in diesem Fall nur über solche Systeme erfolgen, die nicht mit dem Verwaltungsnetz verbunden sind und auf denen ansonsten keine sensiblen Daten verarbeitet werden.

2.3 Sicherheitsrisiken und Schutzmaßnahmen

Mit dem Zugang zum Internet sind Risiken verbunden, die großenteils daraus resultieren, dass das Datennetz nicht unter Sicherheitsaspekten entwickelt wurde. Schwächen finden sich in den Protokollen für die Datenübertragung, in den Implementierungen und Installationen der Programme für die Internet-Dienste und in den angeschlossenen Rechnersystemen. So stellt das zugrunde liegende Protokoll beispielsweise keine sicheren Mechanismen zur Identifikation und Authentisierung bereit.

Die nachfolgend dargestellten Sicherheitsrisiken spiegeln lediglich einen kleinen Ausschnitt der möglichen Angriffe auf Rechnersysteme mit Internet-Anschluss wider. Selbst wenn Maßnahmen gegen die bekannten Gefährdungen getroffen werden, lässt sich ein hundertprozentiger Schutz ohne Verzicht auf die Internet-Anbindung nicht realisieren. Sobald ein Computer Zugang zu einem Datennetz hat, ist er von anderen angeschlossenen Rechnern aus erreichbar. Damit wird das eigene System der Gefahr eines unberechtigten Gebrauches ausgesetzt. Es gibt jedoch eine Reihe von Schutzvorkehrungen, um das Sicherheitsrisiko zu minimieren.

2.3.1 Protokollimmanente Sicherheitsrisiken

Bei vielen gängigen Diensten werden die Inhaltsdaten im Klartext über das lokale Netz (z. B. Ethernet) und über das Internet übertragen. Mit Programmen, die unter der Bezeichnung LAN-Analyzer bekannt sind (z. B. Packet Sniffer), kann der Datenverkehr im Netz bzw. auf den Netzknoten belauscht und nach interessanten Informationen durchsucht werden.

Gegenmaßnahmen:
Verschlüsselung der Daten

Datenpakete können nicht nur abgehört, sondern auch manipuliert werden; z. B. lassen sich die IP-Adressen von Sender und Empfänger fälschen, die TCP Sequence Number von Paketen kann häufig vorhergesagt werden, und der Übertragungsweg ist bei dynamischem Routing modifizierbar. Pakete können abgefangen werden, so dass sie nicht an ihrem Ziel ankommen; ein Angreifer kann sie durch eigene Pakete ersetzen. Weiterhin lässt sich die Kommunikation eines autorisierten Nutzers mitschneiden und später wiedereinspielen (Replay Attack), wodurch sich der Angreifer bei vielen Diensten die Rechte des Nutzers verschafft (z. B. beim Festplattenzugriff über NFS [Network File System]).

Gegenmaßnahmen:
Gegen eine unerkannte Manipulation von Nachrichteninhalten können digitale Signaturen eingesetzt werden.
Für starke Authentisierung eignen sich Einmalpasswörter oder Challenge-Response-Systeme gegen Replay Attacks.
Für Router sollte nach Möglichkeit statisches Routing konfiguriert werden. Außerdem sollte das “Source Routing” abgestellt sein.

Bei vielen Internet-Diensten erfolgt die Authentisierung der Rechner lediglich über die IP-Nummer des Nutzers. Dies kann sich ein Angreifer zunutze machen, indem er IP-Pakete mit gefälschten Absenderadressen (IP-Spoofing) ans fremde Rechnersystem schickt. Sofern das System die IP-Adresse für vertrauenswürdig hält, wird dem Eindringling ein Zugang, unter Umständen sogar mit unbeschränkter Administratorberechtigung, gewährt.

Gegenmaßnahmen:
Konfiguration eines Packet Filters, so dass alle Pakete mit ungültigen IP-Adressen*) und mit offensichtlich gefälschten IP-Adressen (z. B. IP-Pakete von außen mit internen Adressen) verworfen werden und nicht ins System gelangen können. Hierbei sollte man ebenfalls verhindern, dass IP-Pakete mit ungültigen Adressen das eigene System verlassen können. **)

*) definiert im RFC 1597

**) Weitere Hinweise: RFC 2267 (Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing)

Angriffe mit gefälschten Paketen von ARP (Address Resolution Protocol) oder ICMP (Internet Control Message Protocols) basieren ebenfalls darauf, dass sich Rechner allein durch ihre IP-Adresse als legitimer Absender ausgeben können. So kann ein Angreifer bei einem Missbrauch von ARP die IP-Adresse eines anderen Benutzers in einem lokalen Netz übernehmen und damit selbst Verbindungen herstellen oder die Erreichbarkeit des anderen Rechners vollständig verhindern. Auch Firewalls, die aufgrund von IP-Adressen entscheiden, ob eine Verbindung zulässig ist, lassen sich dadurch täuschen. Bei ICMP-Angriffen werden gefälschte Statusmeldungen verschickt, die beispielsweise eine Umleitung der Pakete über einen Router des Angreifers bewirken oder die gesamte Kommunikation eines Rechners nach außen verhindern (Denial of Service Attack). Der "Ping of Death" ist ein besonderer ICMP-Angriff, bei dem zu große Pakete beim Empfänger einen Überlauf des Empfangspuffers verursachen und den Rechner zum Absturz bringen. Ein ähnlicher Effekt wird bei vielen Windows-Rechnern durch das Senden spezieller Pakete (Out-of-Band [OOB]) bevorzugt auf den Port 139 erreicht. Gegen diesen Winnuke-Angriff können einige Windows-Versionen durch Patches geschützt werden.

Gegenmaßnahmen:
Installation von Patches,
starke Authentisierung

Durch den "TCP Syn Flood"-Angriff können ebenfalls Rechner blockiert werden. Dabei wird ein WWW-Server mit einer großen Anzahl von IP-Paketen mit ungültigen Absenderadressen bombardiert, auf die das System vergeblich zu antworten versucht. Dadurch kann der ganze Server über einen längeren Zeitraum lahmgelegt werden.

Gegenmaßnahmen:
Installation von Patches

2.3.2 Dienstespezifische Sicherheitsrisiken

2.3.2.1 E-Mail und Usenet-News

Elektronische Post (E-Mail) kann mitgelesen werden, sofern sie nicht verschlüsselt ist. E-Mails und News-Artikel ohne eine digitale Signatur lassen sich leicht verändern oder fälschen. Über den elektronischen Postweg können – wie bei einem Transfer per Diskette – Programme und Textdokumente mit Viren ins System gelangen. Selbst ein automatisches Durchsuchen der Nachrichten nach Viren bietet keinen vollständigen Schutz.

Gegenmaßnahmen:
Verschlüsselung und digitale Signatur,
Virenschutzsysteme

Sendmail, das auf UNIX-Rechnern am häufigsten eingesetzte Programm zum Verschicken elektronischer Post, wies lange Zeit eine ganze Reihe von Sicherheitslücken auf, die zu einer Zugangsmöglichkeit von Administratorrechten führen konnten. Mittlerweile steht sendmail mit der Version 8.10 zur Verfügung, in dem diese Sicherheitslücken beseitigt wurden. Auch nach der Installation dieser neuen sendmail-Version ist es jedoch sinnvoll, regelmäßig die Meldungen über neue sicherheitsrelevante Fehler zu verfolgen und gegebenenfalls entsprechende Patches einzuspielen.

2.3.2.2 Telnet

Ist der Telnet-Dienst nicht eingeschränkt, sondern von beliebigen Adressen aus zu beliebigen Ports auf dem eigenen Rechner möglich, wird die Zugangskontrolle gefährdet. Selbst wenn sich ein Angreifer keinen Zugang mit Administratorrechten verschaffen kann, gelingt es ihm häufig, einen nichtprivilegierten Account auf dem Rechner zu nutzen. Dieser Account kann dann als Ausgangsbasis für den Angriff auf weitere Rechner verwendet werden.

Gegenmaßnahmen:
Einschränkung der Telnet- und verwandten Dienste auf die notwendigen Adressen und Ports an einer Firewall

Mit Hilfe verschiedener Programme (z. B. das Cracker-Tool “Juggernaut”) können mittlerweile Telnet-Verbindungen “entführt” werden, d. h., der Angreifer

kann damit nicht nur Passwörter mitlesen, sondern auch in die Verbindung eingreifen, den ursprünglichen Benutzer abhängen und statt dessen sich selbst einklinken. Ähnliche Sicherheitsrisiken bestehen für "R-Utilities" wie rlogin.

Gegenmaßnahmen:
Vollständiger Verzicht auf den Telnet-Dienst sowie auf rlogin, rsh und rcp, statt dessen Verwendung von SSH (Secure Shell), einem Software-Paket, mit dem man durch anerkannte kryptographische Verfahren eine zuverlässige gegenseitige Authentisierung und eine transparente Verschlüsselung des gesamten Datenstroms erreichen kann. Dabei werden statt rlogin, rsh und rcp neue Programme ssh und scp eingesetzt. Das SSH-Paket steht für alle gängigen Betriebssysteme zur Verfügung (z. B. für UNIX: ftp://ftp.cs.hut.fi/pub/ssh/ oder ftp://ftp.cert.dfn.de/pub/tools/net/ssh; für Windows (kommerziell): http://www.europe.datafellows.com/f-secure/fssh-reg.htm).

2.3.2.3 FTP

Schlecht gewartete FTP-Server stellen ein Risiko dar, da in älteren Versionen bestimmter FTP-Server (ftpd) Sicherheitslücken existieren, die zur Erlangung von Administratorrechten führen können. Besondere Vorsicht ist geboten, da viele Beschreibungen zur Installation und Konfiguration von Anonymous-FTP-Servern sicherheitsrelevante Fehler enthalten. Bei Fehlkonfigurationen kann es einem Angreifer gelingen, die Datei mit den verschlüsselten Passwörtern aller Benutzer auf seinen Rechner zu laden und dort in aller Ruhe zu entschlüsseln. Lässt man zu, dass Benutzer eines FTP-Servers anonym eigene Dateien in Verzeichnissen ablegen können, wo andere sie sich holen können, kann sich der FTP-Server schnell zu einem Umschlagplatz von Raubkopien entwickeln.

Gegenmaßnahmen:
Ersatz des FTP-Dienstes (incl. rcp) durch Programme aus dem SSH-Paket (scp) oder Konfiguration eines SSH-Kanals mit Verschlüsselung und Authentisierung, Beschränkung durch Vergabe von entsprechenden Zugriffsrechten

2.3.2.4 WWW

Gefährdungen entstehen bei WWW-Servern durch fehlerhafte Software oder Konfigurationen. Ohne den Einsatz von SSL (Secure Socket Layer) oder anderen Verschlüsselungen lässt sich die Kommunikation abhören. Außerdem können Skripte zur dynamischen Generierung von Dokumenten Sicherheitslücken aufweisen.

Ende 1996 wurde die Angriffsmethode Web-Spoofing bekannt, bei der ein Angreifer seinen Server zwischen das eigentliche Zielsystem und den Rechner des Benutzers schaltet. Der Angreifer erstellt auf seinem System eine täuschend echte Kopie der Daten, die er komplett kontrollieren und für seine Belange modifizieren kann. Danach hat er nach Belieben die Möglichkeit, vom Benutzer verschickte Informationen abzufangen oder zu manipulieren.

Gegenmaßnahmen:
Verschlüsselung und digitale Signatur für die Kommunikation,
Zertifikate für Web-Server,
gegenseitige Authentisierung von Nutzer und Web-Server

2.3.2.5 DNS

Mit Hilfe des Domain Name Service (DNS) lassen sich Rechnernamen in IP-Adressen umsetzen und umgekehrt. Dabei besteht die Gefahr, dass Informationen über die Struktur des internen Netzes nach außen gelangen. Auch beim DNS gibt es mittlerweile die Angriffsmethode des Spoofing. Mit gefälschten Informationen im DNS können Datenströme in beliebige Bahnen gelenkt werden, wenn der Benutzer statt der numerischen IP-Adresse den leichter zu merkenden Rechnernamen angibt.

Gegenmaßnahmen:
Verbergen der Struktur des internen Netzes durch geeignete Anordnung von DNS-Servern,
Adressierung durch die numerische IP-Adresse, soweit praktikabel,
Einsatz eigener Domain Name Server

2.3.2.6 Finger

Die Daten, die der Finger-Dienst ausgibt, können einem Angreifer Informationen über die Nutzerkennungen auf dem System liefern, die gezielt für einen

Angriff genutzt werden können. Berühmt geworden ist dieser Dienst 1988 durch den so genannten Internet-Wurm. Dabei handelte es sich um ein Angriffsprogramm, das ausnutzte, dass die beim Aufruf von Finger übergebenen Parameter in einen Puffer fester Länge geschrieben wurden. Die Daten, die nicht mehr in den Puffer passten, überschrieben den Stack im Arbeitsspeicher, wo sie als Programmcode behandelt und ausgeführt wurden (Buffer Overflow Bug). Bei geschickter Wahl der übergebenen Zeichenreihe kann so beliebiger Code zur Ausführung kommen. Ähnliche Programmierfehler finden sich auch heute noch in vielen anderen Serverprogrammen.

Gegenmaßnahmen:
Abschalten der Dienste, über die sich Angreifer sicherheitsrelevante Informationen aus dem System beschaffen können: finger, rup, rusers, rwho, SMTP EXPN, SMTP VRFY,
Installation von Patches gegen den Buffer Overflow Bug

2.3.2.7 SNMP

Mit Hilfe des Simple Network Management Protocol-Dienstes können Netzwerkkomponenten von zentraler Stelle aus verwaltet werden. Dazu können Informationen über die Konfiguration und den Betriebszustand der Komponenten abgefragt und verändert werden. Dies bietet dem Angreifer u. U. wertvolle Hinweise über die eingesetzte Hard- und Software, die für weitergehende Attacken ausgenutzt werden können.

Besondere Bedeutung kommt dabei den sog. Community Strings zu, die eine einfache Form der Authentisierung bei SNMP darstellen. Häufig ist bei Auslieferung der Community String “public” eingestellt, der einen unberechtigten Zugriff auf den Dienst sehr erleichtert.

Gegenmaßnahmen:
Verwendung schwer zu erratender Community Strings,
jedenfalls nicht “public”
Begrenzung der von SNMP zur Verfügung gestellten Informationen auf das Erforderliche

2.3.3 Aktive Inhalte/Aktive Elemente

2.3.3.1 ActiveX

ActiveX ist eine Entwicklung der Firma Microsoft. Es steht für eine Reihe von Technologien, die dafür sorgen, dass Windows-Anwendungen mit dem Internet oder Intranet zusammenarbeiten. WWW-Seiten können mit dieser Technologie um eine Vielzahl von multimedialen Effekten, unterschiedlichen Layouts und ausführbaren Applikationen, die über das Internet geladen werden, erweitert werden. Die Technologie besteht im Wesentlichen aus folgenden Elementen: ActiveX-Controls, Active Documents und Active Scripting.

ActiveX-Controls sind Programme, die auf einer WWW-Seite dargestellt oder als eigene Programme aufgerufen werden können. Active Documents ermöglicht die Anzeige und Betrachtung von Nicht-HTML-Dokumenten (z. B. Word oder Excel) innerhalb eines Browsers. ActiveX Scripting ermöglicht das Verwalten und die Kommunikation von ActiveX-Controls, beinhaltet einen Java-Compiler und ist eine Umgebung zur serverseitigen Nutzung von ActiveX-Controls. Eine ActiveX-Sicherheitsarchitektur gibt es nicht. Die vorhandenen Sicherheitsmechanismen bieten kein in sich konsistentes Sicherheitssystem. Microsoft setzt auf die Nachvollziehbarkeit der Herkunft der heruntergeladenen Codes durch Codesignierung. Für die Codesignierung setzt Microsoft die selbstentwickelte Authenticode Technologie ein. Sie beruht auf einer digitalen Signatur und erlaubt neben der sicheren Identifikation des Absenders den Nachweis der Echtheit der übertragenen Codes. Dieses Verfahren macht aber keine Aussage über die Funktionsweise der Software selbst und ob sie gewollt oder ungewollt (Programmierfehler) schadensstiftende Wirkung entfalten kann.

Microsoft arbeitet mit der Firma Verisign als Zertifizierungsstelle zusammen und vergibt zwei unterschiedliche Zertifikate: Individualzertifikate und kommerzielle Zertifikate. Es existiert ein mehrstufiges Sicherheitssystem im Zusammenspiel von ActiveX und den unterschiedlichen Browsern. Neben der Möglichkeit, die ActiveX-Funktionalität (gilt für alle Browser) abzuschalten, besteht auch die Option, im Internet-Explorer einen Sicherheitslevel (hoch, mittel und niedrig) vorzugeben. Bei einem hohen Sicherheitslevel werden nur zertifizierte ActiveX-Controls akzeptiert. Bei einem mittleren Level müssen nicht zertifizierte ActiveX-Controls explizit freigegeben werden. Ein niedriger Level bietet gar keinen Schutz. Eine weitere Möglichkeit, sich zu schützen, bieten ActiveX-Filter, die Listen mit Servern definieren, von denen ActiveX-Komponenten akzeptiert werden. Der Einsatz des Internet-Explorer-Administration-Kit (IEAK) ermöglicht die Erstellung von spezifisch angepassten Internet-Explorern.

ActiveX-Komponenten stellen, da sie keinerlei Einschränkungen bzgl. der Windows- und System-Funktionalität unterliegen, ein immenses Sicherheitsrisiko dar. Folgende Sicherheitsrisiken sind bisher bekannt: Ausforschung von Nutzern und Computersystemen, Installieren und Ausführen von Viren und Trojanischen Pferden, Beschädigung von Systemressourcen und Überlasten des Systems. Aus Sicherheitsgründen empfiehlt es sich daher, die ActiveX-Unterstützung gänzlich abzuschalten.

Gegenmaßnahmen:
Abschalten der ActiveX-Unterstützung,
Verwendung des Microsoft-Authenticodes,
Aktivieren einer hohen Sicherheitsstufe im Internet-Explorer,
Einsatz von ActiveX-Filtern und des Internet-Explorer-Administration-Kits in Netzwerken

Abschließend sei noch auf die unzureichenden Sicherheitsmechanismen der Betriebssystemplattformen hingewiesen. Die Plattform Windows 95 verfügt über keinerlei eingebaute Sicherheitsmechanismen zur Abwehr von Angriffen, und unter Windows NT laufen ActiveX-Controls im Rechteraum (mit den Zugriffsrechten) des gerade angemeldeten Benutzers.

2.3.3.2 Java

Java ist eine objektorientierte Programmiersprache, die unabhängig von der jeweiligen Systemplattform nutzbar ist. Sie wurde von SUN Microsystems entwickelt. Java bietet die Möglichkeit, Stand-Alone-Anwendungen (Java-Applikations) sowie Anwendungen für das WWW (Java-Applets) zu schreiben. Java-Applets können in HTML-Seiten integriert, über das Internet angefordert und auf beliebigen Rechnern ausgeführt werden, ohne dass der Entwickler die lokale Umgebung des Anwenders kennen muss. Einzige Bedingung für die Lauffähigkeit ist die Verfügbarkeit der JVM (virtuelle Java Maschine) auf der Plattform. Java verfügt über ein integriertes Sicherheitssystem. Das Sandbox-System ist mehrstufig, bezogen auf die vier Softwareebenen, die bei der Herstellung und Ausführung von Java-Funktionen beteiligt sind:

1. Programmiersprache Java,
2. Virtuelle Java Maschine,
3. Lader für Java-Klassen und
4. Java Bibliotheken.

Ist JVM Bestandteil des HTML-Viewers, werden Applets ausgeführt, die sehr strengen Sicherheitskontrollen unterliegen. Applets, die über das Netz geladen werden, haben auf dem Client keine Lese- und Schreibrechte, können keine fremden Programme starten, keine Systemfunktionen aufrufen, keine Netzwerkverbindung zu anderen Rechnern aufbauen, keine zusätzlichen Bibliotheken laden und kennzeichnen Fenster besonders, die durch Applets gestartet wurden.

Applets können im Standardfall auch nur definierte Systemeigenschaften (z. B. Betriebssystem NT) lesen. SUN bietet in neueren Versionen die Möglichkeit, mit **signierten Applets** zu arbeiten. Die Applets werden zertifiziert und mit einer digitalen Signatur versehen, bevor sie im Netz zur Verfügung gestellt werden. Somit kann der Client die Authentifikation und die Herkunft prüfen. Die Signierung sagt nichts über die Funktionalität des Programmes. Die Java-Spezifikation bietet mit ihren durchdachten Mechanismen eine ausreichende Sicherheit, aber durch Implementierungsfehler wurden Angriffe durch Java-Applets möglich. Hier muss man unterscheiden zwischen Angriffen, die das System und seine Ressourcen modifizieren (durch Programmier- und Implementationsfehler in den Ablaufumgebungen), die eine weitere Nutzung des Systems verhindern (**Überlasten des Systems**) oder die Nutzer ausforschen oder belästigen.

Um sich vor Angriffen zu schützen, bieten sich mehrere Optionen an. Zusätzlich zu dem eigenen Sicherheitssystem können noch folgende Maßnahmen ergriffen werden. Man kann z. B. im Browser **die Java-Funktionalität abschalten**. Einen weiteren Schutz bieten **Java-Filter**, die Listen mit Servern definieren, von denen Java-Applets akzeptiert werden. In neueren Browser-Versionen ist das **Arbeiten mit signierten Applets** möglich.

Gegenmaßnahmen:
Abschalten der Java-Funktionalität, Einsatz von Java-Filtern, Arbeiten mit signierten Applets,
Verwendung von Browsern, bei denen JVM sauber implementiert ist

2.3.3.3 JavaScript

JavaScript ist eine von der **Firma Netscape Communication** entwickelte **Skriptsprache,** die plattformunabhängig ist. Sie wird direkt in die HTML-Seiten eingebettet und über einen Interpreter interpretiert und ausgeführt. Die Motivation für die Entwicklung von JavaScript waren die Unzulänglichkeiten der vorhandenen Techniken (HTML und CGI) für Benutzer-Interaktivitäten. Jede Interaktion musste an den Server gesendet werden, um mit Hilfe des CGI-Pro-

grammes Plausibilitätsprüfungen durchzuführen. Durch den Einsatz von JavaScript wurde die Anzahl der notwendigen Verbindungen zum Server drastisch verringert. Dynamisch zur Laufzeit können mit JavaScript beispielsweise Eingaben überprüft oder auch Berechnungen durchgeführt werden. Außerdem lassen sich wichtige Funktionen des Browsers, wie Öffnen und Schließen von Fenstern, Manipulieren von Formularelementen oder das Anpassen von Browser-Einstellungen, verwirklichen. Ein Zugriff auf Dateisysteme auf anderen Rechnern ist nicht möglich.

Netscape bietet die Möglichkeit, mit **zertifizierten JavaScript-Codes** zu arbeiten. Es wurden jedoch Sicherheitsprobleme in zwei Bereichen bekannt, zum einen in der **Ausforschung von Nutzern und Computersystemen** und zum anderen in der **Überlastung von Rechnern**. Hier muss man unterscheiden zwischen Angriffen, die das System und seine Ressourcen durch Programmierfehler und Implementierungsfehler in den Ablaufumgebungen modifizieren oder eine weitere Nutzung des Systems – vorsätzlich erzeugt oder ungewollt durch Programmierfehler – verhindern, und Angriffen, die das Lesen von fremden Nachrichten, Ändern von Nachrichten und Verschicken von Texten ermöglichen. Die meisten Sicherheitslöcher sind implementierungsabhängig.

Gegenmaßnahmen:
Arbeiten mit zertifizierten JavaScript-Codes oder das Abschalten der JavaScript-Funktionalität,
Verwendung von Browsern, bei denen die Anwendung sauber implementiert ist

2.3.3.4 Plug Ins

Browser Plug Ins sind auf dem Client laufende Software-Module, die den Funktionsumfang des Browsers erweitern und beispielsweise die Darstellung von Audio- und Videodaten erlauben. Plug Ins sind plattformabhängig, belegen lokalen Plattenspeicher und müssen vom Benutzer beschafft und installiert werden.

Gegenmaßnahmen:
Schulung der Benutzer, um unbeabsichtigtes Installieren der Software zu verhindern

2.3.3.5 Cookies

Cookies (engl. cookie = Keks) sind kleine Datenmengen, die zusammen mit den eigentlich angeforderten Daten aus dem Internet an den Computer des Benutzers übermittelt werden. Dort werden diese Daten gespeichert und für einen späteren Abruf bereitgehalten. Dadurch wird im einfachsten Fall ein wiederholter Zugriff eines bestimmten Benutzers (exakt: des Browsers auf dem Computer, den er verwendet) auf das Internet-Angebot erkennbar. Die Anwendungsmöglichkeiten gehen jedoch weit darüber hinaus.

Typischerweise werden Cookies eingesetzt, damit der Nutzer das Angebot des angewählten Webservers auf seine persönlichen Belange hin abstimmen kann, bzw. um dem Webserver zu ermöglichen, sich selbsttätig auf die (vermuteten) Bedürfnisse des Nutzers einzustellen. Ein Betreiber von WWW-Diensten kann jedoch aus geeignet gewählten und eingerichteten Cookies ein Nutzungsprofil erstellen, das vielfältige Auskunft über den Benutzer gibt und ihn so als geeignete Zielperson (z. B. für Werbebotschaften) identifiziert. Eine Manipulation des Computers über die Speicherung und Abfrage der Cookie-Daten hinaus ist mit dem Cookie-Mechanismus selbst nicht möglich. Da die Cookie-Informationen, die auch benutzerbezogene Passwörter für Web-Seiten umfassen können, jedoch in einer Datei im Dateisystem auf dem Rechner gespeichert werden, kann ein Unberechtigter beispielsweise mit Hilfe von ActiveX-Controls (siehe Abschnitt 2.3.3.1) darauf zugreifen.

Problematisch sind Cookies trotz dieses vergleichsweise geringen Gefährdungspotentials für die Computersicherheit aufgrund ihrer geringen Transparenz für den Benutzer. Der Datenaustausch mittels Cookies erfolgt zwischen den beteiligten Computern vollkommen im Hintergrund, ohne dass der Benutzer über Inhalte, Zweck, Umfang, Speicherdauer oder Zugriffsmöglichkeiten auf die Cookie-Daten informiert wird, sofern er keine besonderen Maßnahmen ergreift. Diese Parameter sind innerhalb der Cookies selbst festgelegt und werden somit allein vom Betreiber des WWW-Servers bestimmt; der Internet-Nutzer hat hierauf im normalen Betrieb keinen Einfluss. Es hängt wesentlich von der Initiative des Nutzers und seiner technischen Kenntnis und Ausrüstung ab, ob er Cookies bemerkt und sich ggf. vor ihnen schützen kann.

Gegenmaßnahmen:
Konfiguration des Browsers, so dass Cookies nicht oder wenigstens nicht automatisch akzeptiert werden und Cookies, die gespeichert werden sollen, angezeigt werden, Löschen bereits gespeicherter Cookies (z. B. Datei cookies.txt bei Netscape-Browsern), Einsatz von Cookie-Filtern

3 Firewall-Systeme

3.1 Grundlagen

Soll ein Verwaltungsnetz an das Internet angeschlossen werden, so kann dies entweder durch einen zentralen oder durch mehrere dezentrale Zugänge erfolgen. Aus Sicherheitsgründen ist für ein (Teil-) Netz mit einheitlichem Schutzbedarf ein zentraler Zugang vorzuziehen. Die durch die Anbindung hervorgerufenen Sicherheitsrisiken lassen sich durch Einsatz einer Firewall reduzieren.

Unter einer Firewall ("Brandschutzmauer") wird eine Schwelle zwischen zwei Netzen verstanden, die 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 Netzes (hier: des Verwaltungsnetzes) vertrauenswürdiger sind als die Teilnehmer des externen Netzes (hier: 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 (Policy-Enforcer).

3.1.1 Charakteristika von Firewall-Systemen

Firewalls weisen die folgenden Charakteristika auf:

- Die Firewall ist die definierte und kontrollierte Schnittstelle zwischen dem zu schützenden und dem nicht vertrauenswürdigen Netz.
- Im internen Netz besteht jeweils ein einheitliches Sicherheitsniveau. Eine weitere Differenzierung nach Sicherheitsstufen geschieht – zumindest auf der Ebene des Netzes – nicht.
- Die Firewall setzt eine definierte Sicherheitspolitik (**Security Policy**) für das zu schützende Netz voraus; in diese müssen die Anforderungen aller vernetzten Stellen einfließen.
- Es besteht die Notwendigkeit, die Benutzerprofile der internen Teilnehmer, die mit Rechnern in dem externen Netz kommunizieren dürfen, auf die Firewall abzubilden.

Die Stärke der Firewall hängt wesentlich von der eingesetzten Technik und ihrer korrekten Administration ab; entscheidend für die Sicherheit sind jedoch auch die Staffelung und die organisatorische Einbindung von Firewalls in die EDV-Infrastruktur.

3.1.2 Schutzniveau

Von besonderer Relevanz ist es, für den von einer Firewall geschützten Bereich das erforderliche Schutzniveau zu definieren. Diese Anforderung kann mit drei Lösungsvarianten erfüllt werden:

1. einheitlich hohes Schutzniveau im internen Netz, d. h. Orientierung am höchsten vorhandenen Schutzbedarf;
2. einheitlich niedriges Schutzniveau, d. h. Orientierung am niedrigsten vorhandenen oder an einem insgesamt geringen oder mittleren Schutzbedarf;
3. einheitlich niedriges Schutzniveau sowie Durchführung zusätzlicher Maßnahmen zum Schutz von Netzkomponenten mit höherem Schutzbedarf.

Die Varianten 1 und 2 entsprechen am ehesten zentralen Firewall-Lösungen, wobei angesichts der Sensibilität der in der Verwaltung verarbeiteten Daten Variante 2 indiskutabel und mit den Anforderungen des Datenschutzrechts unvereinbar sein dürfte. Variante 3 führt zur Lösung gestaffelter Firewalls, d. h. zu einer Konstellation, bei der neben einer zentralen, den mittleren Schutzbedarf abdeckenden Firewall (die u. a. die interne Netzstruktur nach außen sichert) bereichsbezogen und bedarfsorientiert Firewall-Anschlüsse mit unterschiedlichem Sicherheitsniveau implementiert werden können. Allerdings können selbst bei einheitlich hohem Schutzniveau im Gesamtnetz gestaffelte Firewalls sinnvoll sein, um den möglichen Schaden, der mit Sicherheitsverletzungen verbunden ist, auf ein Netzsegment zu begrenzen. Dies gilt insbesondere auch für die Abwehr von internem Missbrauch.

3.2 Firewall-Technologien

Eine Firewall kann durch verschiedene Konzepte realisiert werden. Im Wesentlichen unterscheidet man folgende Grundkonzepte:

- Packet Filter (Packet Screen, Screening Router)
- Application Level Gateway (Dual-homed Gateway)
- Stateful Inspection (Stateful Packet Filter, Dynamic Packet Filter)

Ein **Packet Filter** (auch **Packet Screen** oder **Screening Router**) ist ein Router, der IP-Pakete zur Unterscheidung zwischen der erlaubten und der unerlaubten Nutzung von Kommunikationsdiensten filtert. Packet Filter können nach Quell-

und Zieladresse sowie nach Quell- und Zielport filtern. Damit ist sowohl einschränkbar, welche Rechner im zu schützenden und welche im unsicheren Netz an der Kommunikation beteiligt sein dürfen, als auch, welche Kommunikationsdienste erlaubt sind. Die Filterregeln sind an die Netzschnittstellen gebunden. Sie werden vom Packet Filter in der Reihenfolge abgearbeitet, in der sie angegeben sind.

Ein **Application Level Gateway** ist ein speziell konfigurierbarer Rechner, über den die gesamte Kommunikation zwischen dem zu schützenden und dem unsicheren Netz stattfindet. Ein Application Level Gateway arbeitet im Gegensatz zum Packet Filter auf der Anwendungsschicht, d. h., die Kontrolle der Kommunikationsbeziehungen findet auf Anwendungsebene statt. Für jeden Dienst (Telnet, FTP usw.) werden **Security Proxys** eingeführt, die den direkten Zugriff auf den Dienst verhindern. Hierbei bestehen z. B. die Möglichkeiten einer ausführlichen Protokollierung (Audit) und einer benutzerbezogenen Authentisierung für die unterschiedlichen Dienste. Die meisten Application Level Gateways sind nicht in der Lage zu unterscheiden, über welche Netzschnittstelle ein Paket hereinkommt. Ein Application Level Gateway mit zwei Netzschnittstellen wird **Dualhomed Gateway** genannt.

Die Kombination von Packet Filter und Application Level Gateway wird als **Screened Gateway, Transparent Application Gateway** oder **Sandwich-System** bezeichnet und erhöht die Sicherheit der Firewall gegenüber den beiden Einzelkomponenten erheblich. Die Anordnung der beteiligten Komponenten kann variieren und erlaubt die individuelle Realisierung eines Firewall-Konzeptes.

Stateful Inspection (auch **Stateful Packet Filter** oder **Dynamic Packet Filter**) ist eine recht neue Firewall-Technologie und arbeitet sowohl auf der Netz- als auch auf der Anwendungsschicht. Die IP-Pakete werden auf der Netzschicht entgegengenommen, von einem Analysemodul, das dynamisch im Betriebssystemkern geladen ist, zustandsabhängig inspiziert und gegenüber einer Zustandstabelle abgeglichen. Die Regeln, nach denen das Modul agiert, können sehr differenziert vorgegeben werden. Für die Kommunikationspartner stellt sich eine Firewall mit Stateful Inspection als eine direkte Leitung dar, die nur für eine den Regeln entsprechende Kommunikation durchlässig ist. Im Out-Of-Band-Betrieb erfolgt die Wartung und Konfiguration nicht über TCP/IP. Die Firewall besitzt dann keine eigene IP-Adresse, so dass keine Möglichkeit besteht, sie über TCP/IP direkt aus

den angeschlossenen Netzen anzusprechen oder auf diesem Wege anzugreifen. Optional führt die Firewall ein Rewriting durch, d. h., Pakete werden vor dem Weitersenden nach vorgegebenen Regeln transformiert.

Stateful Inspection vereinigt bereits konzeptuell die Schutzmöglichkeiten von Packet Filter und Application Level Gateway, so dass diese beiden Funktionen nicht in getrennten Komponenten realisiert werden müssen. Experten streiten sich darüber, welches Konzept in welcher Realisierung mehr Sicherheit mit sich bringt. Inzwischen werden auch hybride Firewalls angeboten, die zusätzlich zur Stateful Inspection wie beim Application Gateway Proxys zur Verfügung stellen.

	Vorteile	**Nachteile**
Packet Filter (Router oder Rechner mit spezieller Software)	leicht realisierbar, da von vielen Routern angeboten leicht erweiterbar für neue Dienste Router auf dem Markt verfügbar Transparenz für den Benutzer Arbeitsgeschwindigkeit	Übernahme des Packet Filter durch einen Angreifer führt zu einem vollständigen Verlust der Sicherheit es ist bei den meisten Produkten nicht möglich, Dienste nur für bestimmte Benutzer zuzulassen alle Dienste, die erlaubt sind und erreicht werden können, müssen sicher sein Protokollierung nur auf unteren Netzschichten möglich keine Authentisierung möglich
Dual-homed Gateway (Application Level Gateway mit zwei Netzschnittstellen)	kein Paket kann ungefiltert passieren aussagekräftige Protokollierung auf höheren Schichten möglich interne Netzstruktur wird verborgen durch den Einsatz von Network Address Translation (NAT)	Übernahme des Gateways durch einen Angreifer führt zu einem vollständigen Verlust der Sicherheit keine Transparenz für den Benutzer Probleme bei neuen Diensten, schlechte Skalierbarkeit

Screened Gateway (Anordnung aus Application Level Gateway mit einem oder zwei Packet Filtern (Teilnetz-Bildung))	kein direkter Zugang zum Gateway möglich interne Netzstruktur wird verborgen Network Address Translation (NAT) vereinfachte Regeln durch 2. Filter durch Einsatz mehrerer Gateways lässt sich die Verfügbarkeit steigern aussagekräftige Protokollierung möglich	keine Transparenz für den Benutzer bei Realisation mit mehreren Rechnern und Routern: erhöhter Platzbedarf Probleme bei neuen Diensten, schlechte Skalierbarkeit
Stateful Inspection (Firewall-Rechner mit zustandsabhängiger Analyse und Reaktion)	gute Skalierbarkeit arbeitet auf Netz- und Anwendungsschicht Out-Of-Band-Betrieb: keine Angriffsmöglichkeit über TCP/IP interne Netzstruktur wird verborgen Rewriting möglich (über NAT hinaus) umfangreiche Authentisierungsvarianten	Übernahme des Gateways durch einen Angreifer führt zu einem vollständigen Verlust der Sicherheit keine Zwischenspeicherung, daher nicht volle Gateway-Funktionalität und kein Caching schneller Rechner erforderlich, da wegen der umfangreichen Analyse und Aktionsmöglichkeiten sonst Performance-Einbußen

3.3 Firewall-Architekturen

Neben den im Folgenden dargestellten Architekturen von Firewalls sind auch Abwandlungen oder Kombinationen der Anordnungen möglich.

3.3.1 Zentrale Firewalls

Rein zentrale Firewall-Lösungen (vgl. Abbildung 3.1) sind durch folgende Aspekte charakterisiert:

- Die zentrale Firewall bildet die einzige Schnittstelle (Choke Point) zwischen dem kompletten zu schützenden Verwaltungsnetz und dem übrigen Internet.

- Innerhalb des gesamten Verwaltungsnetzes besteht ein einheitliches Sicherheitsniveau; eine weitere Differenzierung nach Sicherheitsstufen erfolgt nicht.
- Eine Kontrolle der internen Verbindungen durch die Firewall ist nicht möglich.
- Die zentrale Firewall setzt eine definierte Sicherheitspolitik für das gesamte Verwaltungsnetz voraus. Abweichende Sicherheitspolitiken für besonders schützenswerte Bereiche sind auf Netzebene nicht durchsetzbar.
- Es besteht die Notwendigkeit einer zentralen Benutzerverwaltung. Für jeden Teilnehmer muss sowohl auf Dienstebene als auch bezogen auf die zugelassenen Adressen die zulässige Kommunikation festgelegt werden.

Da eine zentrale Firewall eine Differenzierung nach Teilnetzen nicht unterstützt und dementsprechend ein einheitliches Sicherheitsniveau für das gesamte Verwaltungsnetz voraussetzt, muss sich der Grad des gewährleisteten Schutzes nach den sensibelsten Daten richten und ist dementsprechend hoch. Dies hat jedoch für Verwaltungsbereiche mit weniger sensiblen Daten den Nachteil, unnötig hohe Schranken zu errichten. Daraus ergibt sich die Gefahr, dass gerade von diesen Stellen zusätzliche Internet-Zugänge mit geringeren Restriktionen geschaffen werden, wodurch der gesamte Zweck der Firewall ad absurdum geführt wird.

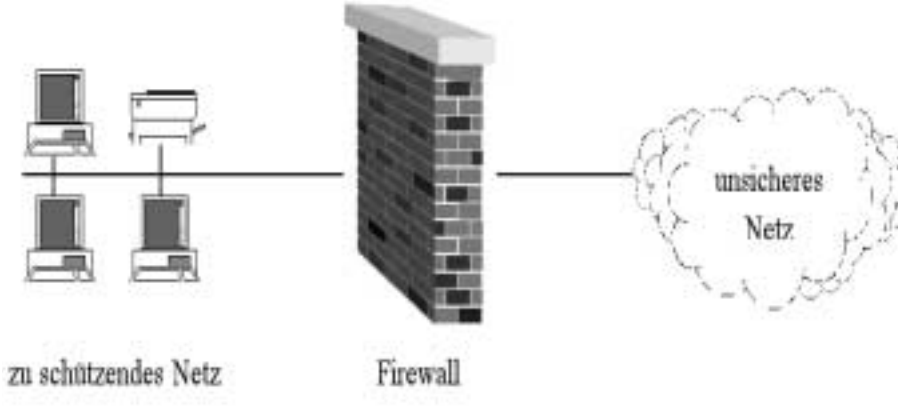


Abbildung 3.1: Zentrale Firewall-Anordnung

Ein weiterer Nachteil zentraler Firewalls besteht in dem – auch aus dem Großrechnerbereich bekannten – Problem, dass eine Benutzerverwaltung, die fernab von dem jeweiligen Fachbereich erfolgt, häufig zu Abweichungen zwischen der Realität von Benutzerrechten und deren Abbildung in Form von Accounts führt.

Da eine Firewall Zugriffe innerhalb des internen Netzes nicht kontrolliert, besteht bei rein zentralen Lösungen die Gefahr, dass das gesamte Verwaltungsnetz als eine Einheit betrachtet wird und insofern nur die Zugriffe von oder nach außen restringiert werden. Dieser Aspekt ist zwar nur mittelbar Teil des Themas "Internet-Anbindung", muss bei einer Gesamtbetrachtung von Netzsicherheit jedoch unbedingt einbezogen werden.

Der Einsatz einer alleinigen zentralen Firewall ist allenfalls dann vertretbar, wenn alle angeschlossenen Teilnetze über ein gleiches Sicherheitsbedürfnis bzw. -niveau verfügen und zudem nicht die Gefahr des internen Missbrauchs besteht. Davon kann in behördenübergreifenden Verwaltungsnetzen mit einer Vielzahl angeschlossener Rechner jedoch nicht ausgegangen werden.

3.3.2 Gestaffelte Firewalls

Gestaffelte Firewall-Lösungen (vgl. Abbildung 3.2) sind durch folgende Aspekte charakterisiert:

- Es handelt sich um eine Kombination zentraler und dezentraler Komponenten, wobei durch eine zentrale Firewall ein Mindestschutz für das Gesamtnetz gegenüber dem Internet realisiert wird und dezentrale Firewalls in Subnetzen mit besonderem Schutzbedarf ein angemessenes Schutzniveau sicherstellen.
- Innerhalb des jeweiligen geschützten Subnetzes besteht jeweils ein einheitliches Sicherheitsniveau.
- Eine Kontrolle der verwaltungsinternen Verbindungen ist möglich, sofern die Kommunikation den durch dezentrale Firewalls geschützten Bereich überschreitet.
- Auch ein gestaffeltes Firewall-System setzt eine definierte Sicherheitspolitik für das Gesamtnetz voraus. Bei ihrer Definition müssen insbesondere die Anforderungen an einen zu garantierenden Grundschutz einfließen. Darüber hinaus sind für die Subnetze gesonderte Sicherheitsanforderungen zu definieren.
- Die Benutzerverwaltung kann weitgehend dezentralisiert werden. Allerdings sind einheitliche Regeln festzulegen, nach denen Benutzer das Recht haben, über die zentrale Firewall mit Systemen im Internet in Verbindung zu treten.
- Auch die dezentralen Firewalls müssen qualifiziert administriert werden.

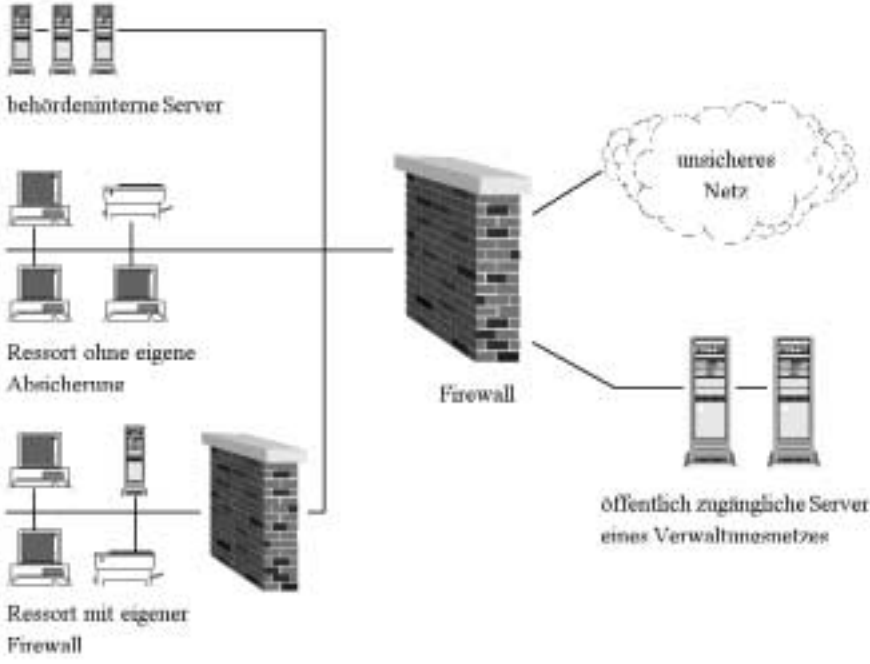


Abbildung 3.2: Gestaffelte Firewall-Anordnung

Für die dezentralen Firewalls bieten sich prinzipiell die gleichen Technologien wie bei einer zentralen Firewall an. Die Kombination zentraler und dezentraler Schutzmechanismen erlaubt die Realisierung des Prinzips eines autonomen Schutzes; bei sorgfältiger Konfiguration bleiben besonders geschützte Subnetze auch dann gesichert, wenn die zentrale Firewall durch einen Eindringling überwunden wurde.

Mit gestaffelten Firewalls kann – anders als bei zentralen Lösungen – das datenschutzrechtlich bedeutsame Prinzip der informationellen Gewaltenteilung abgebildet werden, mit dem es nicht zu vereinbaren wäre, wenn die Verwaltung als informatorisches Ganzes betrachtet würde. Die Teilnetze können sowohl gegen Angriffe von außen – aus dem Internet – als auch untereinander abgeschottet werden. Da gestaffelte Lösungen besser als ausschließlich zentrale Firewalls die Anforderungen der Benutzer abbilden können, ist auch die Gefahr der Umgehung der kontrollierten Schnittstellen durch Schaffung "wilder" Internet-Zugänge geringer. Zudem würden sich die Folgen derartiger Verstöße gegen die festgelegte Sicherheitspolitik besser isolieren lassen.

Auch gestaffelte Firewalls sind mit einem insgesamt hohen Administrations- und Pflegeaufwand verbunden, der jedoch auf die zentrale Firewall und die dezentralen Firewalls verteilt ist. Die Festlegung der individuellen Benutzerrechte kann dabei im Wesentlichen den anwendernäheren dezentralen Firewalls zugeordnet werden.

3.3.3 Entmilitarisierte Zone

Server, die Dienste für Internet-Nutzer zur Verfügung stellen (z. B. WWW oder Mail), werden häufig hinter einer Firewall in der so genannten **entmilitarisierten Zone (DMZ, Demilitarized Zone,** auch **Screened Subnet**) eingerichtet, von der das interne Netz durch eine (weitere) Firewall abgeschottet ist. Dies hat den Vorteil, dass das lokale Netz auch dann noch geschützt ist, wenn ein Angreifer bis zum WWW-Server gelangt.

Die entmilitarisierte Zone kann beispielsweise zwischen zwei Firewalls realisiert werden (vgl. Abbildung 3.3). Durch Verwendung unterschiedlicher Firewall-Produkte lässt sich dabei eine höhere Sicherheit erreichen, da mögliche Fehlfunktionen bei unabhängiger Entwicklung der Produkte wahrscheinlich nicht gleichzeitig auftreten.

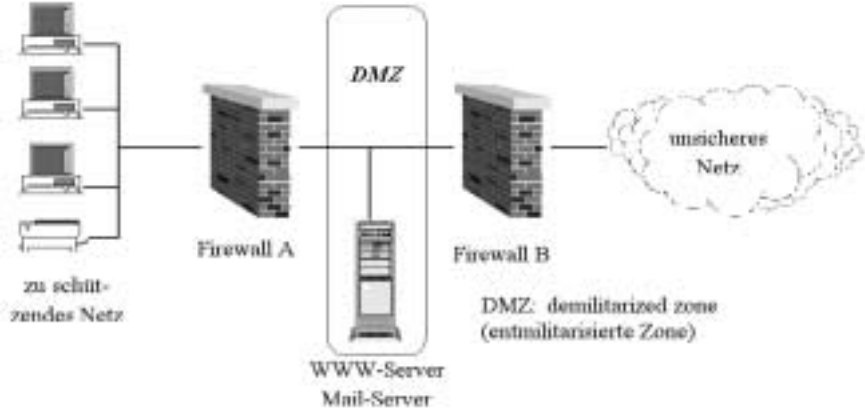


Abbildung 3.3: Kaskadierte Firewall-Anordnung mit DMZ

Die Aufgaben der beiden Firewalls können auch von nur einer Firewall mit mehreren Schnittstellen übernommen werden, mit denen sich mehrere Netze mit

unterschiedlicher Sicherheit bilden lassen. So können auch eine oder mehrere entmilitarisierte Zonen eingerichtet werden. Diese Lösung ist kostengünstiger, verzichtet aber auf die erhöhte Sicherheit.

3.3.4 Screened Gateway

Zumeist werden neben der Firewall Router eingesetzt, die oft die Funktion von Packet-Filtern übernehmen können. Damit lässt sich eine “Sandwich-Lösung” (vgl. Abbildung 3.4) realisieren, die durch Verwendung unterschiedlicher Systeme eine erhöhte Sicherheit gewährleisten kann. Auch hier ist die Einrichtung einer entmilitarisierten Zone möglich.

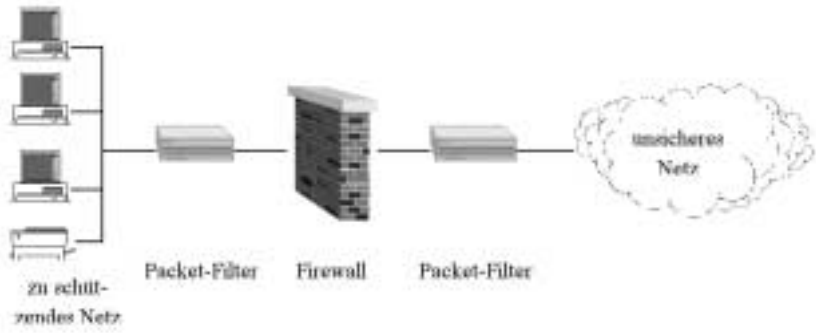


Abbildung 3.4: Screened Gateway (Sandwich-System)

Die Anordnung von Mail-, WWW- und DNS-Servern bei Sandwich-Systemen mit entmilitarisierten Zonen wird in der folgenden Abbildung beispielhaft veranschaulicht:

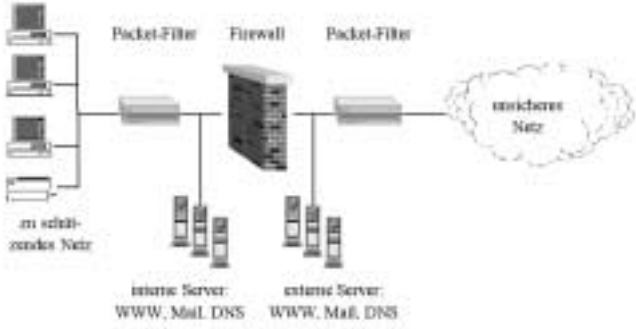


Abbildung 3.5: Screened Gateway (Sandwich-System) mit DMZ

4 Zulässigkeit von Protokollierung und Inhaltskontrolle mittels einer Firewall

4.1 Allgemeines

Firewalls sind selbst keine eigenständigen Telekommunikations-, Tele- oder Mediendienste, sondern als unselbständiger Bestandteil eines solchen Dienstes zu betrachten. Daher kommt für den Betrieb einer Firewall das Datenschutzrecht zur Anwendung, das auch für den zu Grunde liegenden Dienst gilt. Deshalb sollen im Folgenden kurz die Anwendungsbereiche der für die Dienste einschlägigen Datenschutzvorschriften erläutert werden.

Das Verhältnis zwischen Telekommunikationsdiensten einerseits und Tele- bzw. Mediendiensten andererseits wird grundsätzlich durch die in § 2 Abs. 1 Teledienstegesetz (TDG)/§ 2 Mediendienste-Staatsvertrag (MDStV) enthaltenen Begriffsdefinitionen beschrieben. Danach handelt es sich bei einem Teledienst um einen elektronischen Informations- und Kommunikationsdienst, der für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt ist und dem eine **Übermittlung mittels Telekommunikation** zu Grunde liegt. Mediendienste sind solche elektronischen Informations- und Kommunikationsdienste, die an die Allgemeinheit gerichtet sind.

Ausgehend von diesen gesetzgeberischen Vorgaben kann die Beziehung zwischen Telekommunikations- und Tele- bzw. Mediendiensten durch ein Schichtenmodell beschrieben werden. Dabei stellt die Telekommunikation die Transportebene dar, auf deren technischer Basis der jeweilige Tele- bzw. Mediendienst erfolgt. Das hierfür maßgebliche datenschutzrechtliche Rechtsregime wird durch die einschlägigen Vorschriften des Telekommunikationsgesetzes (TKG) sowie der Telekommunikations-Datenschutzverordnung (TDSV) bestimmt. Zusätzlich greifen nachrangig die Regelungen des allgemeinen Datenschutzrechts (Bundesdatenschutzgesetz (BDSG), Landesdatenschutzgesetze). Um im Bild zu bleiben, handelt es sich bei den Tele-/Mediendiensten demgegenüber um die Transportbehälter. Für diesen Bereich sind das TDG sowie das Teledienstedatenschutzgesetz (TDDSG) bzw. der MDStV einschlägig. Schließlich muss noch eine dritte Ebene betrachtet werden, nämlich die durch bzw. mit den Tele-/Mediendiensten vermittelten – also in diesen Transportbehältern befindlichen – Inhalte. Die rechtliche Bewertung der Inhalte richtet sich nach den jeweiligen Gesetzen, wie etwa den Verwaltungsverfahrensgesetzen, dem Strafgesetzbuch, dem Gesetz gegen den unlauteren Wettbewerb, dem BDSG oder den Landesdatenschutzgesetzen.

Die Verarbeitung und Nutzung personenbezogener Daten auf der Transportebene wird in Umfang und Grenzen maßgeblich durch das Fernmeldegeheimnis (Art. 10 GG, § 85 TKG) geprägt, das die dabei anfallenden Verbindungsdaten und die Kommunikationsinhalte schützt. Nach § 85 Abs. 2 TKG sind alle zur Wahrung des Fernmeldegeheimnisses verpflichtet, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken. Entsprechend den einschlägigen Begriffsbestimmungen in § 3 TKG ist es dabei unerheblich, ob diese Dienste für die Allgemeinheit bestimmt sind oder nur einem bestimmten Kreis von Berechtigten gegenüber angeboten werden. Ohne Bedeutung ist auch, ob Telekommunikationsdienste mit oder ohne Gewinnerzielungsabsicht erbracht werden. Durch diesen weiten Anwendungsbereich soll ein umfassender Schutz des Fernmeldegeheimnisses gewährleistet werden. Vor diesem Hintergrund muss beispielsweise auch eine Behörde, die ihren Mitarbeitern die private Nutzung der vorhandenen Telekommunikationsanlage erlaubt, als Telekommunikationsdiensteanbieter mit all den sich daraus ergebenden Verpflichtung beurteilt werden. Auch die bei Tele- und Mediendiensten entstehenden Nutzungsdaten unterliegen dem Schutz durch das Fernmeldegeheimnis, weil diese Dienste definitionsgemäß auf Grundlage der Telekommunikation abgewickelt werden.

Bei der Protokollierung sind deshalb nicht nur die Bestimmungen des TDDSG bzw. des MDStV, sondern auch das Fernmeldegeheimnis und ggf. einschlägige Bestimmungen über kommunizierte Inhalte (z. B. Arzt- oder Sozialgeheimnis) zu beachten. Betroffen von einer Protokollierung durch Firewalls sind in erster Linie die Bediensteten oder Arbeitnehmer der Stelle, deren Datenverarbeitungsanlage von der Firewall geschützt werden soll, im Fall der E-Mail-Kommunikation und bei interaktiven Angeboten aber auch die externen Kommunikationspartner. Bei Angriffen auf die Firewall können zudem personenbezogene Daten der Angreifer registriert werden.

Hinsichtlich des Umfangs und der Zulässigkeit der Protokollierung von Zugriffen, die über eine Firewall erfolgen, und der Kontrolle von Inhaltsdaten lassen sich die im Folgenden beschriebenen Fallkonstellationen unterscheiden.

4.2 Kontrolle von Inhaltsdaten bei E-Mail-Kommunikation

Die Frage nach der Zulässigkeit der Kontrolle von Inhaltsdaten wird insbesondere relevant bei eingehenden E-Mails, die nicht an die Mail-Adresse einer zentralen Poststelle, sondern an die Mail-Accounts einzelner Arbeitnehmer der betreffenden Dienststelle gerichtet sind. Hierbei können folgende Fallkonstellationen unterschieden werden:

4.2.1 Kontrolle auf Virenbefall mittels automatischem Virencheck

Sowohl bei dienstlicher als auch bei privater Nutzung bestehen grundsätzlich gegen eine Kontrolle auf Virenbefall mittels automatischem Virencheck keine Bedenken, soweit die Kontrolle ausschließlich automatisch erfolgt und die Kenntnisnahme von den Inhalten privater E-Mails durch Vertreter der Dienststelle (z. B. den Systemadministrator) nicht ohne Einwilligung des Benutzers erfolgt.

Dadurch kann allerdings eine dezentrale Überprüfung der Dateien auf Viren nicht bzw. nicht vollständig ersetzt werden, da Virencheckprogramme Viren, die in verschlüsselten E-Mails enthalten sind, nicht erkennen können. Mindestens für diese E-Mails muss daher nach der Entschlüsselung eine Virenüberprüfung beim Benutzer selbst erfolgen.

4.2.2 Kontrolle eingehender dienstlicher E-Mails

Wie bei herkömmlicher Post können Vorgesetzte sich auch eingegangene dienstliche E-Mails von den betreffenden Mitarbeitern vorlegen lassen. Der Arbeitnehmer hat auf Verlangen dem Arbeitgeber Ausdrucke der E-Mails auszuhändigen bzw. diesem den Zugang zu den E-Mails zu ermöglichen.

4.2.3 Kontrolle eingehender privater E-Mails

Soweit die private Nutzung des E-Mail-Dienstes gestattet ist, ist der Arbeitgeber insoweit als Anbieter von Telediensten einzuordnen und unterliegt damit in Bezug auf die Protokollierung den Vorschriften des Teledienstedatenschutzgesetzes (TDDSG) über die Verarbeitung personenbezogener Daten. Im Hinblick auf den Inhalt der privaten E-Mails der Beschäftigten hat er auch das Fernmeldegeheimnis nach § 85 Telekommunikationsgesetz (TKG) zu wahren. Daraus folgt insbesondere, dass es ihm untersagt ist, sich oder anderen über das für die Erbringung des Dienstes erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Die Weitergabe von Informationen, die dem Fernmeldegeheimnis unterliegen, ist strafbewehrt.

Wenn die private Nutzung von E-Mail zugelassen wird, ergibt sich die Notwendigkeit, dienstliche und private E-Mails zu trennen. Hat der Mitarbeiter eine personalisierte E-Mail-Adresse nach dem Muster “Vorname.Name@Behörde.de”, so kann nicht ausgeschlossen werden, dass eingehende Mails nicht an die Behörde, sondern an den Mitarbeiter privat gerichtet sind. Dieses Problem kann dadurch gelöst werden, dass den Beschäftigten für die dienstliche und die private Benutzung von E-Mail verschiedene E-Mail-Adressen zugewiesen werden.

Unabhängig vom Aufbau und von der Differenzierung der E-Mail-Adressen einer Behörde gilt, dass private E-Mails, die beim Posteingang fälschlich zunächst als dienstliche E-Mails angesehen wurden, so zu behandeln sind, wie bei der Behörde eingegangene, für einen Mitarbeiter bestimmte private Schreiben, deren privater Charakter nicht besonders, etwa durch den Zusatz “persönlich” gekennzeichnet ist. Sobald der private Charakter dieser E-Mails erkannt wurde, sind sie unverzüglich dem betreffenden Mitarbeiter zur alleinigen Kenntnis zu geben.

4.2.4 Kontrolle ausgehender E-Mails

Auch bei ausgehenden E-Mails kann die automatische Kontrolle auf Virenbefall sinnvoll sein. Zwar träfe der Schaden hier den Empfänger, dies kann allerdings eine Rufschädigung der absendenden Stelle zur Folge haben. Ausgehende private E-Mails sind genauso vom Fernmeldegeheimnis geschützt wie die eingehenden, so dass die inhaltliche Überprüfung ausscheidet.

Hinsichtlich ausgehender dienstlicher E-Mails gilt grundsätzlich das oben zu den eingehenden dienstlichen E-Mails Gesagte entsprechend. Die Vertreter der Dienststelle müssen feststellen können, welche Inhalte in dienstlichen E-Mails nach außen gelangt sind. Die Kontrolle der Inhalte durch die Vorgesetzten ist daher ohne weiteres zulässig. Darüber hinausgehend wäre es technisch durch den Einsatz entsprechender Auswertungsprogramme auch möglich, z. B. anhand der Absendezeiten und Länge der E-Mails oder mit der gezielten automatischen Suche nach darin verwendeten Begriffen eine umfassende Leistungs- und Verhaltenskontrolle zu bewirken. Der Einsatz derartiger Programme stellt allerdings einen weitgehenden Eingriff in das Persönlichkeitsrecht der Beschäftigten dar und ist daher lediglich in Ausnahmefällen und auch dann nur aufgrund einer Dienstvereinbarung zulässig.

4.3 Protokollierung von Internet-Zugriffen mittels einer Firewall

Für Art und Umfang der Protokollierung lassen sich vor allem zwei Szenarien unterscheiden:

- Die Firewall dient lediglich der Abschottung des internen Netzes gegen das Internet, Zugriffe von außen sind grundsätzlich nicht zugelassen. In diesem Szenario kommt die Protokollierung der zulässigerweise von innen erfolgenden Zugriffe der Mitarbeiter auf das Internet in Betracht. Dabei ist zwischen den Zugriffen bei dienstlicher und bei privater Nutzung zu unterscheiden. Außerdem kann die Protokollierung dazu dienen, den Versuch eines unzulässigen Zugriffs von außen rechtzeitig zu erkennen.
- In einem anderen Szenario geht es um Zugriffe von außen auf Komponenten des internen Netzes, die dafür grundsätzlich vorgesehen sind (z. B. Web-Server). Die selbstverständlich möglichen Mischformen bleiben der Einfachheit halber außer Betracht.

Ordnet man die Maßnahmen nach ihrer Zielrichtung, ergibt sich daraus folgendes Schema:

Abbildung 4.1: Protokollierung von Internetzugriffen

Soweit zur Aufrechterhaltung der Datensicherheit die Protokollierung erforderlich ist, stellt sich die Frage, wie lange die dabei erzeugten Logfiles aufbewahrt werden dürfen. Dies muss für den Einzelfall entschieden werden. Die Daten sind zu löschen, sobald sie für Zwecke der Datensicherheit nicht mehr erforderlich sind.

4.3.1 Protokollierung der von innen erfolgenden Zugriffe (Protokollierung von Mitarbeiterdaten)

Sämtliche Maßnahmen der Inhaltskontrolle und Protokollierung sind geeignet, die Beschäftigten einer Organisation zu überwachen und ihre Leistung und ihr Verhalten zu kontrollieren. In jedem Fall muss für die Betroffenen transparent sein, welche potenziell zur Überwachung ihres Verhaltens geeigneten Maßnahmen aktiviert sind. Derartige Maßnahmen unterliegen außerdem ohne Ausnahme der Mitbestimmung der gewählten Mitarbeitervertretungen (Personalrat bzw. Betriebsrat). Da – wie im Folgenden dargelegt wird – eine Reihe von Einzelfragen zu klären sind, bietet es sich an, zu diesen Themen eine Dienst- bzw. Betriebsvereinbarung abzuschließen.

Vorab ist festzuhalten, dass die Protokolldaten in allen Fällen den besonderen Zweckbindungsvorschriften des § 14 Abs. 4 BDSG bzw. der entsprechenden Vorschriften der Landesdatenschutzgesetze (z. B. § 11 Abs. 5 BlnDSG) unterliegen, soweit die Protokollierung der Aufrechterhaltung der Datensicherheit dient.

Grundsätzlich ist eine pauschale, flächendeckende und "vorbeugende" Protokollierung aller Internet-Zugriffe der Mitarbeiter zur Verhaltens- und Leistungskontrolle nicht erforderlich und damit unzulässig. Gleiches gilt auch bei der Nutzung eines Intranet. Hier sollte regelmäßig der Sperrung unerwünschter Angebote bzw. der Beschränkung des Zugriffs auf dienstlich erforderliche Angebote der Vorzug gegeben werden.

Für alle Kontrollmaßnahmen ergibt sich eine grundsätzliche Weichenstellung bei der Frage, ob den Nutzern die private Verwendung des dienstlichen Internetanschlusses erlaubt ist. Für den Dienstherrn bzw. Arbeitgeber besteht keine Pflicht, die private Nutzung zuzulassen. Ist die private Nutzung gestattet, so greift das Fernmeldegeheimnis nach § 85 TKG. Dieses umfasst den Inhalt der Telekommunikation und deren nähere Umstände (wer hat wann mit wem kommuniziert oder dies versucht?). Sämtliche Kontrollmaßnahmen sind dann nur noch unter sehr engen Voraussetzungen zulässig.

4.3.1.1 Dienstliche Nutzung

Beim Bereitstellen eines Internet-Zugangs für die ausschließlich dienstliche Nutzung handelt es sich nicht um einen Teledienst im Sinne des Teledienstegesetzes (TDG). Der Arbeitgeber bietet dem Arbeitnehmer keinen Dienst an, sondern stellt ihm lediglich ein Arbeitsmittel zur Verfügung; bei diesem "In-Sich-Verhältnis" fehlt das vom Teledienstegesetz vorausgesetzte Merkmal,

dass es sich bei Diensteanbieter und Nutzer um zwei unterschiedliche Rechtssubjekte handelt (vgl. § 3 TDG). Damit finden die Vorschriften des Teledienstedatenschutzgesetzes auf die Protokollierung der ausschließlich dienstlichen Nutzung von Telediensten keine Anwendung.

Zulässigkeit und Umfang der Protokollierung richten sich in diesen Fällen vielmehr nach den Vorschriften, die auf die Verarbeitung von Daten im jeweiligen Beschäftigungsverhältnis Anwendung finden, also z. B. nach dem jeweiligen Landesdatenschutz- bzw. Landesbeamtengesetz. Art und Umfang einer Protokollierung sollten durch eine Dienstvereinbarung geregelt werden.

Dagegen sollte die Protokollierung der dienstlichen Nutzung nicht auf die Einwilligung der Arbeitnehmer gestützt werden, da es auf Grund der Abhängigkeit im Beschäftigungsverhältnis häufig an der erforderlichen Freiwilligkeit der Einwilligung fehlt. Bei der dienstlichen Nutzung hat der Arbeitgeber grundsätzlich auch das Recht zu prüfen, ob das Surfen der Mitarbeiter im WWW tatsächlich vollständig dienstlich motiviert war. Allerdings gilt hier, wie bei der Kontrolle der ausgehenden dienstlichen E-Mails, dass eine automatisierte Vollkontrolle im Hinblick auf das Persönlichkeitsrecht der Beschäftigten auf erhebliche Bedenken stößt. In jedem Fall müssen die Beschäftigten auf die geplanten Überwachungsmaßnahmen und die drohenden Sanktionen ausdrücklich hingewiesen werden.

In der Regel geht es darum zu vermeiden, dass Mitarbeiter in der Arbeitszeit und unter Nutzung dienstlicher Ressourcen aus rein privatem Interesse auf Informationen zugreifen. Daher sollten nach Möglichkeit die bekanntesten Angebote (z. B. erotische Angebote, Spiele oder Börsenkurse) bereits gesperrt sein. Umgekehrt wäre es auch denkbar, die Zugriffe auf dienstlich erforderliche Angebote zu beschränken (Positivliste). Um weiteren Missbrauch zu verhindern, bietet es sich an, in einer Dienstvereinbarung datenschutzfreundliche Verfahren (z. B. stufenweise, zunächst nicht personenbezogene Protokollierung der Zugriffe) festzulegen.

4.3.1.2 Private Nutzung

Bei der privaten Nutzung eines vom Dienstherren zur Verfügung gestellten Internet-Zuganges handelt es sich um die Nutzung eines Teledienstes im Sinne des Teledienstegesetzes. Wenn der Arbeitgeber die private Nutzung gestattet, wird er damit zum Dienstanbieter im Sinne des § 3 des TDG. Art und Umfang der Protokollierung von Nutzungs- und Abrechnungsdaten richten sich nach § 6 des TDDSG. Außerdem gilt das Fernmeldegeheimnis aus § 85 TKG. Sind

bestimmte Protokollierungen aus technischer Sicht für die Aufrechterhaltung eines regelgerechten Firewall-Betriebs unabdingbar, können sie ergänzend auf § 9 BDSG nebst Anlage bzw. die entsprechenden Vorschriften der Landesdatenschutzgesetze gestützt werden.

4.3.2 Protokollierung der von außen (aus dem Internet) erfolgenden Zugriffe

4.3.2.1 Nur Anschluss des internen Netzes an das Internet; keine Angebote der öffentlichen Stelle nach außen

In diesen Fällen ist die Firewall nicht Bestandteil eines Tele- bzw. Mediendienstes. Die Vorschriften des Teledienstegesetzes bzw. des Teledienstedatenschutzgesetzes finden daher keine Anwendung. Zulässigkeit und Umfang der Protokollierung richten sich nach § 9 BDSG und Anlage. Für öffentliche Stellen des Bundes kommt als Rechtsgrundlage § 14 BDSG in Betracht; in den Ländern ggf. entsprechende Vorschriften der Landesdatenschutzgesetze.

4.3.2.2 Angebot nach außen (Web-Server)

Soll über eine Firewall der Zugriff aus dem Internet auf einen Web-Server einer öffentlichen Stelle reguliert werden, so bemisst sich die rechtliche Einordnung der Firewall nach der Einordnung des Angebotes, das die öffentliche Stelle auf dem betreffenden Web-Server macht. Dabei kann es sich – je nach Art des Angebotes – entweder um einen Teledienst im Sinne des Teledienstegesetzes handeln, aber auch um einen Mediendienst nach dem Mediendienste-Staatsvertrag (MDStV). Zulässigkeit und Umfang der Protokollierung von Nutzungs- und Abrechnungsdaten richten sich nach § 6 TDDSG bzw. § 15 MDStV. Für Zwecke der Datensicherung kann die Protokollierung auf § 9 BDSG und Anlage bzw. für öffentliche Stellen des Bundes ergänzend auf § 14 BDSG, in den Ländern auf entsprechende Vorschriften der Landesdatenschutzgesetze gestützt werden.

Die Protokollierung ist dabei auf das unabdingbar Notwendige zu begrenzen; der Anbieter unterliegt hier den Verpflichtungen zur datenarmen Gestaltung des Tele- bzw. Mediendienstes gemäß § 3 Abs. 4 TDDSG bzw. § 13 Abs. 5 MDStV.

Soweit die Protokollierung personenbezogen erfolgt, unterliegt der Anbieter darüber hinaus den Informationspflichten nach § 3 Abs. 5 TDDSG bzw. § 12 Abs. 6 MDStV auch hinsichtlich der Protokollierung personenbezogener Daten auf der Firewall. Soweit die Daten zur Gewährleistung der Datensicherheit oder

des Datenschutzes gespeichert werden, unterliegen sie der besonderen Zweckbindung nach § 14 Abs. 4 BDSG bzw. den entsprechenden Vorschriften der Landesdatenschutzgesetze (z. B. § 11 Abs. 5 BlnDSG).

Bei nach außen offenen Internet-Angeboten kann die Protokollierung an der Firewall nicht auf die Einwilligung des bzw. der Betroffenen gestützt werden, da eine rechtswirksame Einholung der Einwilligung von Betroffenen auf Grund der technischen Gegebenheiten im Internet nicht möglich ist.

5 Auswahl und Umsetzung der Sicherungsmaßnahmen; Betriebsphase

5.1 Security Policy und Sicherheitskonzept

Aus den Anforderungen der im Vorfeld gemachten Sicherheitsbetrachtungen der Kommunikations- und der Risikoanalyse ist ein Regelwerk zu erstellen. In dieser Security Policy sind die Rahmenbedingungen zur Einrichtung, zum Betrieb und zur Verwaltung der Systeme für die interne Kommunikation und die Verbindungen zum Internet festzulegen. Die Zuständigkeiten für Betrieb, Verwaltung und Administration der für den Verbund eingesetzten Kommunikationssyteme müssen aufeinander abgestimmt sein. Es müssen die notwendigen Maßnahmen aufgeführt werden, die dem Schutz nach innen und außen dienen. Bereiche mit sensiblen Datenbeständen müssen besonders berücksichtigt werden.

In Bezug auf die Firewall sollte die Security Policy folgende Festlegungen enthalten (vgl. [BSI]):

- Was soll geschützt werden?
- Welche Dienste sind erforderlich?
- Welche Benutzer werden zugelassen?
- Welche Ereignisse werden protokolliert, und wer wertet diese Daten aus?
- Welcher Datendurchsatz ist zu erwarten?

Da die Sicherheit des Gesamtsystems nicht allein von der Firewall bestimmt wird, sind in die Security Policy auch flankierende Vorgaben aufzunehmen, wie das Verbot von zusätzlichen Netzzugängen, z. B. per Modem oder ISDN, Virenschutz und Backup-Konzept. Basierend auf der Security Policy ist ein Sicherheitskonzept zu erstellen, welches die Vorgaben in konkrete Maßnahmen (Konfigurationen, Filterregeln etc.) umsetzt.

Voraussetzung für die Anbindung eines Behördennetzes an das Internet ist das Vorliegen einer schlüssigen Security Policy und eines davon abgeleiteten Sicherheitskonzepts sowie dessen konsequente Umsetzung. Die Internet-Anbindung darf nur erfolgen, wenn die Risiken durch technische und organisatorische Maßnahmen wirksam beherrscht werden können.

5.2 Auswahl, Konfiguration und Wartung von Firewall-Systemen

Firewall-Systeme müssen transparent und einfach aufgebaut sein. Mit zunehmender Komplexität steigt auch die Wahrscheinlichkeit von Fehlern. Nicht für den Betrieb der Firewall benötigte Anwendungen und Systemprogramme sind daher zu löschen. Auch die Bedienung und die Konfiguration der Firewall müssen benutzungsfreundlich realisiert sein, da sonst unbeabsichtigte Fehleinstellungen Sicherheitseinbußen mit sich bringen. Vertrauenswürdige Systeme müssen ihre Funktionsweise offen legen, denn nur dann ist es Experten möglich, Hintertüren auszuschließen und die Gefahr von Sicherheitslücken fundiert zu diskutieren. Sicherheitszertifikate für Firewalls können dazu beitragen, dass sich der Grad des Schutzes, den das jeweilige Produkt bietet, leichter einschätzen lässt und Vergleiche zwischen verschiedenen Produkten möglich werden.

Durch den Einsatz verschiedener Produkte, die unabhängig voneinander entwickelt wurden und arbeiten, lässt sich das Sicherheitsniveau steigern. "Monokulturen" sollten vermieden werden, denn wenn ein Angreifer einen bisher unentdeckten Fehler ausnutzt, kann dort leicht der gesamte Schutzwall zusammenbrechen. Bei der Konfiguration einer Firewall folgt man am besten der Regel: "Alles, was nicht ausdrücklich erlaubt ist, ist verboten." Wenn man bei der Definition der Regeln etwas übersehen hat, wird nur die Funktionalität und nicht die Sicherheit eingeschränkt. Während man eine Einschränkung der Funktionalität im Bedarfsfall schnell merkt, bleiben Einbußen in der Sicherheit oft unerkannt.

Es gibt keine 100%ige Sicherheit. Hinzu kommt, dass sich meist im Laufe der Zeit die Stärke der Sicherheit verringert, z. B. durch Entdeckung von Fehlern, Herausbildung neuer Angriffsformen oder auch Verbesserung der Systemausstattung von Angreifern. Unverzichtbar ist es daher, eine ausreichende und fortlaufende Betreuung des eingesetzten Firewall-Systems durch qualifiziertes Personal zu gewährleisten (vgl. auch [CheBel]). Die Administratoren sollten ständig die Diskussion um Sicherheitslücken verfolgen[2] und sich auch weiterbilden. Das Sicherheitsniveau des Firewallsystems ist regelmäßig neu zu bewerten, damit die Systeme auf den aktuellen Stand gebracht werden.

Treten neue Bedrohungen auf, so ist die Kommunikations- und Risikoanalyse entsprechend zu aktualisieren. Eine solche Anpassung ist auch notwendig, wenn beabsichtigt ist, bisher nicht vorgesehene Internetdienste zur Verfügung zu stellen. Die Firewallsoftware ist laufend zu aktualisieren. Falls notwendig, ist das Firewallsystem umzukonfigurieren, oder es sind einzelne Module oder die gesamte Firewall auch außerplanmäßig auszutauschen. Da nicht alle Angriffsversuche auf das lokale Netz von der Firewall vollständig abgeblockt werden können, ist durch die Systemadministration der laufende Betrieb der Firewall zu überwachen. Dazu müssen die Protokolle regelmäßig ausgewertet werden, um auch solche Angriffsversuche zu entdecken, die durch die Firewall nicht abgewiesen werden können. Es ist dafür zu sorgen, dass dringende Warnmeldungen der Firewall der Bedrohungslage angemessen konfiguriert sind. Ferner müssen diese Meldungen das Wartungspersonal unverzüglich erreichen und zeitnah behandelt werden.

Die Firewalladministration kann nicht losgelöst von der Verwaltung des (lokalen) Verwaltungsnetzes gesehen werden. Kommen beispielsweise Benutzerinnen und Benutzer hinzu, scheiden sie aus oder wechseln sie ihr Aufgabengebiet, so kann sich daraus eine Veränderung in den zur Verfügung zu stellenden Diensten ergeben. Dies erfordert eine entsprechende Aktivität der Firewalladministration. Umgekehrt hat die lokale Administration den Schwachstellen im lokalen Netz besondere Aufmerksamkeit zu schenken, die durch Angriffe von außen ausgenutzt werden können. Werden aufgrund der Größe oder Struktur der Verwaltungseinheit auch zwischen verschiedenen Teilen dieser Einheit Firewalls eingesetzt, so können bestimmte Aufgaben der Firewall-Administration sinnvoll zentralisiert werden. Insbesondere zählen dazu diejenigen Tätigkeiten, die unabhängig von der Rechteverwaltung der einzelnen Benutzerinnen und Benutzer sind.

5.3 Rahmenbedingungen für Konfiguration und Betrieb

Sind bereits für die Planung und Einführung eines Firewall-Systems[3] eine Vielzahl von Fragestellungen hinsichtlich technischer, organisatorischer, planerischer und rechtlicher Art zu beachten, kommen während der Betriebsphase weitere Problemkreise hinzu, die durch den Betreiber, ggf. in Abstimmung mit den Benutzern bzw. deren Personalvertretung, zu beantworten sind. Da die in diesem Zusammenhang zu treffenden Maßnahmen teilweise auch auf die Planungs- und Einführungsphase zurückwirken, sollte auch die Betriebsphase der Firewall

2 vgl. Hinweis zum CERT im Abschnitt “Weiterführende Informationen und Literatur”

3 Mit Firewall-System ist nicht nur die Firewall im eigentlichen Sinne, sondern auch das System, das den Zugang zum Internet ermöglicht, gemeint. So sollten auf der Firewall selbst keinerlei Accountingfunktionen laufen. Diese können aber im Zugangssystem integriert sein.

bereits frühzeitig berücksichtigt werden. Die rechtlichen Rahmenbedingungen ergeben sich aus Kapitel 4.

Typische Anforderungen während des Betriebs eines Firewall-Systems sind:

A1 Schutz des ordnungsgemäßen Betriebs der Firewall, d. h. der Durchlässigkeit für zugelassenen Netzverkehr einerseits und der Undurchlässigkeit für nicht zugelassenen Netzverkehr andererseits (eingehend oder ausgehend),
A2 Schutz des internen Netzes vor Angriffen von außen, sowohl bezogen auf online-Angriffe als auch auf offline-Angriffe (z. B. durch eingeschleuste Viren),
A3 Schutz vor einer unzulässigen bzw. rechtswidrigen Nutzung der Firewall, sei es von außen (z. B. Hacking) oder von innen (z. B. unerlaubte private Nutzung oder unzulässiger Zugriff auf für dienstliche Zwecke nicht erforderliche Informationsangebote),
A4 die rechtliche, organisatorische und technische Differenzierung zwischen der dienstlichen und der privaten Nutzung des Internet-Anschlusses, soweit eine außerdienstliche Nutzung überhaupt zugelassen wird,
A5 Abrechnung von Leistungen, die durch die Firewall erbracht werden,
A6 Statistische Auswertungen der Firewall-Benutzung, z. B. zur Angebotsoptimierung.

Um diese Anforderungen umzusetzen, stehen – im Wesentlichen unabhängig von der technischen Entwicklung oder einer rechtlichen Beurteilung – folgende technisch-organisatorische Maßnahmen zur Verfügung:

M1 Gestaltung der Netzzugangspolicy und der Betriebsparameter der Firewall allgemein,
M2 Auswertung der Inhalte übertragener Daten (z. B. hinsichtlich eines potentiellen Virenbefalls),
M3 Auswertung der Verbindungsdaten, insbesondere der URL (z. B. hinsichtlich Datenvolumen, Adressen).

Dabei ergibt sich grundsätzlich folgende Eignungsmatrix für die genannten Maßnahmen, wobei die rechtliche Zulässigkeit der jeweiligen Maßnahme im Einzelfall zu prüfen bleibt:

	A1	A2	A3	A4	A5	A6
M1	x	x	x	x	x	x
M2	-	x	x	x	-	-
M3	x	x	x	-	x	x

5.4 Empfehlungen für den Betrieb einer Firewall

Die nachfolgenden Empfehlungen gelten unabhängig davon, ob öffentliche Stellen selbst die Internet-Dienste anbieten oder ob sie sich dabei eines Providers bedienen.

- Aufgrund der rechtlich unterschiedlichen Bewertung der Datenübertragung für eigene Zwecke der Stelle einerseits und für Dritte andererseits sowie der damit verbundenen praktischen Konsequenzen sollte in einer Dienst- oder Betriebsvereinbarung klar geregelt werden, ob und wenn ja welche Dienste zur privaten Nutzung freigegeben sind.
- Im Hinblick darauf, dass bei behörden- und unternehmensinternen Systemen Mitbestimmungstatbestände erfüllt sind (Verhaltens- und Leistungskontrolle), müssen die Personalvertretungen und Betriebsräte schon bei der Planung und Einführung von Firewallsystemen und insbesondere der Protokollierung beteiligt werden. Gegebenenfalls müssen entsprechende Betriebs- oder Dienstvereinbarungen abgeschlossen werden, in denen das Verfahren der Protokollierung, der Kontrolle und der Auswertung der Protokolle verbindlich geregelt wird. Eine Einwilligung der Arbeitnehmer als Grundlage für die Protokollierung der dienstlichen Nutzung ist abzulehnen.
- Bei Datenübertragung für eigene Zwecke der Stelle sind die Mitarbeiter auf die Art und den Umfang technischer Kontrollen hinzuweisen, damit sie ihr Nutzerverhalten entsprechend steuern können; ferner müssen sie darüber informiert werden, welche Folgen es hat, wenn Nachrichten ausgefiltert werden.
- Zur Durchsetzung des Verbots einer privaten Nutzung oder des Zugriffs auf unerwünschte Adressen sollte grundsätzlich auf eine Protokollierung verzichtet werden. Die Durchsetzung dieses Verbots sollte soweit möglich durch die Beschränkung der Zugriffe auf dienstlich erforderliche Angebote (Positivliste) oder über die Sperrung der unerwünschten Adressen versucht werden. Zugriffsversuche auf gesperrte Adressen sollten protokolliert werden. Für erforderliche Protokollierungen sollte in der Dienstvereinbarung ein stufenweises, zunächst nicht personenbezogenes Verfahren festgelegt werden.
- Eine vollständige Protokollierung aller Internetzugriffe der Mitarbeiter zur Verhaltens- und Leistungskontrolle ist grundsätzlich nicht erforderlich und damit unzulässig.
- Die erlaubte private Nutzung des Internet-Zugangs unterliegt dem Fernmeldegeheimnis nach § 85 TKG. Für die Protokollierung gelten § 6 TDDSG

und § 9 BDSG. Sie darf danach grundsätzlich nur insoweit erfolgen, als es für die Abrechnung der Dienste oder zur Aufrechterhaltung eines regelgerechten Firewallbetriebs unerlässlich ist.

- Die Protokollierung der von außen (aus dem Internet) erfolgenden Zugriffe oder Zugriffsversuche, die einen Angriff darstellen, ist im Rahmen von §§ 9, 14 BDSG bzw. der entsprechenden Normen der Landesdatenschutzgesetze zulässig. Darüber hinaus ist eine derartige Protokollierung auch erlaubt, wenn sie zum Erkennen potentieller Angriffe erforderlich ist.
- Für die Protokollierung der Zugriffe von außen auf Informationsangebote für die Öffentlichkeit gelten – in Abhängigkeit von der Art des Dienstes – § 6 TDDSG bzw. § 15 MDStV hinsichtlich der Nutzungs- und Abrechnungsdaten. Der Nutzer muss auf der entsprechenden Web-Site über den Umfang der Protokollierung informiert werden.
- Jede nach den voranstehenden Ausführungen zulässige Protokollierung ist so auszugestalten, dass ein datenschutzrechtlicher Missbrauch vermieden wird, d. h.:
  - der Umfang der Protokolle sollte im Rahmen des Möglichen minimal sein,
  - aufgrund der Datenschutzgesetze (z. B. § 14 Abs. 4 BDSG) dürfen Protokolldaten nicht für andere Zwecke verwendet werden,
  - Protokolle sind durch Zugriffsmaßnahmen gegen unbefugte Kenntnisnahme zu sichern,
  - es sind technisch-organisatorische Auswertungsverfahren festzulegen,
  - es sind möglichst kurze Löschfristen vorzusehen.
- Bei eingehenden Daten, beispielsweise E-Mails, sind, unabhängig davon, ob sie dienstlicher oder privater Natur sind, automatisiert ablaufende zentrale und dezentrale Virenchecks zulässig und angezeigt. Dies gilt auch dann, wenn die Daten im Auftrag verarbeitet werden. Dabei ist zu beachten, dass
  - nur eine automatisierte Kontrolle ohne regelmäßige Kenntnisnahme des Kontrollvorgangs oder -ergebnisses durch Administratoren o. ä. erfolgt,
  - das Inhalts-Scanning auf fest definierte Pattern (Virensignaturen) begrenzt und das Scanning nach frei wählbaren Textstellen ausgeschlossen ist,
  - der Betroffene über das Auffinden von Viren in einer für ihn bestimmten Nachricht unterrichtet wird und mit dieser nur unter seiner Beteiligung oder nach Rücksprache umgegangen wird.
- Private E-Mails der Beschäftigten unterliegen dem Fernmeldegeheimnis. Ihre Kenntnisnahme durch den Arbeitgeber über das für die Erbringung des Dienstes erforderliche Maß ist daher unzulässig.

- Der Einsatz von Programmen zur Auswertung von E-Mails ist wegen des damit verbundenen weitgehenden Eingriffs in das Persönlichkeitsrecht der Beschäftigten nur zulässig, wenn die folgenden drei Voraussetzungen kumulativ gegeben sind:
  – es handelt sich ausschließlich um dienstliche E-Mails,
  – das Vorgehen ist in einer Dienstvereinbarung geregelt,
  – es liegt ein die Auswertung rechtfertigender Ausnahmefall vor.
- Bei Datenübertragung für Dritte sind Inhaltskontrollen nur im Auftrag bzw. mit der Einwilligung des Betroffenen[4] zulässig, wobei dem Auftraggeber (z. B. beim Outsourcing) Gestaltungsmöglichkeiten hinsichtlich folgender Aspekte einzuräumen sind:
  – Nutzung bzw. Umfang der Inhaltskontrolle,
  – technische und organisatorische Folgen bei ausgefilterten Nachrichten.

6. Zusatzmaßnahmen bei der Verarbeitung sensibler Daten

6.1 Sensible Daten

Die steigende Attraktivität des Internet führt in zunehmendem Maße dazu, dass auch solche Bereiche einen Internet-Anschluss erhalten, in denen sensible personenbezogene Daten verarbeitet werden (z. B. Gesundheits- oder Personaldaten). Dies kann entweder im Zuge einer Strategie erfolgen, bei der das Internet als allgemeines Informationsmedium bedarfsunabhängig jedem Mitarbeiter zur Verfügung gestellt wird, oder aber aus einer konkreten Bedarfsermittlung, die etwa im Gesundheitsbereich die Erforderlichkeit einer medizinisch-fachlichen Recherche ergibt.

In diesem Kapitel wird erläutert, inwieweit die in den vorangehenden Kapiteln dargestellten Maßnahmen ausreichen, um auch in solchen Fällen einen datenschutzgerechten Betrieb zu gewährleisten, welche konkreten Risiken bei Betrieb einer Firewall weiterhin bestehen und welche Zusatzmaßnahmen getroffen werden sollten, um diesen Risiken zu begegnen.

6.2 Schutzniveau von Firewalls

Firewalls bieten eine Reihe von Möglichkeiten, um den Datenverkehr in das und aus dem Internet zu kontrollieren und damit das Schutzniveau gegenüber einem direkten Anschluss wesentlich zu erhöhen. Dazu gehören:

4 Bei der zulässigen privaten Nutzung kommt u. U. auch eine generelle Einwilligung durch den Personal- oder Betriebsrat in Betracht. Die Betroffenen sind hierüber ausführlich zu informieren.

- Begrenzung des Zugangs zum Internet auf einen einzigen kontrollierbaren Punkt
- Begrenzung der zugelassenen Dienste auf das Erforderliche
- Begrenzung der Internet-Nutzung auf bestimmte Stationen oder Benutzer
- Verbergen der lokalen IP-Adressen
- Verhindern eines Verbindungsaufbaus aus dem Internet nach innen
- Ausschluss bestimmter Internet-Server oder -Domains
- Ausschluss aktiver Inhalte wie Java oder ActiveX
- Kontrolle auf schädliche Inhalte wie Viren oder Trojanische Pferde
- Protokollierung von Angriffsversuchen

Ein gut konfiguriertes und administriertes Firewall-System kann daher die Gefahren, die beispielsweise durch Trojanische Pferde wie "BackOrifice" oder "NetBus" entstehen, wirkungsvoll begrenzen. Dennoch können auch große und mit erheblichem Aufwand betriebene Firewall-Installationen nicht gegen sämtliche Gefahren aus dem Internet schützen; dies zeigen Vorfälle wie die Verbreitung der E-Mail-Würmer "Iloveyou" oder "Melissa". Diese Ereignisse belegen grundsätzliche Aspekte von Firewalls:

- Jeder Kommunikationskanal, der eröffnet wird, um einen gewünschten Datenaustausch zu ermöglichen, kann auch missbraucht werden. Ein Firewall-System hat im Rahmen des Zugelassenen keine Möglichkeit, zwischen Gebrauch und Missbrauch eines Kommunikationskanals zu unterscheiden. Dies können sich Angreifer zunutze machen.
- Die zunehmende Tendenz, Daten (passive Inhalte) und Programme (aktive Inhalte) zu koppeln, indem Standardanwendungen oder das ganze Betriebssystem skriptfähig gemacht werden, führt zu immer weiteren Schwierigkeiten, den lokalen Betrieb eines PC zu kontrollieren. Neben Makros und Skripten führen auch Browser-basierte Technologien wie Java oder ActiveX immer wieder zu Problemen.
- Virenscanner, zentral oder dezentral, können nur auf bereits bekannte Schadenssoftware reagieren. Bei den rapiden Ausbreitungsgeschwindigkeiten, die das Internet für Schadenssoftware bietet, kommen Updates in der Regel zu spät, um den Schaden wirkungsvoll zu begrenzen.

6.3 Kommunikationsverbindungen als verdeckte Kanäle

Da die Anbindung an das Internet zum Ziel hat, eine Kommunikation mit anderen Rechnern außerhalb des internen Netzes zu ermöglichen, muss selbst eine

sehr restriktiv konfigurierte Firewall eine bestimmte Menge an Datenaustausch zwischen dem internen und dem externen Bereich zulassen. Sowohl der Kommunikationsbedarf als auch die zugrunde liegende Technik des Internet machen es dabei unumgänglich, dass Daten nicht nur in den internen Bereich hineinfließen, sondern auch aus diesem herausgelangen – und sei es nur in Form von Steuerungsinformationen an einen Web-Server.

Dies kann bereits genügen, um einen weitgehenden Angriff auf den geschützten Bereich hinter einer Firewall durchzuführen. So kann etwa das HTTP-Protokoll, das zum Zugriff auf das WWW verwendet wird, missbraucht werden, um – mittels eines entsprechenden Trojanischen Pferdes auf dem betroffenen PC – gespeicherte Daten auf einen Rechner im Internet zu übertragen, ohne dass der Benutzer dies merkt und ohne dass die Firewall dies als unzulässig erkennt. Zwar sind entsprechende Schadprogramme noch nicht öffentlich bekannt geworden, allerdings sind die zugrunde liegenden Konzepte bereits entwickelt und werden in der Sicherheits- und Hackerszene diskutiert. Auch der Kommunikationskanal für E-Mail könnte auf diese Weise missbraucht werden. Die erwähnten E-Mail-Würmer waren – aus Datenschutzsicht – insofern vergleichsweise harmlos, als keine schützenswerten Daten nach außen versandt wurden. Dies hätte jedoch problemlos in die entsprechenden Programme integriert werden können.

Für die Firewall ist diese Kommunikation von normalen, berechtigten Zugriffen durch den Benutzer mittels seines Browsers oder E-Mail-Programms nicht zu unterscheiden. Auch so genannte Intrusion Detection Systeme (IDS), die als Zusatzkomponente von besonders aufwändigen Firewalls den laufenden Betrieb auf Unregelmäßigkeiten hin überwachen, sind kaum in der Lage, eine solche "Nutzung" von der normalen zu unterscheiden (zu IDS siehe http://www.bsi.bund.de/literat/studien/ids/ids-stud.htm).

6.4 Risiken und Maßnahmen im Einzelnen

Das geschilderte Angriffsszenario setzt vier Komponenten voraus:

- eine aktive lokale Komponente, d. h. ein Schadprogramm auf dem betroffenen PC,
- einen Kommunikationskanal, der auf geeignete Weise missbraucht wird,
- einen oder mehrere Kommunikationspartner im externen Netz, d. h. im Internet,
- ein lokales Schadenspotenzial, z. B. in Form gespeicherter personenbezogener Daten.

Dabei müssen alle vier Bestandteile *zur gleichen Zeit* vorliegen. Sofern es gelingt, eine dieser Voraussetzungen zu unterbinden, wird das Risiko eines Datenmissbrauchs erheblich reduziert. Zwar sind prinzipiell auch Angriffe denkbar, die diese Beschränkungen umgehen, z. B. indem die schützenswerten Daten zwischengespeichert werden und damit dauerhaft zugreifbar sind. Dies setzt jedoch eine weitgehende Kenntnis der internen Systemlandschaft voraus, über die ein externer Angreifer in der Regel nicht verfügt.

6.4.1 Beschränkung der aktiven lokalen Komponenten

Die Risiken, von trojanischen Pferden oder anderer Schadsoftware befallen zu werden, sind hinreichend bekannt. Das Internet bildet dabei heute das Hauptverbreitungsmedium, indem entweder ausführbare Programme direkt oder als Bestandteil von Dokumenten (dazu gehören z. B. auch Java-Applets) von dort aktiv oder aber per E-Mail passiv bezogen werden.

Die Schutzmechanismen dagegen sind ebenfalls vergleichsweise gut entwickelt; dazu gehören Virenscanner (zentral und dezentral), Verhindern des Downloads zumindest bestimmter Dateitypen, Begrenzung der lokal ausführbaren Programme auf bekannte Software, lokales Ausschalten von Skript- und Makrokomponenten. Allerdings schränken diese Maßnahmen den Benutzer relativ stark ein und werden daher nach Möglichkeit umgangen. Zudem kann damit in der Regel nur bereits bekannte Schadsoftware kontrolliert werden.

6.4.2 Eingeschränkte Kommunikationskanäle

Die Risiken bestehender Kommunikationskanäle wurden bereits beschrieben. Zunächst einmal sollte die Internetanbindung daher auf die erforderlichen Dienste begrenzt werden; dies ist Bestandteil und Aufgabe jeder Firewall-Installation. Darüber hinaus können die Risiken dadurch begrenzt werden, dass die Kommunikationskanäle nicht dauerhaft zur Verfügung stehen, sondern nur unter bestimmten Bedingungen. Beispielsweise könnte die Verbindung nur für bestimmte Benutzer zugelassen oder sichergestellt werden, dass die Verbindung zu einem Server mit schützenswerten Daten zuvor unterbrochen wurde. Schließlich besteht die Möglichkeit, statt der Standard-Kommunikationskanäle andere, weniger bekannte oder proprietäre Protokolle zu verwenden, die den Aufwand für einen Angriff erhöhen.

6.4.3 Begrenzung der Kommunikationspartner

Wird die Verbindung zu jedem Rechner im Internet sowie von und zu jeder E-Mail-Adresse zugelassen, besteht das Risiko, von jedem Internet-Rechner weltweit attackiert zu werden. In vielen Fällen ist jedoch aus fachlicher Sicht nur ein begrenzter Internetzugang erforderlich. Dabei kann mit einer überschaubaren (und administrierbaren) Liste zugelassener Kommunikationspartner gearbeitet werden. Diese können daraufhin überprüft werden, ob von dort Angriffe zu erwarten sind. Demgegenüber kann auch eine Negativliste implementiert werden, die bekannte oder vermutete Angreifer ausschließt. Dies ist jedoch in der Regel wenig effektiv, da nicht einmal annähernd bekannt ist, von welchen Stellen aus Angriffe stattfinden oder zu erwarten sind. Zudem macht die Dynamik des Internet eine sehr aufwändige Pflege erforderlich.

Zu beachten ist in jedem Fall, dass die Überprüfung auf gute oder schlechte Kommunikationspartner nur dann hilfreich ist, wenn deren Identität zweifelsfrei feststeht. Allerdings lassen sich sowohl E-Mail- als auch IP-Adressen bzw. Domainnamen fälschen. Zudem können Angriffe durchaus auch von bekannten (und ansonsten harmlosen) Kommunikationspartnern ausgehen, wie die Beispiele der E-Mail-Würmer ”Melissa” und ”Iloveyou” zeigen.

6.4.4 Verminderung des lokalen Schadenspotenzials

Der Schaden, der auf Seite des angegriffenen Systems entstehen kann, hängt aus Datenschutzsicht vor allem damit zusammen, welche personenbezogenen Daten von dort aus direkt oder indirekt zugreifbar sind. Maßnahmen sollten daher daran ansetzen, diesen Zugriff zu begrenzen. Dies kann durch die Möglichkeiten des Betriebssystems (Dateirechte) geschehen, durch Verschlüsselung, durch die Vermeidung einer lokalen Datenhaltung, durch eine anwendungsbezogene Authentisierung etc.

6.5 Vorgeschlagene Systemkonfigurationen

Die genannten Einzelmaßnahmen müssen zu sinnvollen Gesamtkonfigurationen zusammengefasst werden. Im Folgenden werden praxiserprobte Lösungen für jeweils unterschiedliche Nutzungsprofile des Internet vorgestellt. Dabei ist teilweise auch eine Kombination der Modelle möglich, um die Sicherheit weiter zu erhöhen.

6.5.1 Proxy mit Positivliste (inhaltliche Begrenzung)

Dieses Konzept ist für solche Benutzer gedacht, die für die Erledigung ihrer fachlichen Aufgaben den Zugriff auf lediglich einen klar definierbaren und überschaubaren Ausschnitt des Internet benötigen, z. B. Arbeitsvermittlungsangebote lokaler oder regionaler Anbieter. Ein solches Nutzungsprofil ermöglicht es, die risikobehafteten Bereiche des Internet pauschal auszublenden, ohne sie im Einzelnen definieren oder bewerten zu müssen. Technisch kann dies durch eine Kontrolle der zugelassenen Internet-Adressen oder Domainnamen auf der Firewall geschehen. Sollen mehrere verschiedene solcher Ausschnitte des Internet verwaltet werden, ist es zweckmäßig, jeweils eigene Proxies vorzusehen, die lediglich dieser Adressfilterung dienen. Dabei ist darauf zu achten, dass die Benutzer dann nur noch über den zugehörigen Proxy und nicht mehr über die Firewall auf das Internet zugreifen können, z. B. indem nur die IP-Adressen der Proxies auf der Firewall eingetragen werden.

Diese Lösung eignet sich auch für solche Fälle, bei denen ein zeitgleicher Zugriff auf personenbezogene Daten und das Internet aus fachlichen Gründen erforderlich ist. Der Mehraufwand liegt in der Erstellung und Pflege der Positivliste sowie in der Beschaffung und dem Betrieb des Proxies.

6.5.2 Umgebungsmodell (zeitliche Begrenzung)

Dieses Konzept kommt für solche Benutzer in Betracht, die einen inhaltlich unbegrenzten Zugang zum Internet benötigen, der jedoch nicht dauerhaft zur Verfügung stehen muss. Die Idee beruht darauf, die Gleichzeitigkeit des Zugriffs auf schützenswerte Daten und auf das Internet (oder auf E-Mail) zu unterbinden. Dadurch kann das Risiko für die schützenswerten Daten deutlich reduziert werden.

Voraussetzung ist ein Betriebssystem wie Windows NT oder UNIX, das eine Authentisierung des Benutzers voraussetzt und mittels dieser Identität Zugriffsrechte an Objekten verwalten kann. Mit dieser Technik ist es möglich, für jeden Realbenutzer zwei Konten einzurichten, wovon eines ausschließlich für den Zugriff auf schützenswerte Daten dient, das andere ausschließlich für den Internet-Zugang. Dazu müssen für das Internetkonto sämtliche Zugriffsrechte auf die schützenswerten Daten entzogen werden. Zudem muss für das andere Konto der Kommunikationskanal ins Internet unterbunden werden. Dazu reicht es allerdings nicht aus, dem Benutzer in dieser Umgebung keinen Browser o. ä. zur Verfügung zu stellen. Vielmehr ist an zentraler Stelle eine benutzerbezogene Kon-

trolle des Internetzugangs vorzusehen. Dies kann durch geeignete Firewalls oder durch vorgelagerte Proxies, die die Benutzeridentität überprüfen, erzielt werden (z. B. MS Proxy Server).

Für die Benutzer bedeutet dies, dass sie sich jeweils auf Betriebssystem-Ebene ummelden müssen. Dies stellt zwar einen Mehraufwand dar, der jedoch bei der Nutzung des Internet nicht allzu sehr ins Gewicht fallen dürfte. Für die E-Mail-Nutzung, die in der Regel sowohl umfangreicher als auch zeitkritischer ist, kann sich jedoch eine andere Einschätzung ergeben.

6.5.3 Grafischer Internetzugang (logische Systemtrennung)

Diese Lösung ist für solche Benutzer geeignet, die eine weder inhaltlich noch zeitlich begrenzbare Internet-Nutzung benötigen. Die Idee beruht darauf, den PC lediglich als Fenster ins Internet zu nutzen. Per Terminal-Emulation wird auf einen Browser oder ein E-Mail-System auf einem anderen Gerät (Terminal-Server) zugegriffen, auf dem keine schützenswerten Daten verarbeitet werden. Nur der Terminal-Server benötigt einen Internet-Zugang, während der Arbeitsplatz-PC, obwohl in das interne Netz integriert, keinen direkten Kontakt zum Internet oder zur Firewall benötigt. Schadsoftware kann daher nur an dem Terminal-Server ansetzen, wovon jedoch keine schützenswerten Daten betroffen sind. Beispielprodukte sind VNC (www.uk.research.att.com/vnc) oder der Windows Terminal Server unter Windows NT und 2000.

Der Mehraufwand für diese Lösung besteht zum einen in dem zusätzlichen Gerät für den Internet-Zugang und zum anderen in der erhöhten Netzlast und Reaktionszeit, die die Übertragung der Bildschirminhalte zwischen Terminal-Server und Arbeitsplatz-PC mit sich bringt. Zudem kann der Benutzer heruntergeladene Dokumente oder empfangene E-Mail zwar öffnen und betrachten sowie gegebenenfalls drucken, jedoch nicht auf seinen eigenen PC übertragen. Dies erfordert einen Austausch über Datenträger oder andere gesicherte Wege.

Prinzipiell kann auf diesem Weg auch Schadsoftware importiert werden, die sich anschließend sowohl den Kommunikationskanal für die Terminalverbindung als auch den Kommunikationskanal für die Internet-Verbindung zunutze macht. Hierzu müssten allerdings lokale Komponenten auf dem Internet-Gerät und auf dem Terminal-PC installiert sowie das verwendete Protokoll für die Terminalverbindung missbraucht werden. Dies stellt eine erheblich höhere Hürde für einen Angreifer dar, insbesondere wenn die interne Systemkonfiguration nicht bekannt ist.

6.5.4 Stand-alone-System (physikalische Systemtrennung)

Diese rigideste Lösung ist für all die Fälle geeignet, in denen die verbleibenden Restrisiken der vorgenannten Modelle als zu hoch eingeschätzt werden. Eine vollständige Systemtrennung zwischen Internet und der Verarbeitung schützenswerter Daten schützt die Vertraulichkeit dieser Daten optimal. Allerdings ist der Aufwand sowohl finanzieller als auch organisatorischer Art unter Umständen erheblich. Bei einer nur sporadischen Internet-Nutzung genügt ein einzelner Internet-PC für mehrere Mitarbeiter. Eine extensive Nutzung setzt jedoch jeweils ein Zweitgerät am Arbeitsplatz voraus. Zu beachten ist dabei, dass auch bei einer vollständigen systemischen Trennung durch verschiedene Geräte bzw. Netze häufig gleichwohl der Bedarf besteht, Daten zwischen diesen Bereichen auszutauschen, z. B. ein Dokument, das im geschützten Netz erstellt wurde, per E-Mail zu versenden. Dies kann per Datenträger (Diskette o. ä.) geschehen. Auf diesem Weg kann zwar Schadsoftware importiert werden, diese kann jedoch ausschließlich Effekte im lokalen Bereich erzielen.

7 Ausblick

In der Vergangenheit war das Design und die Weiterentwicklung der TCP/IP-Protokollfamilie nicht an Zielen wie IT-Sicherheit oder Datenschutz ausgerichtet; lediglich die Ausfallsicherheit von Netzwerken ist als Designkriterium erkennbar und durchgehalten. Inzwischen werden in den einschlägigen RFCs jedoch eine Reihe von sicherheitsrelevanten Problemen behandelt. Um die Dynamik dieses Prozesses zu verdeutlichen, sei hier auf eine zentrale und für die Entwicklung der Firewallsysteme besonders bedeutsame Neuerung hingewiesen, nämlich die Sicherheitsmerkmale (IPSec) der IP-Version 6 (IPv6). Sie sollen eine konsistente Lösung einer Reihe von Sicherheitsproblemen mit IPv4 ermöglichen, siehe auch [BonWol].

IPSec wird die wesentlichen Dienste Authentifikation und Vertraulichkeitssicherung implementieren. So wird auch ein Modus zur Vertraulichkeitssicherung verfügbar sein, bei dem komplette IP-Pakete verschlüsselt und mit einem neuen IP-Header versehen werden (sog. tunnel mode). Wird ein solches Verfahren in einem Gateway oder einer Firewall implementiert, so kann dadurch nicht nur der unbefugte Zugriff auf die Inhalte der Datagramme vermieden, sondern auch die Verkehrsflussanalyse erschwert werden. Denn die IP-Pakete tragen lediglich

die Absenderadresse des Gateways oder der Firewall, und aus dem Inhalt der Datagramme kann auch kein Rückschluss gezogen werden. Verbindungen dieser Art zwischen Firewalls eignen sich zur Kopplung von LANs eines VPN. Die Migration zu einer solchen Lösung gestaltet sich problemlos, da keine weiteren (insbesondere konzeptionellen) Änderungen nötig sind.

Sollen jedoch andere Szenarien als diese Art von VPN realisiert werden, sind weitere Probleme zu lösen. Zum einen ist eine Schlüsselverwaltung notwendig, die den Zugriff auf Authentifikationsschlüssel bisher unbekannter Partner ermöglicht. Eine solche Infrastruktur ist jedoch kein originäres Problem von IPSec, sondern wird in gleicher Weise für die Sicherung der Zurechenbarkeit etwa von elektronischer Post oder von HTTP-Verbindungsinhalten benötigt. Darüber hinaus lassen sich IP-Datagramme im tunnel mode auch durch eine Firewall senden, ohne dass diese die Datagramme in der bisher üblichen Weise analysieren kann. Hier stellt sich die Frage, ob man der Firewall erlauben sollte, die Pakete mitzulesen und ihr das Schlüsselmaterial zur Verfügung zu stellen oder nicht. Die erste Alternative erfordert ein hohes Maß an Hostsicherheit, stellt dafür aber eine echte, gegen Abhören auf dem gesamten Transportweg kryptographisch gesicherte Ende-zu-Ende-Verbindung dar. Im zweiten Fall bestehen an den beteiligten Firewalls Abhörmöglichkeiten, dafür kann die Firewall aber bestimmte Angriffe abwehren, die sonst erst beim Host erkennbar und behandelbar sind.

Neben den Protokollneuerungen im Rahmen der Version 6 des Internet Protocol sind noch weitere Änderungen zu erwarten. Das betrifft Fragen, die sich aus Protokollerweiterungen für mobile Teilnehmer ergeben, ebenso wie Probleme im Zusammenhang mit der Sicherung von Hochgeschwindigkeitsverbindungen.

Festzuhalten bleibt, dass der Anschluss von Netzen der öffentlichen Verwaltung an das Internet nur dann das Attribut datenschutzgerecht verdient, wenn auf die sicherheitsrelevanten Entwicklungen auf dem Gebiet von Internet-Protokollen und -Werkzeugen bis hin zur Endgerätesicherheit zeitnah und adäquat reagiert wird.

8 Anhang

8.1 Weiterführende Informationen und Literatur

8.1.1 Fundstellen im WWW

Allgemeine Informationen und Verweise finden sich unter:
http://www.datenschutz.de

Hamburger Datenschutzhefte -
Datenschutz bei Multimedia und Telekommunikation
http://www.hamburg.de/Behoerden/HmbDSB/Material/hamdat.htm

Landesbeauftragter für den Datenschutz Schleswig-Holstein: Die wichtigsten Bestimmungen des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) und des Mediendienstestaatsvertrages (MDStV)
http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/material/themen/multimed/index.htm

Materialien des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder:
- Arbeitspapier Datenschutzfreundliche Technologien - Privacy Enhancing Technology PET
http://www.datenschutz-berlin.de/to/datenfr.htm

- Arbeitspapier Datenschutzfreundliche Technologien in der Telekommunikation:
http://www.datenschutz-berlin.de/to/tk/ds_tk123.htm

Ergebnisse der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
http://www.datenschutz-berlin.de/doc/de/konf/index.htm

Die Adressen der Landesbeauftragten für den Datenschutz:
http://www.datenschutz-berlin.de/sonstige/behoerde/ldbauf.htm

Die Adressen der Aufsichtsbehörden für den Datenschutz
http://www.datenschutz-berlin.de/sonstige/behoerde/aufsicht.htm

Gesetze und datenschutzrechtliche Regelungen auf Bundesebene:
http://datenschutz-berlin.de/recht/de/rv/index.htm

– **Telekommunikationsgesetz:**
http://www.datenschutz-berlin.de/recht/de/rv/tk_med/tkg_de1.htm

– **Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (IuKDG)** (Art.1: Teledienstegesetz, Art. 2 Teledienstedatenschutzgesetz, Artikel 3 Signaturgesetz und weitere Artikel)
http://www.datenschutz-berlin.de/recht/de/rv/tk_med/iukdg_de.htm

Mediendienste-Staatsvertrag:
http://www.datenschutz-berlin.de/ recht/de/stv/mdstv.htm
Das **CERT** (Computer Emergency Response Team) warnt vor neuen Angriffstechniken aus dem Internet und gibt Ratschläge für Sicherheitsmaßnahmen. CERT-Warnings erscheinen unregelmäßig in der Newsgroup comp.security.announce. Das deutsche CERT ist unter der folgenden Adresse zu erreichen:

DFN-CERT, Universität Hamburg, FB Informatik,
Vogt-Kölln-Str. 30, D-22527 Hamburg
Telefon: 040/5494-2262, Telefax: 040/5494-2241
E-Mail: dfncert@cert.dfn.de (für Mitteilungen, die konkrete Vorfälle oder Sicherheitslücken betreffen) oder info@cert.dfn.de (für sonstige Anfragen oder Kommentare),
WWW: http://www.cert.dfn.de

Technische Informationen zum Internet:
http://www.geocities.com/CollegePark/Quad/6450/menu.htm

8.1.2 Broschüren

Folgende Publikationen können beim Bundesbeauftragten für den Datenschutz[5] angefordert werden:
– Bundesdatenschutzgesetz (BfD - Info 1)
enthält u. a. das Bundesdatenschutzgesetz und Erläuterungen
– Der Bürger und seine Daten (BfD - Info 2)

[5] Der Bundesbeauftragte für den Datenschutz; Postfach 200112; 53131 Bonn; Tel.: 0228/81335-0; Fax: -50; E-Mail: poststelle@bfd.bund400.de

– Schutz der Sozialdaten (BfD - Info 3)
– Der behördliche Datenschutzbeauftragte (BfD - Info 4)
– Datenschutz und Telekommunikation (BfD - Info 5)
enthält u. a. das Telekommunikationsgesetz, TDSV, Auszüge aus dem IuKDG (Teledienstgesetz - TDG - und Teledienstedatenschutzgesetz – TDDSG -)

8.1.3 Literatur

[AKT-DFT] Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern – Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder: Datenschutzfreundliche Technologien (allgemein und in der Telekommunikation), Schwerin, 1998

[ArsRie] Arslan, Ahmet; Riekert, Wolf-Fritz: Sicherheit für Benutzer der Internet-Technologie, Studie des Forschungsinstituts für anwendungsorientierte Wissensverarbeitung (FAW) Ulm im Auftrag des Landes Baden-Württemberg, Ulm, 1997 – http://www.david-datenschutz.de/secinternet.html

[BonWol] Bonnard, Andreas; Wolff, Christian: Gesicherte Verbindung von Computernetzen mit Hilfe einer Firewall, München, 1997 – http://www.bsi.bund.de/literat/studien/fw-stud.pdf

[BSI] Bundesamt für Sicherheit in der Informationstechnik (Hg.): Sicherheit im Internet. – Bonn, 1997. – http://www.bsi.bund.de/literat/faltbl/015_netz.htm

[ChaZwi] Chapman, D. Brent; Zwickey, Elizabeth D.: Einrichten von Internet Firewalls, Bonn, 1996

[CheBel] Cheswick, William R.; Bellovin, Steven M.: Firewalls und Sicherheit im Internet - Schutz vernetzter Systeme vor cleveren Hackern, Bonn, Paris, 1996

[HamDa] Der Hamburgische Datenschutzbeauftragte/Datenschutzbeauftragter des debis Systemhaus: Hamburger Datenschutzhefte – Datenschutz bei Multimedia und Telekommunikation; Hamburg, 1998

[MV-TuD] Der Landesbeauftragte für den Datenschutz Mecklenburg Vorpommern: Technik und Datenschutz, Schwerin, 1996 http://www.tec.informatik.uni-rostock.de/RA/LfD-MV/ak_tech/tud/index_td.html

[Nds] Der Landesbeauftragte für den Datenschutz Niedersachsen: Checkliste Grundschutz durch Firewalls, Hannover, 1998 – http://www.lfd.niedersachsen.de/dokumente/firewall.pdf

[Poh] Pohlmann, Norbert: Firewall-Systeme – Sicherheit für Internet und Intranet, Bonn, 1997

[Ran] Ranum, Marcus J.: Thinking About Firewalls, Proceedings of Second International Conference on System and Network Security, Washington DC, 1993, V2.0 (“Beyond Perimeter Security”) – http://www.clark.net/pub/mjr/pubs/think/

[RanCur] Ranum, Marcus J.; Curtin, Matt: Internet Firewalls Frequently Asked Questions, 26.05.1998 – http://www.clark.net/pub/mjr/pubs/fwfaq/ oder http://www.interhack.net/pubs/fwfaq/

[TelMedR] Telekommunikations- und Multimediarecht; Becktexte im DTV, München, 1998

8.2 Abbildungsverzeichnis

8.3 Abkürzungsverzeichnis

ARP	Address Resolution Protocol
BDSG	Bundesdatenschutzgesetz
CGI	Common Gateway Interface
DMZ	Demilitarisierte Zone
DNS	Dynamic Name Service
FTP	File Transfer Protocol
HTML	HyperText Markup Language
HTTP	HyperText Transport Protocol
ICMP	Internet Control Message Protocols
IP	Internet Protocol
MDStV	Mediendienste-Staatsvertrag
NFS	Network File System
SSH	secure shell
TCP	Transmission Control Protocol
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TKG	Telekommunikationsgesetz
WWW	Word wide Web

8.4 Wichtige Dienste und Begriffe[6]

Das Internet ist ein weltumspannender Zusammenschluss vieler lokaler Computernetze. Die Zahl der Benutzerinnen und Benutzer wurde Anfang 1998 auf etwa 100 Millionen geschätzt. Bisher wurde das Internet hauptsächlich von wissenschaftlichen Einrichtungen wie Universitäten genutzt. Inzwischen hat sich der Nutzerkreis ausgeweitet, und es ist eine fortschreitende Nutzung für kommerzielle Zwecke zu beobachten.

Der Datenübertragung im Internet liegen die einheitlichen TCP/IP-Protokolle (Transmission Control Protocol/Internet Protocol) zugrunde. Jeder Rechner im Internet erhält eine eindeutige numerische Adresse, die IP-Adresse. Die zu übertragenden Daten werden in Pakete zerlegt, die u. a. mit der Absender- und der Empfänger-IP-Adresse versehen werden. Die Datenpakete werden über zumeist eine

6 Mit freundlicher Genehmigung der Autorin aus http://www.klick.link-m.de/hilfe/glossar entnommen, überarbeitet und ergänzt.

Vielzahl von Zwischenstationen weitergeleitet, die den Weg zum Zielrechner aufgrund der Adressinformationen bestimmen (Routing). Die Zwischenstationen tauschen die Daten über Wähl- oder Standverbindungen im Telefonnetz (per Kabel oder Satellit) aus.

Im folgenden werden einige Termini und Dienste des Internet sowie weitere Begriffe der Datenfernübertragung (DFÜ) erklärt.

Account Account heißt übersetzt Konto. Gemeint ist ganz allgemein der Zugang zum Internet oder sonstigen Netzen. Ein Account beinhaltet immer einen ⇨ Usernamen, ein Passwort und natürlich bestimmte Nutzungsbedingungen.

Archie Archie ist ein mächtiger Dienst für die weltweite Suche nach Dateien auf ⇨ FTP-Servern. Der Zugriff erfolgt über ⇨ Telnet, ⇨ E-Mail oder einen eigenen Archie-Client. Als Suchergebnis liefert Archie entweder Server-, Verzeichnis- und Dateinamen oder eine Kurzbeschreibung zu gesuchten Dateien.

Attachment Heute kann man an ⇨ E-Mails Dateien (z. B. ein Winword-Dokument) anhängen und gemeinsam verschicken. Diese Anlagen werden Attachments genannt.

Brett Brett ist die deutsche Bezeichnung für ⇨ Newsgroup. Der Begriff ist vor allem in Mailboxnetzen geläufig und kommt von dem Vergleich mit einem schwarzen Brett, einer Pinwand für öffentliche Nachrichten. Newsgroups werden auch Foren oder Diskussionsgruppen genannt.

Browser Ein Browser ist das Programm, mit dem man durch das ⇨ WWW surfen kann. Ein Browser ist notwendig, um WWW-Seiten überhaupt anschauen zu können (siehe auch ⇨ HTML).

Cookies Cookies (engl. cookie = Keks) sind kleine Datenmengen, die zusammen mit den eigentlich angeforderten Daten aus dem Internet an den Computer des Benutzers übermittelt werden. Dort werden diese Daten gespeichert und für einen späteren Abruf bereitgehalten. Dadurch wird im einfachsten Fall ein wiederholter Zugriff eines bestimmten Benutzers (exakt: des Browsers

auf dem Computer, den er verwendet) auf das Internet-Angebot erkennbar. Vor allem Firmen benützen Cookies, um Kundenprofile zu erstellen oder ein persönliches Angebot zusammenstellen zu können. Man kann einstellen, ob der Browser Cookies akzeptieren darf: InternetExplorer 4.0: Menü Ansicht/Optionen/ Erweitert, Netscape 4.0: Menü Bearbeiten/Einstellungen/Erweitert.

DFÜ DFÜ (Abk. für Datenfernübertragung) ist der Sammelbegriff für alles, was elektronische Kommunikation beinhaltet, besonders verbreitet im Mailboxbereich.

Domain Eine Domain ist eine weltweit erreichbare Adresse, die von Computern im Internet gebraucht wird, um Nachrichten automatisch zustellen zu können. Rhein-main.de, spiegel.de oder aol.com sind z. B. eine Domain, siehe auch ⇨ Username.

Download Download nennt man den Vorgang, wenn man sich von einem fremden Rechner via ⇨ DFÜ eine Datei lädt. Man stellt sich den fremden Rechner quasi oben und den eigenen unten vor (siehe auch ⇨ Upload).

E-Mail Electronic Mail (kurz E-Mail) ist der am weitesten verbreitete Internet-Dienst. E-Mail ermöglicht das Verschicken von "elektronischen Briefen" zwischen mehreren Computerbenutzern. Die Nachrichten können aus Texten, Programmen, Grafiken oder Tönen bestehen. Sender und Empfänger müssen jeweils eine eindeutige E-Mail-Adresse besitzen (Form: Name@Anschrift), die ähnlich der postalischen Anschrift funktioniert. Um E-Mails in andere Datennetze zu verschicken oder von dort zu empfangen, werden Gateways benötigt, die den Übergang von einem System zum anderen handhaben. E-Mail kann außerdem für eine indirekte Inanspruchnahme von anderen Diensten (z. B. ⇨ FTP, ⇨ WWW) genutzt werden. ⇨ Mailbox

Emoticons auch Smileys genannt, mit ihnen werden Stimmungen in Texten (z. B. in mail und news) ausgedrückt (z. B.: **:-)** lächeln; **;-)** verschmitzt lächeln; **:-(** traurig)

FAQ FAQs (Abk. für Frequently Asked Questions) sind sehr hilfreiche Texte, die für Neueinsteigerinnen und Neueinsteiger empfehlenswert sind und verhindern sollen, dass immer dieselben Fragen gestellt werden.

Finger Finger ist ein Werkzeug zur Suche nach Informationen über Personen und Rechner, die an der Kommunikation im Internet beteiligt sind. Es können sowohl personenbezogene Daten (Name, E-Mail-Adresse, Telefonnummer, Arbeitszeit, öffentliche Schlüssel usw.) als auch sicherheitsrelevante Informationen über angeschlossene Rechner in Erfahrung gebracht werden.

FTP FTP steht für File Transfer Protocol und dient dem Übertragen von Dateien zwischen Rechnern mit Hilfe eines normierten Befehlssatzes. Auf dem eigenen Rechner läuft der FTP-Client, der die Befehle an den entfernten FTP-Server weiterleitet. Voraussetzung für die Nutzung sind Accounts auf beiden Rechnern oder eine öffentliche Zugriffsmöglichkeit auf dem FTP-Server durch "Anonymous FTP", wodurch ein eingeschränkter Zugriff auf bestimmte Dateien des entfernten Rechners ermöglicht werden kann. Weltweit gibt es tausende Anonymous-FTP-Server, die Programme, Texte, Grafiken oder Tondateien bereithalten.

Gate(way) Ein Gateway ist ein Computer, der den Übergang von einem Netz zu dem anderen (z. B. von dem Internet zu einem Mailboxnetz) darstellt. Gateways sind notwendig, da die verschiedenen Netze mit unterschiedlichen technischen Sprachen (⇨ Protokollen) arbeiten.

Gopher Gopher ist ein menü-orientiertes Werkzeug zur Recherche, das unabhängig davon eingesetzt werden kann, auf welchem Rechner die gesuchten Informationen zu finden sind, in welchem Format sie vorliegen und welche Zugriffsmöglichkeiten (⇨ FTP, ⇨ Telnet, ⇨ WAIS usw.) existieren. Jeder Gopher-Server ist öffentlich zugänglich. Benutzer können mit ihrem Gopher-Client nur lesend auf die angebotenen Daten zugreifen. Gopher ist im ⇨ WWW integriert.

Header Der Header ist der erste Teil (Vorspann) einer Nachricht, in dem die Adresse, der Absender, die Länge der Nachricht, das Datum und andere Informationen stehen.

HTML HTML (Abk. für Hypertext Markup Language) ist die Sprache, in der Webseiten geschrieben werden. Erst der ⇨ Browser ermöglicht eine grafische Umsetzung der HTML Befehle. Das Besondere von HTML sind die universelle Einsetzbarkeit für alle Arten von Computern und die Verweise, sog. ⇨ Links.

HTTP HTTP (Abk. für Hypertext Transport Protokol) ist quasi die technische Grundlage für das WWW. Dem Computer wird mitgeteilt, dass die Daten aus HTML-Code bestehen, deswegen beginnen WWW Adressen mit http:// Bei neueren Browsern funktioniert das Ansehen von Webseiten allerdings auch, wenn man http:// weglässt.

Hypertext Hypertext wird ein Text genannt, der interaktive Verweise (⇨ Links) beinhaltet.

IRC IRC (Internet Relay Chat) ist ein Internetdienst, der die Möglichkeit bietet, nicht nur via ⇨ E-Mail und ⇨ Newsgroups zeitversetzt zu diskutieren, sondern "live" in Echtzeit rund um die Welt.

ISDN ISDN ist eine Telefon(leitungs)-Technik. Herkömmliche Telefonleitungen funktionieren analog, d. h. übertragen Töne. ISDN hingegen funktioniert – wie der Computer – digital und überträgt also 0 und 1. ISDN bedeutet vor allem auch dadurch eine Geschwindigkeitsverbesserung. Ein ISDN-Anschluss beinhaltet 3 bis 10 Rufnummern und 2 Leitungen, was den Nebeneffekt hat, dass man während des Surfens auch telefonieren kann.

IP-Adresse, IP-Nummer IP-Adressen sind Zahlenkombinationen, z. B. 195.35.6.214. Diese Zahlenkombinationen sind die Adresse des Computers. Jeder Computer hat sowohl eine Adresse aus Wörtern (siehe

Domain) als auch eine IP-Adresse. Die IP-Adresse wird von den Computern benutzt, die Namen sind für die Menschen leichter zu merken.

Link Link ist der engl. Ausdruck für Verbindung und bezeichnet die (anklickbaren) Verweise von einer WWW-Seite auf eine andere.

Mailbox

1. Im Internet wird das Wort Mailbox für ein persönliches Postfach benützt, in dem eingehende Nachrichten (⇨ E-Mails) gespeichert werden.
2. Ansonsten ist damit allerdings ein Mailbox-Computer gemeint, der anrufbar ist und nicht nur die persönliche Post für seine Nutzerinnen und Nutzer aufbewahrt, sondern auch öffentliche Diskussionsforen anbietet. Auch Firmen bieten manchmal Mailboxen an, um Produktinformationen, Treiber und Software anzubieten. Eine Mailbox muss man direkt anrufen (dazu muss man oft einen ⇨ Account besitzen) und im Gegensatz zum Internetprovider verlässt man den angerufenen Rechner nicht, sondern greift nur auf dort vorhandene Informationen zu. Deswegen sind Mailboxen zu Mailboxnetzen zusammengeschlossen, um eine Vielzahl von Informationen anbieten zu können.

Mailingliste Eine Mailingliste ist eine Art Diskussionsforum via Briefverteiler. Alle teilnehmenden Personen müssen sich bei dem Mailinglistenverteiler anmelden und schicken alle Nachrichten dorthin. Die Nachrichten werden dann an alle Teilnehmerinnen und Teilnehmer weitergeleitet. Mailinglisten gibt es zu allen erdenklichen Themen. Je nach Mailingliste können verschiedene Regeln gelten. Generell stellt man sich meistens kurz vor. Mailinglisten bieten überschaubarere Gemeinschaften als ⇨ Newsgroups.

Metasearch Metasearch nennt man eine Suche, die in mehreren Katalogen und Datenbanken unterschiedlicher Suchmaschinen gleichzeitig erfolgt, bzw. eine Suchmaschine, die anbietet, auf einfache Art und Weise dieselbe Suche auf beliebigen Suchmaschinen durchzuführen.

Netcall Netcall nennt man sowohl den Datenaustausch von ⇨ Mailboxen untereinander, als auch das Anrufen und Nachrichtenabgleichen eines ⇨ Points bei der ⇨ Mailbox.

Netikette Die Netikette ist die Menge der Umgangsregeln für das Internet und die anderen Netze.

Newsgroup Newsgroup ist die Internetbezeichnung für öffentliche Foren, Gesprächsgruppen, also den öffentlichen Bereich, in dem alle die von einer Person gesendeten Nachrichten lesen und beantworten können (siehe auch ⇨ Usenet-News, ⇨ Brett).

Online Online bedeutet "mit offener Telefonleitung". Nach der Einwahl bei einem ⇨ Provider oder einer ⇨ Mailbox ist man "online", also mit bestehender Telefonverbindung zu einem anderen Rechner.

Offline Offline ist das Gegenteil von Online. Aus Kostengründen gibt es auch Programme, mit denen man Nachrichten lesen und schreiben kann ohne Telefonverbindung und erst hinterher die fertigen Nachrichten über die Telefonleitung verschickt.

PGP Pretty Good Privacy, ein Verschlüsselungsprogramm für ⇨ E-Mails. Das Programm kann sowohl elektronische Unterschriften leisten als auch E-Mails sicher verschlüsseln.

Point Ein Point ist ein Programm, dass sich in die ⇨ Mailbox (2.) einwählt und automatisch die neuen Nachrichten empfängt und versendet, so dass man die Nachrichten in Ruhe daheim schreiben kann, ohne bestehende Telefonverbindung (⇨ offline).

PoP PoP (Abk. für Point of Presence), gleichbedeutend mit Provider bzw. Einwahlknoten.

Postmaster Postmaster sind die Verantwortlichen eines Systems. Bei Unis oder sonstigen Providern gibt es in der Regel immer einen Account Postmaster, an den man schreiben kann, wenn man Hilfe braucht.

PPP (Point to Point Protocol) PPP ist notwendig, um sich von Zuhause über Modem und Telefonleitung ins Internet einzuwählen. Die meisten Betriebssysteme und Provider unterstützen dieses Protokoll.

Protokoll Ein Protokoll ist eine technische Regelung von Abläufen, quasi eine Sprachregelung, mit der sich Computer verständigen.

Provider Ein Provider ist ein Internetanbieter. Er ermöglicht Privatpersonen/Firmen Zugang zum Internet.

Proxy Ein Proxy-Server ist ein Rechner, der nicht direkt jede Anfrage einer Internetadresse in das Netz weitergibt, um die Seite anzufordern, sondern erst in seinem Speicher nachschaut, ob jemand diese Seite heute (oder in den letzen Stunden oder etc.) bereits aufgerufen hat, so dass er sie nicht erneut anfordern muss. Er speichert also jede angeschaute Datei zwischen, um so die Leitungen zu entlasten. Proxy-Server werden vor allem auch bei Firmenintranets, die ans Internet angeschlossen sind, verwendet, um Verbindungskosten zu sparen und die Arbeitsgeschwindigkeit zu erhöhen.

Signatur(e)
1. Abspann nach einer Mail. Meist ein Spruch oder vielleicht auch eine Postadresse, die ähnlich wie bei einem bedruckten Briefpapier immer mitgeschickt wird. Es sollten nur kurze Signaturen verwendet werden, da lange Signaturen eine überflüssige Datenlast ausmachen, die die Leitungen belegt.
2. digitale Signatur: Siegel zu digitalen Daten, das den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen lässt (vgl. auch § 2 Abs. 1 Signaturgesetz). Ein solches Siegel wird mit Hilfe spezieller kryptographischer Verfahren aus dem Signaturschlüssel und den Daten erzeugt.

TCP/IP Internetprotokoll (genaugenommen zwei verschiedene Protokolle: Transmission Control Protocol/Internet Protocol). Die technische Erfindung, die es erlaubt, dass sich völlig unterschiedliche Computer verstehen können, und die festlegt, was warum wie wohin gesendet wird und somit die technische Basis des Internet darstellt.

Telnet Mit Hilfe von Telnet ist es möglich, auf einem entfernten Rechner eine Terminalsitzung aufzubauen (Remote Login) und textorientierte Anwendungen zu nutzen. Dazu benötigt man einen ⇨ Account oder einen öffentlichen Zugang auf dem entfernten Rechner. Über Telnet sind zum Beispiel Informationssysteme wie Datenbanken oder Bibliotheken zu nutzen (z. B. ⇨ Archie). Telnet wird ebenfalls häufig für die Fernwartung von Rechnern einge

URL Ein URL (Universal Ressource Locator) ist eine exakte Adressangabe für Dateien im Internet. Http://tal.cs.tu-berlin.de/~babajaga/fliegen ist ebenso eine URL wie http://www.tagesschau.de.

Usenet-News Öffentliche Nachrichten werden im Internet in thematisch gegliederten Diskussionsforen (⇨ Newsgroups) ausgetauscht. Dieser News-Dienst wird auch als Usenet (Kurzform von Users´ Network) bezeichnet. Er gleicht einer riesigen Zeitung mit Fachartikeln, Leserbriefen und Kleinanzeigen. Zurzeit gibt es etwa 10.000 verschiedene Newsgroups, in denen pro Monat rund 3,2 Millionen Artikel mit einem Datenvolumen von ca. 14 GB geschrieben werden (Stand: August 1995). Die Artikel werden auf zentralen Rechnern (Newsservern) in Datenbanken gehalten; der Zugriff erfolgt über Newsreader-Programme.

Username Name, der jeder Benutzerin und jedem Benutzer zugewiesen wird, z. B. nora.b, danach kommt immer ein @ und der Name der Mailbox oder des Heimatrechners (also des Providers z. B.) und danach die Domain (die Internetadresse des Rechners). Im Gesamten also nora.b@ipn-b.de[7] Der Teil der Adresse nach dem @ kann unterschiedlich lang sein und hängt von dem Heimatrechner bzw. Provider ab.

Wais WAIS (Wide Area Information Server) ermöglicht eine Volltextsuche in einer Vielzahl von Datenbanken ohne Kenntnis komplizierter Abfragesprachen. WAIS-Abfragen können mit ⇨ Telnet, ⇨ E-Mail, einem eigenen WAIS-Client oder über ⇨ WWW durchgeführt werden.

---

7 Dies ist die E-Mail-Adresse der Autorin des Original-Glossars.

WhoIs WhoIs wurde speziell zur Recherche nach personenbezogenen Daten von im Internet registrierten Nutzerinnen und Nutzern entwickelt. Das Vorhaben, eine Datenbank mit weltweit allen Internet-Nutzern aufzubauen, konnte nicht realisiert werden. Zurzeit existiert eine Vielzahl von einzelnen WhoIs-Servern, auf die mit ⇨ Telnet oder mit besonderer Client-Software zugegriffen werden kann.

WWW Der Internet-Dienst WWW (World Wide Web) kann nahezu alle anderen Dienste integrieren. Durch einen multimediafähigen Hypertext-Mechanismus wird eine einfache Bedienbarkeit erreicht. Der Kommunikation zwischen dem WWW-Client und dem WWW-Server, der die multimedialen Daten anbietet, liegt das Protokoll ⇨ HTTP (HyperText Transport Protocol) zugrunde. Die WWW-Dokumente werden mit der Definitionssprache ⇨ HTML (HyperText Markup Language) erstellt. Für die Generierung interaktiver WWW-Seiten können CGI (Common Gateway Interface)-Skripte installiert werden.

Weitere Glossare:
`http://www.geocities.com/CollegePark/Quad/6450/menu.htm`

Teil 2

Orientierungshilfe „Datenschutzrechtliche Aspekte beim Einsatz von Verzeichnisdiensten“

erstellt vom Arbeitskreis "Technik” der Konferenz
der Datenschutzbeauftragten des Bundes und der Länder

Stand: August 2000

In der Arbeitsgruppe haben mitgewirkt:
Ursula Meyer zu Natrup (Berliner Datenschutzbeauftragter),
Walter Ernestus (Bundesbeauftragter für den Datenschutz)

1. Einleitung

In den letzten Jahren hat sich die Informationstechnologie sehr schnell weiterentwickelt. Dies gilt insbesondere im Bereich der Vernetzung und der offenen Kommunikationssysteme. Die verstärkte Nutzung neuer Kommunikationsformen, beispielsweise E-Mail, erfordert eine neue Art der Verbreitung der Kommunikationsadressen. Hierzu werden zunehmend elektronische Verzeichnisse eingesetzt. Da auf die Informationen in diesen Verzeichnissen von verschiedenen Stellen aus direkt zugegriffen werden kann und insbesondere beliebige Informationen gespeichert werden können, geht die Funktionalität weit über die bisherigen Möglichkeiten eines in Papierform vorliegenden Adress- und Telefonverzeichnisses hinaus. Hieraus ergibt sich die Notwendigkeit, dass von der datenverarbeitenden Stelle festgelegt werden muss, welche Daten im Verzeichnis gespeichert werden.

Zum Einsatz kommen sowohl ISO-konforme (X.500) Systeme als auch Industriestandards (z. B. Network Directory System, NDS). Da in einem Verzeichnisdienst auch personenbezogene Daten gespeichert werden können, ist die Betrachtung datenschutzrechtlicher Aspekte notwendig. Im Verzeichnisdienst existieren verschiedene datenschutzrechtliche Probleme. Diese betreffen zum einen technische Aspekte, wie die sichere Übertragung personenbezogener Daten, zum anderen rechtliche Aspekte, wie Inhalt, Form und Zugriff auf Einträge. Im Vordergrund steht dabei, dass schutzwürdige Belange der verzeichneten Personen nicht beeinträchtigt werden.

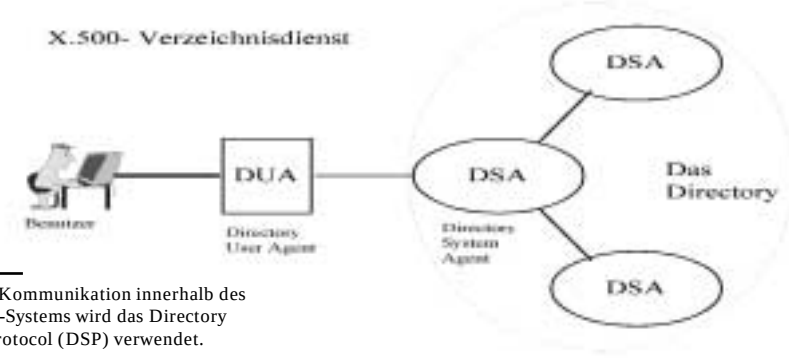
Diese Empfehlung befasst sich mit den Möglichkeiten des datenschutzgerechten Einsatzes von Verzeichnisdiensten. Sie basiert auf dem Betrieb eines Verzeichnisdienstes in einer definierten **Netzwerkumgebung (Intranet) innerhalb der öffentlichen Verwaltung**. Die intranetübergreifende Verbindung mehrerer Verzeichnisse, z. B. über das Internet, wird nicht betrachtet. Des Weiteren wird die generelle Problematik der Systemverwaltung der beteiligten Rechnersysteme auch nicht mit einbezogen, da diese unabhängig von Verzeichnisdiensten sind.

2. Verzeichnisdienste

2.1 Verzeichnisdienst X.500

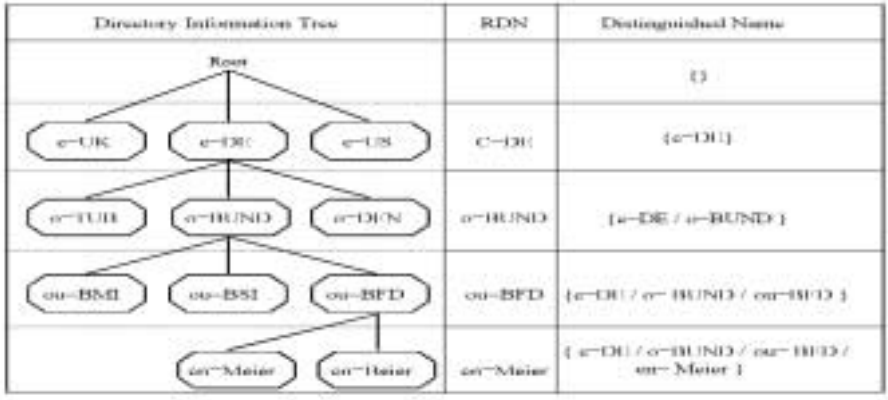
X.500 (ISO-9594) ist ein von der Comité Consultatif International Télégraphique et Téléphonique (CCITT) und der International Standardization Organization (ISO) erarbeiteter Standard, der einen global verteilten Verzeichnisdienst **– den Verzeichnisdienst –** beschreibt. Er kann als ein in vielen Aspekten erweitertes elektronisches Telefonbuch, das neben Telefonnummern auch andere Kommunikationsadressen, z. B. E-Mail-Adressen, enthält, betrachtet werden. Darüber hinaus können relativ beliebige Informationen über Organisationen, deren Mitarbeiter, Rechner, Peripheriegeräte und verfügbare Dienste, also das gesamte Spektrum aller im Kontext von vernetzten Computer- und Kommunikationssystemen vorkommenden Elementen, enthalten sein.

Die Benutzer des Directory-Systems können sowohl menschliche Benutzer als auch Anwendungsprogramme sein. Bei der Interaktion mit dem Directory greift der Benutzer über einen *Directory User Agent* (DUA) auf die Directory-Informationen zu. Dabei sieht die Verzeichnisnorm das *Directory Access Protocol* (DAP) als Zugangsprotokoll vor. Aufgrund der Komplexität hat sich dieses allerdings am Markt nicht durchgesetzt, sondern wurde teilweise (insbesondere in den Endgeräten) durch das **Lightweight Directory Access Protocol** (LDAP) als stark vereinfachtes Zugriffsprotokoll ersetzt. Das Directory besteht aus mehreren kooperierenden *Directory System Agents* (DSA), die auf verschiedenen Rechnern realisiert sein können[1].



1 Für die Kommunikation innerhalb des Directory-Systems wird das Directory System Protocol (DSP) verwendet.

Die Informationen, die das Verzeichnis bereitstellt, sind physikalisch über die DSAs verteilt, erscheinen jedoch für den Benutzer als eine logische Datenbasis. Die Gesamtheit aller Informationen über Objekte, die im Verzeichnis bekannt sind, wird als *Directory Information Base* (DIB) bezeichnet. Jedes Objekt wird darin durch einen Verzeichnis-Eintrag repräsentiert, der die für das Objekt relevanten Daten enthält. Die Einträge der Datenbasis sind hierarchisch angeordnet. Die logische Sicht auf die Datenbasis erscheint als Baumstruktur[2]. Diese Baumstruktur bildet die Grundlage einer eindeutigen Namensgebung innerhalb des Verzeichnisses. Die Namen der Einträge werden gemäß einer mehrstufigen hierarchischen Namenskonvention gebildet. Ein Directory-Name (Distinguished Name - DN) setzt sich aus einer geordneten Folge einzelner Komponenten (Relative Distinguished Name - RDN) zusammen.



Die Namen von Einträgen der DIB sind eindeutig, d. h., jeder Name bezeichnet genau ein Objekt. Dieses wird dadurch erreicht, dass jede Namensgeberautorität (naming authority) innerhalb einer Hierarchiestufe unterschiedliche RDNs verwendet. Jeder Eintrag im Directory besteht aus mehreren Informationen (Attributen). Ein Attribut wird durch einen Attributtyp und einen bzw. mehrere Attributwerte definiert. Ein Beispiel hierfür ist ein Personeneintrag, der folgendes Aussehen haben könnte:

2 Die Directory Information Base stellt sich somit als Directory Information Tree (DIT) dar.

Name des Eintrags (DN): {c=DE / o=Berliner Datenschutzbeauftragter / ou=Bereich Informatik und Organisation / cn=Meyer}

Attributtyp	Attributwert(e)
Name	Mustermann
Nachname	Mustermann
Postanschrift	Musterstr, 1000 Musterstadt
Telefonnummer	+49 30 12345678 +49 30 11223344
Faxnummer	+49 30 9999999
Email	mzn@muster.de
favourite drink	Sekt extra dry

Die im Verzeichnis gespeicherten Daten müssen gegen unautorisierten Zugriff geschützt werden. Hierzu wurde in der Norm X.509 die Sicherung der im Verzeichnis durchgeführten Kommunikation beschrieben. Die dargestellten Verfahren unterscheiden zwischen schwacher und starker Authentifizierung. Die schwache Authentifizierungsprozedur basiert auf dem eindeutigen Namen (DN) und einem Passwort. Die starke Authentifizierung arbeitet mit einem asymmetrischen Kryptosystem (z. B. dem RSA-Algorithmus).

Für die Zugriffskontrolle existiert ein generelles Zugriffskontroll-Modell, das die Anwendung einer bestimmten Sicherheitspolitik (security policy), die jedoch nicht durch das Verzeichnis vorgeschrieben wird, erlaubt. Als Basis wird ein Zugriffskontroll-Schema definiert, das auf Zugriffskontroll-Listen (Access Control Lists, ACL) basiert. Über die Zugriffskontroll-Listen wird festgelegt, wer auf welche Daten in einem Eintrag in welcher Weise (beispielsweise lesend, schreibend) zugreifen kann. Die Normung des Zugriffskontrollmechanismus erfolgte im X.500-Standard erst 1993.

2.2 Network Directory System (NDS)

Das Network Directory System (NDS) ist ein von Novell entwickelter Verzeichnisdienst. Es wurde als verteilte Datenbank konzipiert und ist für die Verwaltung von Netzwerken geeignet. NDS verwaltet Informationen über alle Komponenten im Netzwerk, z. B. Benutzer, Benutzergruppen und Drucker. Ein NDS-Objekt besteht aus einer Vielzahl von Informationen – Properties genannt – und den dazugehörenden Daten, die diese Properties haben können. Es existieren Objekte, mit deren Hilfe eine Baumstruktur ähnlich wie bei X.500 aufgebaut werden kann. Für jedes Objekt können Zugriffsberechtigungen vergeben werden. Dieses wird über Access Control Lists realisiert. Die Funktionalität von

NDS umfasst weniger die Bereitstellung der Telefonbuch-Funktionalität, sondern eher die Verwaltung von allen Objekten in großen Netzwerken.

2.3 Domain Name System (DNS)

Der Verzeichnisdienst wird im Internet zur Auflösung von logischen Rechnernamen auf IP-Adressen verwendet. Für die weiteren datenschutzrechtlichen Betrachtungen spielt DNS keine Rolle, wenn keine Personennamen, Standorte etc. in Zusatzfeldern (txt, ggf. HINFO) des DNS verwaltet werden. Ist dies der Fall, sind die typischen Probleme der anderen genannten Verzeichnisdienste nicht zu erwarten; deshalb wird DNS im Weiteren nicht besonders betrachtet. Gleichwohl ist die Sicherheit dieses Dienstes für eine korrekte Funktion von IP-Infrastrukturen bedeutsam. Die Korrektheit kommt allerdings auch ohne Personenbezug aus.

3. Komponenten und Beteiligte

Ein Verzeichnisdienst stellt in der Regel nur eine Unterstützungsfunktion innerhalb eines anderen Verfahrens oder Dienstes bereit, beispielsweise liefert er Kommunikationsadressen, Telefonnummern und öffentliche Schlüssel bei der Telekommunikation. Allerdings sind auch Lösungen vorstellbar, in denen die Verzeichnisdienste die Verwaltung und Organisation von anderen Datenbeständen übernehmen. In der Regel werden heute Verzeichnisdienste zur Verwaltung der Objekte in großen Netzwerken (Intranet) eingesetzt (Administration). In beiden Fällen werden für den Betrieb des Dienstes gewisse Grundkomponenten – ein Übertragungsnetz, Knotenrechner, eine verteilte Datenbank etc. – benötigt. Auch treten in allen Fällen die gleichen Beteiligten auf, die entweder den Betrieb des Verzeichnisses sicherstellen oder als Betroffener mitwirken.

4. Datenschutzaspekte von Verzeichnisdiensten

In Verzeichnisdiensten wird der eindeutige Teilnehmername (Distinguished Name, DN) definiert. Dieser Name dient als Adresse im Verzeichnis, mit der Personen gefunden werden können. Um das Verzeichnis in einer benutzerfreundlichen Weise zu organisieren, wird zur Identifizierung eine Kette von Namen und Namensteilen verlangt. Dies führt dazu, dass eine Person eindeutig identifiziert werden kann. In Verbindung mit der Möglichkeit, beliebige Informationen zu einer Person zu speichern, erwachsen hieraus besondere datenschutzrechtliche Gefahren. Hierbei ist insbesondere die einfache Zusammenführung bisher getrennt gespeicherter Daten zu sehen. Die Verbindung von verteilt vorliegenden Informationen und eventuell existierender Kopien (Repliken) kann zu Problemen hinsichtlich der Aktualität der Daten führen[3]. Dies stellt insbesondere für die datenschutzrechtlichen Anforderungen bei der Berichtigung und Löschung ein Problem dar. Darüber hinaus bieten sich zudem noch Verknüpfungsmöglichkeiten mit anderen elektronisch vorliegenden Daten, z. B. Telefonbuch auf CD-ROM, Adressbuch auf CD-ROM etc. Dieses ermöglicht die Erstellung von sehr detaillierten Profilen, deren Umfang nicht absehbar ist.

Üblicherweise wird der Verzeichnisdienst als Unterstützungsfunktion in bestehende Verfahren integriert. Damit muss sichergestellt sein, dass der Zugriff auf Informationen in Einträgen nur auf das für die Aufgabenerledigung Notwendige beschränkt wird.

Gefahren für das informationelle Selbstbestimmungsrecht erwachsen auch aus dem komplexen Zusammenspiel der verschiedenen Komponenten, die für den Betrieb des Verzeichnisdienstes benötigt werden. Jede Komponente für sich ist dabei einer Vielzahl von Bedrohungen ausgesetzt. Für jede einzelne Komponente kann dabei von den üblichen Bedrohungspotentialen ausgegangen werden, z. B. Manipulation der Einträge auf den Telekommunikationsleitungen, Zugriffe Unberechtigter (Mithören), Zerstörung der Infrastruktur, Einspielen alter Versionen des Dienstes, Virenbefall etc. Neben diesen allgemeinen Bedrohungen gibt es allerdings auch verzeichnisspezifische.

Das Bedrohungspotential ist abhängig vom Verbreitungsgrad und den Zugriffsmöglichkeiten auf die Inhalte. Ein Beispiel ist die Einführung eines Verzeich-

3 Die Möglichkeit der Replikationen ist wesentlicher Bestandteil der Funktionalität eines Verzeichnisdienstes

nisdienstes in einem Intranet, in dem nur die Adressdaten der Mitarbeiter aufgenommen wurden und das ausschließlich zur Verbesserung der internen Kommunikation dienen soll. Die Verbreitung der Adressen über das eigene Netz hinaus ist nicht vorgesehen. Damit ist das Verzeichnis als eine Art "hausinternes elektronisches Telefonbuch" zu bewerten. Die Bedrohung ist als sehr gering zu bewerten.

Verzeichnisdienste können durch Nutzung von systemimmanenten Replikationsmechanismen oder durch automatisiertes Abfragen zur Bildung von zeitabhängigen Profilen missbraucht werden. Dies sollte vor allem bedacht werden, wenn Verzeichnisdienste bereitgestellt werden, da die Auswerteverfahren und –werkzeuge dann nicht kontrollierbar sind.

4.1 Rechtliche Einordnung von Verzeichnisdiensten

Soweit Verzeichnisdienste nur im Intranet einer datenverarbeitenden Stelle angeboten werden, handelt es sich weder um einen Tele- noch einen Mediendienst. Es liegt somit kein „Angebot" i. S. d. §§ 2 Abs. 2 TDG bzw. MDSTV vor. Die Zulässigkeit derartiger Verzeichnisdienste richtet sich daher allein nach den allgemeinen datenschutzrechtlichen Bestimmungen für Dienst- und Arbeitsverhältnisse.

Wird der Verzeichnisdienst als Basis von Personalinformationssystemen genutzt oder gar ausgebaut, ist der Personalrat (und im Bereich der Privatwirtschaft der Betriebsrat) aufgefordert, durch Nutzung seiner Mitbestimmungsrechte und Abschluss von Dienst- und Betriebsvereinbarungen die Zusammenführung von Daten zu unterbinden bzw. zu kontrollieren.

4.2 Veröffentlichung von Klarnamen

Grundsätzlich sollte allen Bediensteten, die keine herausgehobene Funktion innehaben, ein Wahlrecht dahingehend eingeräumt werden, ob sie mit ihrem Klarnamen oder mit einem selbstgewählten Pseudonym in ein über das Intranet abrufbares Verzeichnis eingestellt werden wollen. Dieses Modell könnte auch genutzt werden, um die Zusammenführung von verschiedenen Verzeichnissen zu unterbinden, wenn der Betroffene verschiedene rollenspezifi-

sche Pseudonyme wählt. Auf diese Weise könnten auch die Risiken einer unkontrollierten Sammlung personenbezogener Informationen durch Suchmaschinen begrenzt werden.

4.3 Beschäftigtendaten in Verzeichnisdiensten

Die Verarbeitung von Personaldaten ist im Bund und in den Ländern unterschiedlich geregelt. Zum Teil enthalten die allgemeinen Datenschutzgesetze einschlägige Bestimmungen, zum Teil wird die Verarbeitung in den Beamtengesetzen angesprochen, wobei einige Landesbeamtengesetze diese Regelungen im Tarifbereich für entsprechend anwendbar erklären. Das Bundesbeamtengesetz (BBG) enthält keine umfassenden Vorschriften über die Verarbeitung von Personaldaten, sondern lediglich Regelungen über die Datenerhebung und den Umgang mit Personalaktendaten. Inhaltlich stimmen alle Regelungen darin überein, dass Beschäftigtendaten verarbeitet werden dürfen, wenn dies u. a. zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht.

Soweit auf den Verzeichnisdienst nur Mitarbeiterinnen/Mitarbeiter der eigenen Verwaltung zugreifen können, dürfen die erforderlichen Angaben über sämtliche Mitarbeiterinnen/Mitarbeiter zur Verfügung gestellt werden. Erstreckt sich die Zugriffsmöglichkeit auch auf andere Stellen im jeweiligen Bundesland, dürfen Familienname, dienstliche Telefonnummer und Hinweise auf den Aufgabenbereich von solchen Personen in den Verzeichnisdienst aufgenommen werden, die den Anschluss aus dienstlichen Gründen nutzen müssen und bei denen die Erreichbarkeit zu ihrer dienstlichen Aufgabe gehört. Unterschiedlich ist die Frage zu beurteilen, ob über diese Angaben hinaus die Amtsbezeichnung oder der Vorname in den Verzeichnisdienst eingestellt werden darf. Hier greifen unterschiedliche Regelungen in den einzelnen Bundesländern, so dass eine generelle Aussage hierzu unmöglich ist.

Für Bedienstete, die in der Regel keinen unmittelbaren Kontakt außerhalb der eigenen Dienststelle haben (z. B. Angehörige interner Dienste, wie des Schreib- oder Botendienstes), ist die Bekanntgabe ihrer Daten nicht erforderlich. Deren Aufnahme in den Verzeichnisdienst wäre nur mit Einwilligung zulässig.

Soweit die Auffassung vertreten wird, dass Name, Dienst-, Funktionsbezeichnung und Organisationseinheit von Bediensteten wegen ihres engen Bezuges zur amtlichen Tätigkeit nicht deren grundsätzlicher Verfügungsbefugnis und damit ihrem Recht auf informationelle Selbstbestimmung unterfallen (Amtswaltertheorie), ergeben sich keine anderen Ergebnisse. Das Erfordernis, die genannten Daten für dienstliche Zwecke einzusetzen, dürfte sich regelmäßig auf das jeweilige Bundesland beschränken. Bei einer über den Landesbereich hinausgehenden Bereitstellung von Daten, beispielsweise bei einer Verbindung zweier öffentlicher Netze, empfiehlt sich – wie allgemein in Zweifelsfällen – der Abschluss einer Dienstvereinbarung.

5. Maßnahmen

Aus datenschutzrechtlicher Sicht sind beim Betrieb eines Verzeichnisdienstes technische und organisatorische Maßnahmen vorzunehmen, die geeignet sind, den aufgeführten Gefahren und Bedrohungen entgegenzuwirken. Für die Komponenten, auf die der Verzeichnisdienst aufsetzt, sind hinreichende und angemessene technische und organisatorische Datenschutzmaßnahmen zu realisieren. Allgemeine Empfehlungen finden sich in entsprechenden Orientierungshilfen (z. B. Unix-Systeme, PCs, Mail-Systeme oder Datenträger) oder auch im BSI-Grundschutzhandbuch, im UNIX-Leitfaden des Hamburger Datenschutzbeauftragten und in Checklisten des Landesbeauftragten für den Datenschutz in Niedersachsen.

Über die grundlegenden Maßnahmen hinaus ist beim Einsatz von Verzeichnisdiensten Folgendes zu beachten:

- Der Verzeichniseintrag ist auf die notwendigen Angaben zu beschränken, beispielsweise E-Mail-Adresse, Telefonnummer, Faxnummer, öffentliche Schlüssel etc. Andere Informationen, wie Hinweise auf Zuständigkeiten, Aufgabenbereiche, Tätigkeitsfelder, Arbeitszeiten, Örtlichkeiten etc., sollten, soweit nicht für die Aufgabenerledigung notwendig, nicht in das Verzeichnis aufgenommen werden.

- Die Zugriffsregelungen sind so eng wie möglich zu fassen. Die Verantwortung hierzu muss eindeutig und durch eine hierfür verantwortliche Stelle vorgenommen werden. Grundsätzlich sollten starke Authentifizierungsme-

chanismen (Digitale Signatur, biometrische Verfahren) zum Einsatz kommen (siehe Kapitel 2.1). Produkte, die lediglich dem X.500-Standard entsprechen, sind nicht einzusetzen.

- Die Organisation des Verzeichnisdienstes muss so gestaltet werden, dass sichergestellt ist, dass die Einträge des Verzeichnisdienstes immer in möglichst zeitnaher Aktualität vorliegen. Dies schließt auch Kopien des Verzeichnisses (Repliken) ein.

- Die Neueinrichtung, Änderung und Löschung von Verzeichniseinträgen sowie die Erstellung und Verbreitung von Repliken sind zu Zwecken der Revision und Datenschutzkontrolle zu protokollieren. Sofern die Protokollierung kein Bestandteil des Produkts ist, muss eine ausreichende Protokollierung durch andere Komponenten, beispielsweise das Betriebssystem, sichergestellt werden.

- Es ist zu prüfen, zu welchen Personen Angaben im Verzeichnisdienst zur Verfügung gestellt werden dürfen.

- Der Verzeichniseintrag ist auf die Angaben zu beschränken, die in der ausgeübten Funktion für die Nutzer des Verzeichnisses relevant sind. Mögliche Angaben sind E-Mail-Adresse, Telefonnummer, Faxnummer, öffentliche Schlüssel, Hinweise auf die Zuständigkeit, Aufgabenbereiche.

- Vor "Veröffentlichung" des Eintrags im Verzeichnis müssen dem Betroffenen die Daten des Eintrags zur Einsichtnahme und/oder Korrektur vorgelegt werden. Anhand von Attributen ist eine Filterung der Verzeichniseinträge nach dem Gesichtspunkt der internen/externen Bereitstellung zu ermöglichen oder die Möglichkeit zu schaffen, dass die Betroffenen selbst eine Sperrung oder Freischaltung bestimmter Attribute vornehmen können.

- Zur Sicherung der Integrität sind bei der Übertragung grundsätzlich kryptographische Verfahren einzusetzen. Ist die Vertraulichkeit von Verzeichnisdaten zu gewährleisten, z. B. bei Abfragen oder Replikation über unsichere Leitungen, so sind auch hierfür geeignete kryptographische Methoden zu benutzen. Dazu stehen auch Werkzeuge außerhalb des Verzeichnisdienstes (etwa zur Verbindungsverschlüsselung) zur Verfügung.

Teil 3

Internetnutzung durch öffentliche Stellen

Auszug aus dem Arbeitspapier "Vom Bürgerbüro zum Internet" der Arbeitsgruppe "Serviceorientierte Verwaltung" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Stand: November 2000

1. Informationsangebote öffentlicher Stellen im Internet

1.1 Inhaltsebene und Tele-/Mediendienste

Bei der Bereitstellung von Informationsangeboten öffentlicher Stellen im Internet und deren Nutzung werden auf vielfältige Weise personenbezogene Daten verarbeitet. Je nach Art bzw. Zweck der Verarbeitung sind unterschiedliche Regelungen zu beachten. Man unterscheidet:

- Dienstedaten
  - Bestandsdaten
  - Nutzungsdaten
  - Abrechnungsdaten
- Inhaltsdaten

Die Datenarten werden in der nachstehenden Tabelle näher erläutert. Bei Bestands-, Nutzungs- und Abrechnungsdaten handelt es sich überwiegend um Daten der Nutzerinnen und Nutzer, die von der öffentlichen Stelle oder einem von ihr beauftragten Mediendienste- oder Telediensteanbieter verarbeitet werden, um ein entsprechendes Internet-Angebot zu realisieren. Bei der Bereitstellung von reinen Informationsangeboten fallen neben den Inhaltsdaten insbesondere Nutzungsdaten an. Auf die datenschutzrechtlichen Regelungen zur Verarbeitung dieser Daten wird in Kap. 1.3 eingegangen.

Datenart		Beschreibung	Beispiele	Rechts-grundlage
Dienste-daten	Bestands-daten	Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses erforderlich sind.	Name, Anschrift der Nutzer, statische IP-Nummer, Kontonummer Kreditkarten-Nummer	TDDSG, MDStV
	Nutzungs-daten	Nutzerdaten, die für die Inanspruchnahme von Diensten erforderlich sind.	Name oder IP-Adresse des anfragenden Clients, Username, Anfrage und deren Status	TDDSG, MDStV
	Abrech-nungs-daten	Nutzerdaten für die Abrechnung von Diensten	Zeitpunkt und Dauer von Verbindungen, Datenvolumen	TDG, TDDSG, MDStV
Inhalts-Daten		In den Internet-Angeboten zum Abruf bereitgestellte Informationen	Zeichen, Bilder, Töne	Landes-datenschutz-gesetze, BDSG, Fachgesetze

Inhaltsdaten sind die eigentlichen Informationen, die von der öffentlichen Stelle zum Abruf bereitgestellt werden. Die Zulässigkeit der Verarbeitung von Inhaltsdaten wird in Kap. 1.2 behandelt.

1.2 Inhaltsdaten: Was darf ins Internet?

Die Bereitstellung von personenbezogenen (Inhalts-)Daten im Internet hat sich in vielen Fällen nach bereichsspezifischen Regelungen zu richten (z. B. Sozialgesetzbuch, Meldegesetze). Fehlen solche Regelungen, so sind die jeweiligen Landesdatenschutzgesetze und bei Stellen des Bundes das Bundesdatenschutzgesetz einschlägig. Soweit die Bereitstellung von Daten im Internet ohne Einschränkungen erfolgt, also keine geschlossene Benutzergruppe durch z. B. ein Passwortverfahren gebildet wird, besteht weltweit die Möglichkeit zu einem Abruf. Da es Staaten gibt, in denen keine oder sehr schwach ausgeprägte Datenschutzbestimmungen existieren, können die schutzwürdigen Belange von

Betroffenen durch die Einstellung ins Netz in besonderem Umfang beeinträchtigt sein. Ein Bereithalten personenbezogener Daten im Internet ist daher nur zulässig, wenn die betroffenen Personen

- dies aufgrund einer Rechtsvorschrift hinzunehmen
- oder eingewilligt haben.

Einwilligung

Die Merkmale einer wirksamen Einwilligung sind:

- **Freiwilligkeit**
  Eine wirksame Einwilligung liegt nur vor, wenn diese freiwillig erteilt worden ist.

- **Informiertheit**
  Voraussetzung jeder Einwilligung ist, dass die Betroffenen umfassend über die Verarbeitung (Verwendungszweck, Beteiligte/Empfänger, Form der Verarbeitung, Anonymisierung) unterrichtet werden. Die Betroffenen sind darüber zu unterrichten, dass aus der Verweigerung einer Einwilligung keine Nachteile entstehen.

- **Schriftlichkeit**
  Von der Schriftform kann nur abgewichen werden, wenn wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, so ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben. Die neuen Datenschutzgesetze sehen auch eine elektronische Form der Einwilligung vor.

- **Widerrufbarkeit**
  Die Betroffenen sind darauf hinzuweisen, dass sie die Einwilligung verweigern oder in Zukunft widerrufen können.

Auch bei einer Verarbeitung mit Einwilligung sind die sonstigen Datenschutzvorkehrungen zu beachten.

Unabhängig hiervon ist der Grundsatz der Datenvermeidung zu beachten. Auch wenn die Verarbeitung von personenbezogenen Daten im Internet zulässig ist, sind alternative anonyme oder pseudonyme Verfahren zu wählen, wenn der Zweck der Verarbeitung so in gleicher Weise erreicht werden kann.

Diese allgemeinen Aussagen zur Zulässigkeit der Bereitstellung werden im Folgenden in einzelnen Teilbereichen verifiziert.

1.2.1 Bedienstetendaten

In Bund und Ländern ist die Verarbeitung von Bedienstetendaten der öffentlichen Stellen bereichsspezifisch geregelt (Sondervorschriften in den Datenschutzgesetzen, Beamtengesetze der Länder). Danach ist eine Übermittlung der Daten von Beschäftigten an Personen oder Stellen außerhalb des öffentlichen Bereichs nur zulässig, wenn der Dienstverkehr es erfordert oder die Betroffenen eingewilligt haben. Eine Veröffentlichung von Bedienstetendaten im Internet ist demnach zulässig, wenn der Dienstverkehr eine solche Veröffentlichung erfordert.

Diese Voraussetzungen sind in der Regel erfüllt für die Bekanntgabe des Namens, der dienstlichen Telefon- und Faxnummer, der E-Mail-Adresse und eines Hinweises auf den Aufgabenbereich von Bediensteten, die aufgrund ihres Aufgabenbereichs mit privaten oder anderen Dritten regelmäßig in Kontakt stehen, oder von herausgehobenen Funktionsträgern. Für Bedienstete, die in der Regel keinen unmittelbaren dienstlichen Kontakt mit Bürgerinnen und Bürgern haben (z. B. Angehörige interner Dienste wie des Schreib- oder Botendienstes), gilt dies nicht. Ob in diesem Zusammenhang eine Übermittlung von Vornamen und Amtsbezeichnung erforderlich ist, wird unterschiedlich beurteilt. In Zweifelsfällen sollte eine Einwilligung eingeholt oder auf eine Veröffentlichung ganz verzichtet werden. In Betracht kommt auch eine Regelung durch Abschluss einer Dienstvereinbarung. Auf jeden Fall müssen die Bediensteten in geeigneter Form vor der Bereitstellung der Daten im Internet informiert werden. Zusätzlich sollte ihnen ein Widerspruchsrecht eingeräumt werden.

Weitere Daten über Beschäftigte mit Außenkontakten, wie private Telefonnummer, Fotos usw., dürfen nur mit Einwilligung der Betroffenen in Internet-Angeboten bereitgehalten werden. Die Bereitstellung von vollständigen

Geschäftsverteilungsplänen oder Telefonverzeichnissen ist in aller Regel nicht erforderlich und damit ohne Einwilligung oder Dienstvereinbarung unzulässig. Sachsen-Anhalt und Thüringen halten die Veröffentlichung von Bedienstetendaten generell nur mit Einwilligung für zulässig.

1.2.2 Bürgerdaten

Grundsätzlich rechtlich zulässig ist die Bereitstellung von Informationen, die ohnehin rechtmäßig veröffentlicht sind oder werden dürfen. Hierzu gehören u. a.

- Publikationen der Presse,
- Tagesordnungen, Referenten, u. U. Gremienmitglieder öffentlicher Veranstaltungen,
- amtliche Bekanntmachungen.

Dabei ist allerdings zu beachten, dass auf diese Weise ein weltweiter Zugriff möglich ist und die bereitgestellten Daten automatisiert recherchierbar sind. Vor der Entscheidung einer Veröffentlichung im Internet sollten daher mögliche negative Konsequenzen für die Betroffenen untersucht und berücksichtigt werden. Zusätzlich sollte ihnen ein Widerspruchsrecht eingeräumt werden. Bereits bestehende Widerspruchsrechte sind zu beachten. Außerdem sollten die Möglichkeiten zur Reduzierung der Recherchierbarkeit in geeigneter Weise genutzt werden (siehe Kasten).

Fehlt eine Rechtsgrundlage, können Daten von Bürgerinnen und Bürgern nur mit ihrer Einwilligung veröffentlicht werden. Dabei sollten pseudonyme Verfahren gewählt werden, wenn dies möglich und sinnvoll ist. Auch beim Vorliegen einer Einwilligung sollten die Möglichkeiten zur Einschränkung der Recherchierbarkeit in geeigneter Weise genutzt werden.

Einschränkung der Recherchierbarkeit von Webseiten

Der automatisierten Recherchierbarkeit von Webseiten kann begegnet werden, wenn die Daten nur über Downloads oder geeignete Datenbankabfragen übermittelt werden. Eingeschränkt gilt dies auch für Webseiten, die beim Zugriff aus Datenbankinhalten automatisch erstellt werden ("dynamisch generierte Webseiten"). Sie können zwar prinzipiell von Suchmaschinen indiziert werden; die meisten Anbieter von Suchmaschinen verzichten aber hierauf, weil so zu viele Fehleintragungen entstehen würden. Es besteht auch die Möglichkeit, durch die Aufnahme von geeigneten Metainformationen in das Internet-Angebot die automatische Recherche durch Suchmaschinen einzuschränken. So werden z. B. durch den html-Befehl

<META NAME="robots" CONTENT="noindex">

Suchmaschinen angewiesen, den Seiteninhalt nicht zu indizieren. Allerdings hängt es von der Gestaltung der jeweiligen Suchmaschine ab, ob diese Befehle unterstützt werden oder nicht.

1.2.3 Webcams

Es wird immer häufiger üblich, Kameras in öffentlichen und privaten Bereichen aufzustellen und deren Bilder im Internet abrufbar zu speichern. Öffentliche Stellen dürfen dies allenfalls dann tun, wenn die Kameras so aufgestellt sind, dass die anfallenden Bilder keine Daten mit Personenbezug enthalten. Ein Personenbezug ist auf jeden Fall herstellbar, wenn Gesichter, Autokennzeichen oder andere identifizierende Merkmale erkennbar sind oder durch Aufnahmesteuerung oder Bildbearbeitung seitens des Empfängers erkennbar gemacht werden können. In Frage kommen daher allenfalls Übersichtsaufnahmen, die die Herstellung eines Personenbezuges definitiv ausschließen. Dabei spielen Rahmenbedingungen wie Bildausschnitt, Bildschärfe oder Bildfrequenz eine wichtige Rolle.

Es sollte auch beachtet werden, dass die erwarteten Informationen oft auf andere, datensparsamere Weise übermittelt werden können. Z. B. können Informationen über die Verkehrslage in Schriftform ("Stau im Bereich...") oder über markierte Stadtpläne oft wirkungsvoller, schneller und völlig ohne personenbezogene Daten über das Internet weitergegeben werden.

1.3 Nutzungsdaten: Was darf wie verarbeitet werden?

Internet-Angebote öffentlicher Stellen sind entweder Teledienste, die im Teledienstegesetz (TDG) und im Teledienstedatenschutzgesetz (TDDSG) geregelt sind, oder Mediendienste, für die der Mediendienste-Staatsvertrag (MDStV) gilt. Teledienste sind alle elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten, wie Zeichen, Bilder oder Töne bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt. § 2 Abs. 2 TDG nennt einige Beispiele, wie Telebanking, Datenaustausch, Datendienste (z. B. über Verkehrs- oder Wetterdaten), Angebote zur Nutzung des Internet oder weiterer Netze, Angebote zur Nutzung von Telespielen und Angebote von Waren- und Dienstleistungen in elektronisch abrufbaren Datenbanken mit interaktivem Zugriff und unmittelbarer Bestellmöglichkeit. Zu den Mediendiensten gehören die an die Allgemeinheit gerichteten Informations- und Kommunikationsdienste wie Fernseheinkauf, Verbreitung von Messergebnissen in Text und Bild, Fernsehtext und vergleichbare Textdienste.

Da die Datenschutzregelungen für Tele- und Mediendienste in TDG/TDDSG und MDStV weitgehend identisch sind, kann die schwierige Unterscheidung zwischen Telediensten und Mediendiensten bei Internetangeboten öffentlicher Stellen in der Regel dahingestellt bleiben. Öffentliche Stellen haben folgende Anforderungen zu erfüllen:

- Nutzungsdaten sind frühestmöglich, spätestens unmittelbar nach Ende der jeweiligen Nutzung zu löschen (soweit es sich nicht um Abrechnungsdaten handelt; § 6 Abs. 2 TDDSG bzw. § 15 Abs. 2 MDStV).

- Der Anbieter darf die Erbringung von Diensten nicht von einer Einwilligung der Nutzerinnen und Nutzer in eine Verarbeitung und Nutzung ihrer Daten für andere Zwecke abhängig machen (§ 3 Abs. 3 TDDSG bzw. § 12 Abs. 4 MDStV).

- Die Prinzipien der Datenvermeidung und der Datensparsamkeit sind zu beachten (§ 3 Abs. 4 TDDSG bzw. § 12 Abs. 5 MDStV).

- Der Anbieter hat den Nutzerinnen und Nutzern die Inanspruchnahme von Diensten anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Die Nutzerinnen und Nutzer sind über diese Möglichkeit zu informieren (§ 4 Abs. 1 TDDSG bzw. § 13 Abs. 1 MDStV).

- Nutzungsprofile sind nur bei Verwendung von Pseudonymen zulässig (§ 4 Abs. 4 TDDSG bzw. § 13 Abs. 4 MDStV).

1.3.1 Speicherung von Nutzungsdaten

Selbst wenn eine Nutzerin oder ein Nutzer im Internet keine Daten über ihre bzw. seine Identität von sich aus offenbart (Ausfüllen von Formularen, E-Mail-Adressen usw.), fallen beim Anbieter Daten über die Nutzerin bzw. den Nutzer an. Dazu gehören die IP-Adressen, über die der Datenaustausch vollzogen wird.

IP-Adresse

Die IP-Adresse (IP = Internet-Protokoll) ist die eindeutige Adresse eines Rechners im weltweiten Internet. Man schreibt sie meist als vier durch Punkte voneinander getrennte Zahlen zwischen 0 und 255. Da Bezeichnungen leichter zu merken sind als Zahlen, sind den IP-Adressen sog. Domain-Namen zugeordnet. Die Zuordnung wird im Domain Name System (DNS) über bestimmte DNS-Server aufgelöst.

Während die Internet-Server feste IP-Adressen haben, gilt dies für die Rechner der meisten Nutzerinnen und Nutzer nicht. Vielmehr erhalten sie von ihrem Access-Provider für die jeweilige Internet-Session eine IP-Adresse dynamisch zugeteilt. Es besteht die Gefahr, dass dynamische IP-Adressen außer vom Access-Provider auch von Außenstehenden (mit großem Aufwand) einer bestimmten Nutzerin oder einem bestimmten Nutzer zugeordnet werden.

Es gibt außerdem Rechner, die über fest vergebene IP-Adressen verfügen. Dies können Rechner von Universitäten oder Firmen sein, die einen großen Bereich von IP-Adressen erworben haben, oder auch private Nutzer, die sehr früh im Internet präsent waren. In diesen Fällen lässt sich die IP-Adresse häufig auch ohne weitere Hilfsmittel einer bestimmten Nutzerin bzw. einem bestimmten Nutzer zuordnen; sie ist deshalb als ein personenbezogenes Datum anzusehen. Allerdings ist nicht erkennbar, ob eine IP-Adresse statisch oder dynamisch ist. Öffentliche Stellen müssen deshalb darauf achten, dass vollständige IP-Nummern bei der Nutzung ihrer

Informationsangebote nicht dauerhaft protokolliert werden. Dies kann zum einen durch einen vollständigen Verzicht auf Protokollierungen erfolgen. Eine andere Möglichkeit besteht darin, nur die ersten drei Nummern der IP-Adresse zu speichern. Auch ist es denkbar, schon während der Verbindung den Besuch des Internetangebots durch Zuordnung zu einer größeren Nutzergruppe zu erfassen, um so eine gewünschte, anonyme Statistik zu erhalten.

1.3.2 Cookies

Die Verwendung von Cookies stellt einen Eingriff in die Datenverarbeitung auf dem persönlichen Rechner des Nutzers dar. Für die Nutzerinnen und Nutzer ist in den meisten Fällen allenfalls die Tatsache einer Speicherung, nicht aber unmittelbar dessen Inhalt und Bedeutung erkennbar.

Cookies

Cookies sind kleine Dateneinheiten, die von Internet-Servern auf den Rechnern der Nutzer gespeichert werden. In den Cookies können Aktivitäten der Nutzerin bzw. des Nutzers festgehalten werden. Cookies können zur Verbindungssteuerung während einer Sitzung ("Session Cookies") verwendet werden. In diesem Fall werden sie bei Beendigung der Sitzung wieder gelöscht. Häufig werden Cookies aber über viele Jahre gespeichert, um dem Anbieter beim nächsten Zugriff eine "bedarfsgerechte" Angebotsauswahl oder die Führung von Statistiken über das Nutzerverhalten zu ermöglichen bzw. Nutzerprofile zu bilden.

Die Verwendung von Cookies unterliegt dem TDDSG oder dem MDStV, wenn die Cookies bestimmten Personen zugeordnet werden können. Eine Zuordnung ist dann möglich, wenn – wie oben beschrieben – Nutzerinnen und Nutzer statische IP-Adressen verwenden oder ihren Namen in Transaktionen preisgeben. In diesen Fällen ist die Verwendung von Cookies nur mit Einwilligung der Nutzerin bzw. des Nutzers zulässig, wenn sie über das Sitzungsende hinaus gespeichert werden sollen. Dabei ist zu beachten, dass bei einer Preisgabe des Namens auch früher gesetzte Cookies zugeordnet werden können.

Wegen der damit verbundenen Risiken sollten öffentliche Stellen in ihren Informationsangeboten auf das Setzen von Cookies möglichst vollständig verzichten, soweit diese nicht zur Gestaltung des Angebots als so genannte Session Cookies eingesetzt werden.

1.3.3 Active-X, Java, JavaScript, Plug-Ins

Active-X-Controls, Java-Applets und JavaScripts sind Programme, die beim Aufrufen von Angeboten auf den Rechner des Nutzers heruntergeladen und dort zur Ausführung gebracht werden. Eine Gefahr geht insbesondere von Programmeinheiten aus, die unter Ausnutzung von Sicherheitslücken Funktionen mit schädlichen Eigenschaften beinhalten. Diesen Gefahren kann der Nutzer durch Deaktivierung der Ausführbarkeit der Programme begegnen. Anbieter sollten daher damit rechnen, dass Nutzer beispielsweise Active-X-Controls, Java-Applets oder Plug-Ins (im Nutzerbrowser installierte Zusatztools) nicht ausführen können. Dies gilt insbesondere für Active-X-Programme, von denen im Allgemeinen die weitreichendsten Gefährdungen für Internet-Nutzer ausgehen. Die Informationsangebote sollten dementsprechend ohne solche Programme gestaltet werden.

1.4 Gestaltung des Angebots

1.4.1 Datenschutzhinweise

§ 12 Abs. 6 MDStV und § 3 Abs. 5 TDDSG legen fest, dass der Nutzer vor einer Erhebung personenbezogener Daten über Art, Umfang, Ort und Zweck der Erhebung, Verarbeitung und Nutzung seiner Daten zu unterrichten ist. Diese Regelung lässt sich in vielen Fällen umsetzen, wenn im Informationsangebot der öffentlichen Stellen Datenschutzhinweise gegeben werden. Sie sollten immer dann veröffentlicht werden, wenn personenbezogene Daten online über die Web-Site gesammelt werden. Dies ist dann der Fall, wenn z. B. eine Online-Registrierung verlangt bzw. ermöglicht wird, wenn sonstige Formulare online ausgefüllt werden können oder wenn mittels E-Mail mit der öffentlichen Stelle kommuniziert werden kann. Auch wenn dies nicht der Fall ist, sollten entsprechende Datenschutzhinweise gegeben werden.

Die Datenschutzhinweise von Informationsangeboten sollten eine Erklärung zu Grundsätzen und Verfahrensweisen bei der Erhebung, Speicherung und Verarbeitung von personenbezogenen Daten enthalten, die im Zusammenhang mit der Bereitstellung und Nutzung eines Informationsangebotes im Internet auftreten.

Beispiel für Datenschutzhinweise

Mit Ihrem Zugriff auf diese Web-Site werden Ihre um die letzte Zahl verkürzte IP-Adresse und weitere Angaben (Datum, Uhrzeit, betrachtete Seite) auf unserem Server für Zwecke der Datensicherheit für zwei Monate gespeichert. Die Daten werden außerdem für statistische Zwecke ausgewertet. Durch die Verkürzung der IP-Adresse ist ein Bezug der gespeicherten Daten auf Ihre Person ausgeschlossen.

Wir verwenden keine Cookies, Java-Applets oder Active-X-Controls.

Sollten Sie noch Fragen zum Datenschutz haben, so wenden Sie sich bitte an:
Name: ... E-Mail-Adresse: ... Telefon: ...

Darüber hinaus steht Ihnen auch der Landes-/Bundesbeauftragte für den Datenschutz als Ansprechpartner zur Verfügung.

Web-Site: ... E-Mail-Adresse: ... Telefon: ...

Wenn Sie eine E-Mail mit schutzwürdigem Inhalt an uns senden wollen, so empfehlen wir dringend, diese zu verschlüsseln, um eine unbefugte Kenntnisnahme und Verfälschung auf dem Übertragungsweg zu verhindern. Unseren öffentlichen Schlüssel finden Sie unter ... unseres Informationsangebots.

Die Hinweise sollten an zentraler Stelle erfolgen, z. B. direkt auf der Begrüßungsseite oder durch einen Link über eine aussagekräftige Schaltfläche. Hier sollte erläutert werden, ob und inwiefern IP-Adressen für statistische Zwecke verarbeitet werden. Auch sollte darauf hingewiesen werden, ob Cookies verwendet werden. Soweit dies zutrifft, sollte dies begründet und über die Auswirkungen

informiert werden. Wenn dies nicht der Fall ist, sollte hierauf hingewiesen werden, weil damit eventuell vorhandene Bedenken und Befürchtungen der Besucher zerstreut werden können.

1.4.2 Anbieterkennzeichnung, Impressum

Sowohl das Teledienstegesetz als auch der Mediendienstestaatsvertrag sehen eine Anbieterkennzeichnung vor (§ 6 TDG, § 6 MDStV). Diese muss Name und Anschrift, bei Personenvereinigungen und -gruppen auch Name und Anschrift des Vertretungsberechtigten enthalten. Die Anbieterkennzeichnung schafft auch aus Datenschutzsicht Transparenz und sollte dementsprechend zentral und vollständig in das Internet-Angebot eingestellt werden. Das Impressum sollte von jeder Webseite aus erreichbar sein.

Dienstanbieter sollten auch deutlich herausstellen, wenn ein Link des Angebots zu einer Seite führt, die nicht mehr im eigenen Verantwortungsbereich liegt (§ 4 Abs. 3 TDDSG, § 13 Abs. 3 MDStV).

Vorschlag für ein Impressum

Stadt <Name>
Verantwortlich: <Name>
<Straße>
<PLZ/Ort>
Telefon: <Telefonnummer>
Telefax: <Telefaxnummer>
E-Mail: <E-Mail-Adresse>

Hinweis zu externen Links
Die Stadt <Name> ist als Inhalteanbieter (Content provider) nach § 5 Abs.1 des Teledienstegesetzes (TDG) bzw. § 5 Mediendienstestaatsvertrag (MDStV) für die "eigenen Inhalte", die sie zur Nutzung bereithält, verantwortlich. Von diesen eigenen Inhalten sind Querverweise ("Links") auf die von anderen Anbietern bereitgehaltenen Inhalte zu unterscheiden. Durch Querverweise hält die Stadt <Name> "fremde Inhalte" zur Nutzung bereit, die durch den Hinweis ▼

[LINK]
gekennzeichnet sind. Die Stadt <Name> hat bei der erstmaligen Verknüpfung die fremden Inhalte gesichtet. Bei Links handelt es sich allerdings stets um "lebende" (dynamische) Verweisungen; die fremden Inhalte können deshalb geändert worden sein, ohne dass die Stadt <Name> hiervon Kenntnis hat.

1.5 Technische Absicherung

Der Anschluss an das Internet ist mit erheblichen Gefährdungen der Datensicherheit und des Datenschutzes verbunden. Die Rechner und Übertragungswege dieses weltweiten Computernetzes sind nicht kontrollierbar. Welchen Weg eine Nachricht nimmt oder in welchem Vermittlungsrechner die Nachricht bearbeitet wird, ist nicht transparent. Denn das Internet wurde ursprünglich nur unter Verfügbarkeitsaspekten entwickelt – auch wenn neuere Entwicklungen versuchen, weiteren Sicherheitsbedürfnissen Rechnung zu tragen. Deshalb wird den Risiken für Vertraulichkeit, Integrität und Zurechenbarkeit vielfach nicht in der gebotenen Weise begegnet. Schwächen finden sich in den Protokollen für die Datenübertragung, in den Implementierungen und Installationen der Programme für die Internet-Dienste und in den angeschlossenen Rechnersystemen. Ohne besondere Schutzmaßnahmen kann sich ein Angreifer oft mit wenig Aufwand unter Ausnutzung der Sicherheitslücken unberechtigten Zugang zu fremden Rechnern verschaffen und dort Daten ausspähen, manipulieren und zerstören. Dies ist besonders gravierend, weil angesichts von ca. 200 Millionen Internet-Teilnehmern auch die Zahl der potentiellen Angreifer, die diese Sicherheitslücken ausnützen und somit die am Internet angeschlossenen Verwaltungsrechner bedrohen, sehr groß ist.

Dieses Risiko ist bei den Informationsangeboten öffentlicher Stellen zu berücksichtigen. Die meisten Gefahren können durch eine geeignete Platzierung des Web-Servers beseitigt werden. Web-Server sollten sich auf jeden Fall außerhalb der lokalen Netze der öffentlichen Stelle befinden. Dies kann durch eine Insellösung realisiert werden, bei der die Daten über das Internet oder durch direkte Eingabe gepflegt werden. Um einen Zugriff aus den lokalen Netzen in das Internet sowie eine Online-Pflege des Web-Servers zu ermöglichen und dennoch die lokalen Netze zu schützen, ist der Einsatz einer Firewall zwischen

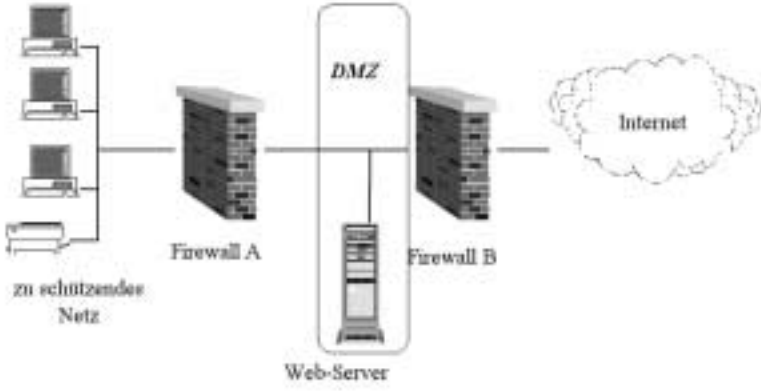
lokalen Netzen und Web-Server erforderlich. Zusätzlich muss der Web-Server selbst gegen Manipulationen aus dem Internet geschützt werden. Er sollte so konfiguriert werden, dass nur die unbedingt erforderlichen Dienste und Protokolle aktiviert sind, die Schreibrechte auf das unabdingbare Maß beschränkt sind und eine Anzeige der Verzeichnisstruktur nicht möglich ist. Weitere Sicherheitsvorgaben lassen sich durch den Aufbau einer doppelten Firewall erreichen, wobei der Web-Server zwischen diesen in der so genannten demilitarisierten Zone steht (siehe Abbildung).

Dabei sollte auf Folgendes geachtet werden:

- Die Anschaffung eines Firewallsystems allein schafft noch keine ausreichende Sicherheit. Die Firewall muss in geeigneter Weise konfiguriert werden. Außerdem müssen die Verantwortlichen für die System- und Netztechnik die Internet-Systeme regelmäßig überprüfen. Auch ist organisatorisch sicherzustellen, dass auf neue Risiken und bekannt werdende Sicherheitslücken sofort mit den geeigneten Maßnahmen reagiert wird.

- Der direkte Zugriff auf Datenbanken der öffentlichen Stelle im LAN sollte nicht zugelassen werden. Soweit ein Datenbankzugriff erforderlich ist, sollten Kopien in Rechnern der entmilitarisierten Zone verwendet werden.

- Das Internet-Angebot ist durch geeignete Maßnahmen gegen unbefugte Manipulationen zu sichern. Hierzu gehören eine sichere Konfiguration der



Rechteverwaltung und eine geeignete Protokollierung unerlaubter Zugriffe auf dem Web-Server sowie eine geeignete Einstellung der äußeren Firewall.

- Besonderes Augenmerk ist auf die personenbezogenen Daten zu richten, die durch die Nutzung entstehen. Sie müssen gegen den Zugriff über das Internet geschützt werden und sollten nur kurzfristig im Web-Server gespeichert sein.

Unabhängig hiervon muss den Risiken begegnet werden, denen eigene Mitarbeiter bei der Nutzung des Internet ausgesetzt sind. Zusätzlich zur Firewall müssen z. B. Maßnahmen gegen Computerviren, schädliche Active-X- und Java-Programme oder Plug-Ins, fehlerhafte Bedienung usw. getroffen werden.

Weitere Informationen zum Thema Datenschutz und Internet können z. B. den Orientierungshilfen der Datenschutzbeauftragten des Bundes und der Länder entnommen werden (Orientierungshilfe Internet des AK Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder unter www.datenschutz.de, Orientierungshilfen und Selbstschutz unter www.lfd.niedersachsen.de u. a.).

2. Interaktive Verwaltung

Im Zusammenhang mit den Informationsangeboten öffentlicher Stellen im Internet (unter 1.) wurden bereits grundlegende Vorgaben für die Gestaltung des Internetauftrittes angesprochen. Wollen die Verwaltungen auch eine interaktive Kommunikation mit den Bürgerinnen und Bürgern im Internet anbieten, sind darüber hinaus weitere Gesichtspunkte bei der Gestaltung des Angebotes zu berücksichtigen:

- Welche Verwaltungsvorgänge können über das Internet abgewickelt werden?

- Wie ist die internetbasierte Kommunikation zwischen Bürgerinnen und Bürgern und der Verwaltung in das Datenschutzrecht einzuordnen?

- Müssen die Verwaltungen Verschlüsselungsverfahren anbieten?

- Ist der Einsatz von Signierverfahren erforderlich?

- Welche technischen und organisatorischen Maßnahmen sind für die Ausgestaltung des Verfahrens denkbar?

2.1 Welche Verwaltungsvorgänge können über das Internet abgewickelt werden?

Die Service-Orientierung der Verwaltung bedingt ein hohes Maß an Organisationsfreiheit der Verwaltung in der Ausgestaltung der Kommunikation mit den Bürgerinnen und Bürgern. Gerade auch Kommunen haben seit jeher auf ihre Organisationshoheit verwiesen, deren Grenzen lediglich in den bestehenden gesetzlichen Bestimmungen liegen dürften. Das bedeutet, dass öffentliche Stellen – wenn nicht etwas anderes ausdrücklich festgelegt ist – ein Verwaltungsverfahren so durchführen können, wie sie es für zweckmäßig halten. Das schließt auch die Wahl des Kommunikationsmediums ein. Wie internetbasierte Kommunikation mit der Verwaltung künftig aussehen könnte, zeigen folgende Beispiele:

Die elektronische Bestellung zur Sperrmüllabholung

Frau A möchte, dass ihr Sperrmüll abgeholt wird. Sie setzt sich an ihren Rechner, wählt die WWW-Adresse ihrer Gemeinde aus und ruft das entsprechende Formular auf der Homepage auf. Bevor sie das Dokument absenden kann, wird mit SSL (Secure Socket Layer) ein "sicherer Kanal" aufgebaut, der von dem PC der Frau A bis zum Server der Kommune reicht. Der Aufbau erfolgt ohne weiteres Zutun von Frau A. Sie erhält lediglich den Browser-Hinweis, dass sie im Begriff ist, Daten über eine sichere Verbindung zu versenden, und dass Dritte Informationen, die mit dieser Seite ausgetauscht werden, nicht sehen können. Sie weiß damit, dass ihre Daten geschützt übertragen werden, füllt das Formular mit den entsprechenden Angaben (Name und Anschrift) aus und sendet es ab. Auf dem gleichen Weg erhält sie auch die Mitteilung über den Abholtag.

Die elektronische Anmeldung zum Volkshochschulkurs

Frau A möchte einen Volkshochschulkurs besuchen. Sie informiert sich auf der Homepage der Volkshochschule über die Angebote und entscheidet sich dort für den Kurs: "Aggressivität und aggressive Kinder – ein Wochenende für Betroffene". Auf der Homepage befindet sich der Hinweis, dass sie die Anmeldung auch online durchführen kann, wenn sie die erforderlichen Angaben per E-Mail übersendet. Da die Kommune ausdrücklich darauf hinweist, dass unver-

schlüsselte E-Mails auf ihrem Weg durch das Internet viele Stationen durchlaufen und unbemerkt gelesen oder verändert werden können, will sie das Angebot wahrnehmen, die E-Mail verschlüsselt zu übersenden. Hierzu installiert sie die erforderliche Software auf ihrem PC, lädt den öffentlichen Schlüssel der Kommune von der Homepage und überprüft ihn mit dem veröffentlichten "Fingerprint". Anschließend verschlüsselt sie ihre Angaben mit dem heruntergeladenen Schlüssel und sendet sie an die Kommune. Diese kann die E-Mail entschlüsseln und die Anmeldung entsprechend weiterleiten.

Da gesetzliche Vorgaben, die die Wahl des Kommunikationsmediums einschränken, weder für die elektronische Bestellung der Sperrgutabfuhr noch für die Anmeldung zu einem Volkshochschulkurs bestehen, wäre in diesen Beispielsfällen eine internetbasierte Kommunikation zulässig.

Dagegen lässt sich eine ebenso eindeutige Aussage für einen anderen Beispielsfall – die Wohnsitzanmeldung – nicht treffen.

Die elektronische Wohnsitzanmeldung

Frau A ist umgezogen und möchte auf elektronischem Weg ihren Wohnsitz ummelden. Zu diesem Zweck ruft sie das elektronische Formular der entsprechenden Internetseite ihrer Kommune auf und gibt ihre Daten ein. Sie signiert das Meldeformular mit ihrem Signaturschlüssel und verschlüsselt das Dokument. Das Formular wird von den zuständigen Mitarbeiterinnen und Mitarbeitern geöffnet und mit einem elektronischen Eingangsstempel versehen. Eine Bestätigung ihrer Anmeldung wird ihr übersandt.

Das Melderechtsrahmengesetz enthält keine Aussage dazu, wie die Meldepflicht konkret zu erfüllen ist. Regeln finden sich aber in den Meldegesetzen der Länder, die vorschreiben, dass die Meldepflichtigen einen Meldeschein auszufüllen, zu unterschreiben und bei der Meldebehörde abzugeben haben. Darüber hinaus sind – in der Regel durch Rechtsverordnung – Form und Inhalt des Meldescheins detailliert festgelegt. Zwar kann in den meisten Bundesländern vom Ausfüllen des Meldescheins abgesehen werden, falls das Melderegister automatisiert geführt wird. Dies gilt aber überwiegend nur dann, wenn die meldepflichtige Person bei der Behörde erscheint, um die erforderlichen

Angaben zu machen. In einigen Ländern wird zusätzlich verlangt, dass die oder der Meldepflichtige die Richtigkeit und Vollständigkeit der Daten durch Unterschrift bestätigt. Ob dort, wo das Gesetz lediglich die eigenhändige Unterschrift vorsieht, internetbasierte Kommunikationsformen der Bürgerinnen und Bürger mit der Verwaltung rechtlich zulässig sind, lässt sich bislang nicht eindeutig beantworten. Schriftliches Handeln setzt auch im Verwaltungs- bzw. Verwaltungsprozessrecht grundsätzlich eine eigenhändige Unterschrift auf einem Papierdokument voraus (vgl. m. w. N. BVerwGE 81, 32 (33)). Bezüglich der von der Verwaltung einzuhaltenden Formvorschriften gibt es gesetzliche Ausnahmen. So kann etwa beim Erlass eines schriftlichen Verwaltungsaktes, der mit Hilfe automatischer Einrichtungen erlassen wird, die Unterschrift fehlen, § 37 Abs. 4 Satz 1 VwVfG (daneben wird die Übermittlung eines Verwaltungsaktes durch E-Mail allerdings mit dem Problem des Nachweises der Bekanntgabe bzw. des Zugangs zu kämpfen haben, wovon wiederum die Wirksamkeit desselben abhängt).

Im Bereich der Kommunikation der Bürgerinnen und Bürger mit ihrer Verwaltung wäre es denkbar, unter Berufung auf die Rechtsprechung des Bundesverwaltungsgerichts im Zusammenhang mit dem Schriftformerfordernis (vgl. etwa BVerwGE 30, 274 ff.; 81, 32 ff.) weitere Ausnahmen zuzulassen.

Das Bundesverwaltungsgericht hat schon in der Vergangenheit zugunsten der Bürgerinnen und Bürger Ausnahmen vom eigenhändig unterschriebenen Dokument etwa bei der Klageerhebung (vgl. BVerwGE 81, 32 (38 ff.)) oder der Erhebung des Widerspruchs (vgl. BVerwGE 30, 274 (277 ff.)) zugelassen, wenn sich aus anderen Anhaltspunkten eine der Unterschrift vergleichbare Gewähr für die Urheberschaft und den Rechtsbindungswillen feststellen ließ. Fortentwickelt wird diese Auffassung, die maßgeblich auf die Rechtssicherheit und Verlässlichkeit als alleinige Zwecke der Schriftform abstellt, auch durch einen Beschluss des gemeinsamen Senates der obersten Gerichtshöfe des Bundes (Az.: GmS-OGB 1/98, NJW 2000, 2340 f.) vom 05.04.2000. Darin wird der technischen Entwicklung Rechnung getragen und ein Computerfax mit eingescannter Unterschrift als ausreichend angesehen. Es dürfte nicht mehr lange dauern, bis auch die E-Mail akzeptiert wird. Eine entsprechende Entschließung, verbunden mit der Aufforderung an die Bundesregierung, die elektronische Abwicklung von Verwaltungsdienstleistungen auch im Bereich der durch Bundesrecht vorgeschriebenen Formerfordernisse zuzulassen, hat der Bundesrat

in seiner Sitzung am 09.06.2000 bereits angenommen (BR-Drs. 231/00; Beschluss). Zeitdruck wird außerdem durch das Europarecht erzeugt, da die Richtlinie 1999/93 EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (Abl. EG L 13 vom 19.01.2000, Seite 12 ff.) bis zum 19.07.2001 in nationales Recht umzusetzen ist. Sie sieht in Art. 5 Abs. 1 a vor, dass die dort näher umschriebene digitale Signatur der eigenhändigen Unterschrift gleichzustellen ist. Gleichwohl sollte in den Bereichen, in denen eine eigenhändige Unterschrift für erforderlich gehalten wird, auf eine kostenintensive Projektierung internetbasierter Kommunikationsformen vorerst verzichtet werden.

Bis zur Klärung der rechtlichen Situation empfiehlt sich folgende Vorgehensweise:

Wird die eigenhändige Unterschrift für erforderlich gehalten, so ist sie nachträglich einzuholen. Ergibt sich auf andere Weise eine der Unterschrift vergleichbare Gewähr für die Urheberschaft und den Rechtsbindungswillen, ist im Einzelfall zu entscheiden, ob ausnahmsweise auf die Unterschrift verzichtet werden kann.

2.2 Wie ist die internetbasierte Kommunikation zwischen den Bürgerinnen und Bürgern und der Verwaltung in das Datenschutzrecht einzuordnen?

Internetbasierte Kommunikation zwischen den Bürgerinnen und Bürgern und der Verwaltung lässt sich datenschutzrechtlich auf zwei Ebenen unterscheiden:

- Auf der Inhaltsebene sind die Vorgaben für die einzelnen Gegenstandsbereiche zu beachten, die spezialgesetzlich normiert oder den allgemeinen Datenschutzgesetzen zu entnehmen sind.

- Auf der Diensteebene gibt es Vorgaben für das Angebot von Informations- und Kommunikationsdiensten, die Pflichten speziell für die Diensteanbieterinnen enthalten.

Mit der Bestellung über das Internet hat Frau A in dem Beispielsfall 1 ihren Namen und ihre Adresse in das Formular eingegeben. Diese Angaben sind erforderlich, damit das Sperrgut abtransportiert werden kann. Die eingegebe-

nen Daten unterliegen nicht der Diensteebene, weil sie unabhängig von der Art der Kommunikation sind. Sie gehören zur Inhaltsebene. So könnte Frau A die Sperrmüllabfuhr mit denselben Angaben schriftlich, durch einen Gang aufs Amt oder telefonisch anfordern. Genauso verhält es sich mit der Anmeldung zum Volkshochschulkurs. Auch hier sind die in der E-Mail versandten Daten (Name, Adresse, Kursart etc.) der Inhaltsebene zuzuordnen. Für die Zulässigkeit der Erhebung der personenbezogenen Inhaltsdaten gilt nichts anderes als auf dem Medium Papier. Fehlt es z. B. schon an der Erforderlichkeit der Angaben, dürfen sie nicht verarbeitet werden.

Die für die Diensteebene maßgebenden rechtlichen Regelungen, nämlich der Mediendienstestaatsvertrag (MStV) und das Teledienstedatenschutzgesetz (TDDSG), enthalten Anforderungen, die erfüllt werden müssen, wenn die Kommunikation auf elektronischem Wege über das Internet geführt werden soll. Für die bei der Individualkommunikation zwischen den Bürgerinnen und Bürgern und der Verwaltung unabhängig von der Inhaltsebene anfallenden personenbezogenen Daten ist das Teledienstedatenschutzgesetz einschlägig. Nach § 6 Abs. 1 Nr. 1 TDDSG darf die Diensteanbieterin personenbezogene Daten über die Inanspruchnahme von Telediensten nur erheben, verarbeiten und nutzen, soweit dies erforderlich ist, um den Nutzerinnen und Nutzern die Inanspruchnahme von Telediensten zu ermöglichen. Die IP-Nummer, die Aufschluss darüber geben kann, welche Rechner miteinander kommunizieren, stellt ein solches Nutzungsdatum im Sinne des Teledienstedatenschutzgesetzes dar, weil es sich hierbei um ein für den Verbindungsaufbau benötigtes Datum handelt. Die zunächst zulässig gespeicherten Nutzungsdaten sind aber frühestmöglich, spätestens nach dem Ende der jeweiligen Nutzung, zu löschen (§ 6 Abs. 2 Nr. 1 TDDSG).

Bei der E-Mail-Kommunikation ist grundsätzlich zwischen dem Transport im Internet über die E-Mail-Server und dem Empfang bzw. Versand über die Endgeräte zu unterscheiden. Im Folgenden soll lediglich auf die rechtlichen Vorgaben eingegangen werden, die die Verwaltungen beim Empfang bzw. Absenden einer E-Mail-Nachricht zu beachten haben. In diesem Fall sind die Verwaltungen nicht Adressatinnen der Befugnisse und Pflichten aus dem Teledienstedatenschutzgesetz. Das in § 3 Abs. 1 TDDSG niedergelegte Verbot mit Erlaubnisvorbehalt, personenbezogene Daten zu verarbeiten, richtet sich an die Diensteanbieterinnen ("vom Diensteanbieter”). Die Empfängerinnen und

Empfänger einer E-Mail sind nicht Anbieterinnen und Anbieter des Informations- und Kommunikationsdienstes E-Mail im Sinne des § 2 Nr. 1 TDDSG, da sie den Teledienst nicht zur Nutzung bereithalten, sondern selber Nutzerinnen und Nutzer des Dienstes sind. Als Diensteanbieterin kommt hier allenfalls die Betreiberin einer Mailbox in Betracht. Das kann im Einzellfall auch eine Kommune sein. Die Zulässigkeit der Speicherung der im Zusammenhang mit der E-Mail-Kommunikation entstandenen Datensätze richtet sich daher auch für die über den Inhalt einer E-Mail-Nachricht hinausgehenden Informationen nach den datenschutzrechtlichen Vorgaben auf der Inhaltsebene. Das bedeutet, dass personenbezogene Daten, wie etwa die Absenderadresse, das Sendedatum oder weitere Sendeinformationen zu löschen sind, wenn ihre Speicherung zur Erfüllung der jeweiligen Aufgabe nicht oder nicht mehr erforderlich ist.

Nutzungsdaten – wie etwa die IP-Nummer – sind spätestens nach dem Ende der jeweiligen Nutzung zu löschen. Auch andere Daten – wie etwa Routinginformationen – müssen gelöscht werden, wenn diese Daten nicht oder nicht mehr zur Erfüllung der jeweiligen Aufgabe der öffentlichen Stelle erforderlich sind.

2.3 Müssen die Verwaltungen Verschlüsselungsverfahren anbieten?

Anders als bei der Verarbeitung von personenbezogenen Daten im Zusammenhang mit dem Informations- und Kommunikationsdienst E-Mail sind die Verwaltungen aber Diensteanbieterinnen, wenn sie die Bürgerinnen und Bürger zu einer internetbasierten Kommunikation etwa im Rahmen einer Homepage einladen. Nach § 4 Abs. 2 Nr. 3 TDDSG hat die Diensteanbieterin durch technische und organisatorische Vorkehrungen sicherzustellen, dass Teledienste gegen Kenntnisnahme Dritter geschützt in Anspruch genommen werden können. Für die Nutzerinnen und Nutzer muss also die Möglichkeit – nicht die Verpflichtung – bestehen, sich durch technische Maßnahmen gegen unbefugte Kenntnisnahme und Verfälschung zu schützen (Schaar / Schulz in: Roßnagel, Recht der Multimediadienste, Stand: Januar 2000, Rdnr. 91 ff. zu § 4 TDDSG).

Die abstrakte Verpflichtung nach § 4 Abs. 2 Nr. 3 TDDSG regelt allerdings nicht, welcher Art die Anforderungen an die Verfahren zur Gewährleistung vertraulicher Kommunikation zu sein haben. Praktisch bedeutet das jedoch, dass die Verwaltungen Verschlüsselungsverfahren anzubieten haben. Das gilt unabhängig vom Inhalt für alle drei Beispielsfälle. Ein Warnhinweis kann zwar der nach § 3 Abs. 5 TDDSG erforderlichen Unterrichtung Rechnung tragen, einen wirksamen Schutz, wie er als technische oder organisatorische Maßnahme von den Diensteanbieterinnen nach dem Teledienstedatenschutzgesetz gefordert ist, stellt der Warnhinweis aber nicht dar, weil er keine vor der Kenntnisnahme Dritter geschützte Kommunikation sicherstellen kann.

Die Auswahl des konkreten Verschlüsselungsverfahrens richtet sich nach den allgemeinen Datenschutzgrundsätzen. Danach hat die Verwaltung diejenigen Verschlüsselungsverfahren anzubieten oder zu verwenden, die erforderlich sind, um die Vertraulichkeit zu gewährleisten. Vorschläge hierzu enthält die Tabelle unter Kap. 2.5.

Es gilt der Grundsatz, dass die Nutzerinnen und Nutzer Informations- und Kommunikationsdienste vor der Kenntnisnahme Dritter geschützt, z. B. durch angemessen sichere Verschlüsselung, in Anspruch nehmen können müssen. Ein bloßer Warnhinweis auf die Risiken unverschlüsselter Kommunikation im Netz reicht nicht aus.

2.4 Ist der Einsatz von Signierverfahren erforderlich?

Zum Schutz von Authentizität und Integrität ist der Einsatz von Signierverfahren zu empfehlen. Nach § 10 Abs. 2 Nr. 2 und 4 Datenschutzgesetz Nordrhein-Westfalen sind Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell (Integrität) bleiben und jederzeit ihrem Ursprung zugeordnet werden können (Authentizität). Eine technische Maßnahme zur Umsetzung dieser Verpflichtung kann der Einsatz von Signierverfahren sein. Ob sich die Erforderlichkeit eines Einsatzes von Signierverfahren auch aus einer Zusammenschau verschiedener Gebote technischer und organisatorischer Maßnah-

men, etwa der Zugriffs-, Übermittlungs-, Benutzer- oder der Transportkontrolle ergeben könnte, wird unterschiedlich beurteilt. Vorschläge für eine technische Umsetzung enthält die Tabelle unter 2.5.

Manchmal erweist sich die Verwendung von Signierverfahren auch aus anderen Erwägungen als sinnvoll. Die Signatur eines Dokumentes als obligatorische Voraussetzung für eine elektronische Bestellung der Sperrgutabfuhr kann notwendig sein, um die Identität der Betroffenen zweifelsfrei sicherzustellen und einer Verbreitung unrichtiger Daten über die Betroffenen, wie etwa bei scherzhaften Massenbestellungen unter einem falschen Namen, vorzubeugen. Zwar ist dies auch derzeit per Telefon möglich. Die unsichere Identifizierung der anrufenden Person ist jedoch auch der angerufenen Person bekannt. Demgegenüber lässt sich im Internet der tausendfache Versand einer E-Mail unter einer Schein-Identität mit wenigen Mausclicks initiieren!

2.5 Welche technischen und organisatorischen Maßnahmen sind für die Ausgestaltung des Verfahrens denkbar?

Die nachfolgende Tabelle soll einer ersten Orientierung über den Umfang der erforderlichen technischen und organisatorischen Maßnahmen dienen. Sie weist auf den Zusammenhang hin, der je nach der konkreten Datenverarbeitungssituation im aktuellen Verwendungszusammenhang entsprechend der unterschiedlichen Sensitivität der Daten unterschiedliche technische und organisatorische Maßnahmen fordert.

Die Anwendung der Tabelle darf nicht schematisch erfolgen. Die Einordnung der einzelnen Daten hängt entscheidend von dem Sachzusammenhang ab, in dem diese Daten verarbeitet werden. Wegen der Kontextabhängigkeit der Sensitivität von Daten müssen besondere Risiken individuell berücksichtigt werden. Sind die Daten eines Datensatzes unterschiedlichen Stufen zuzuordnen, so sind jeweils für den genannten Datensatz die Anforderungen der höchsten Stufe für das einzelne Datum zu wählen. Ebenso wenig darf die Tabelle genutzt werden, um sich der Verpflichtung zu entziehen, ein ausreichendes Sicherheitskonzept zu erstellen.

Die öffentlichen Stellen haben zu gewährleisten, dass – verglichen mit konventionellen Formen des Austausches von Informationen – durch die neuen Kommunikationswege nicht zusätzliche Beeinträchtigungen des Grundrechts

Kategorien personenbezogener Daten	**Technische und organisatorische Maßnahmen**	**Technische Umsetzung**
Kategorie 1: Personenbezogene Daten oder Verwendungszusammenhänge, die wegen ihrer Sensitivität in dem konkreten Datenverarbeitungszusammenhang einen besonderen Datenschutz erfahren müssen. Dieses Schutzniveau ist i. d. R. insbesondere bei Berufs- und Amtsgeheimnissen (z. B. Sozialdaten) und bei personenbezogenen Daten, die nach Art. 8 der EG-Datenschutzrichtlinie als besondere Kategorie eingestuft worden sind (z. B. Daten über die Gesundheit) zu fordern. Ferner personenbezogene Daten oder Verwendungszusammenhänge, deren Missbrauch zu einer Beeinträchtigung von weiteren Grundrechten oder in der Folge zu sonstigen besonders schwerwiegenden Nachteilen führen kann.	Es ist sicherzustellen, dass nur Befugte die personenbezogenen Daten zur Kenntnis nehmen können (Wahrung der Vertraulichkeit). Erforderlich sind außerdem Maßnahmen, die geeignet sind, dass personenbezogene Daten während der Verarbeitung unversehrt und vollständig bleiben (Integrität) sowie jederzeit ihrem Ursprung zugeordnet werden können (Authentizität).	Die Kommunikationspartnerinnen und Kommunikationspartner müssen eine hinreichende Verschlüsselung der Daten vornehmen und eine digitale Signatur einsetzen, die auf dem Signaturgesetz i. V. m. der Signaturverordnung basiert. An die Ausgestaltung der Sicherungsinfrastruktur und an die Verwendung der technischen Komponenten sind die hier beschriebenen besonderen Anforderungen zu stellen.

Kategorie 2: Personenbezogene Daten, deren Missbrauch in ihrem Verwendungszusammenhang geeignet ist, die Betroffenen in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen nicht besonders gewichtig zu beeinträchtigen.	Es sind grundsätzlich die gleichen Maßnahmen wie in Kategorie 1 erforderlich. Allerdings sind an die Ausgestaltung der Sicherungsinfrastruktur keine besonderen (über einen geregelten RZ-Betrieb hinausgehenden) Anforderungen zu stellen. Betroffene und öffentliche Stellen können Zertifikate oder vergleichbare Authentifizierungsmaßnahmen nach eigenen festgesetzten Regeln verwenden.	Eine Umsetzungsmöglichkeit besteht darin, allgemein verbreitete Verschlüsselungs- und Signatursoftware einzusetzen. Notwendige Voraussetzung für einen vertrauenswürdigen Umgang mit einem derartigen Produkt ist die Einrichtung von Zertifizierungsstellen, bei denen die Bürgerinnen und Bürger ihren öffentlichen Schlüssel hinterlegen und digital bestätigen, also zertifizieren lassen können.
Kategorie 3: Personenbezogene Daten, die den Kategorien 1 und 2 nicht zugeordnet werden können.	Es sind Schutzmaßnahmen zu treffen, die einen sicheren Übertragungskanal zwischen den beteiligten Endsystemen mit ausreichender Verschlüsselung ermöglichen. Zusätzliche Maßnahmen sind dann erforderlich, wenn der Verwendungszusammenhang dies erfordert.	Eine Möglichkeit der Kommunikation öffentlicher Stellen mit Bürgerinnen und Bürgern über einen “sicheren Kanal” besteht darin, Secure Socket Layer einzusetzen. Secure Socket Layer (SSL) legt, wie der Name andeutet, eine zusätzliche Schicht zwischen die Transport-Ebene TCP/IP und die Anwendungsebene (HTTP, Telnet, FTP,...) einer Datenübertragung. Von "oben” gesehen ist sie transparent, d. h., die Anwendungsprogramme können ohne große Modifikation auf eine sichere Übertragung zugreifen.