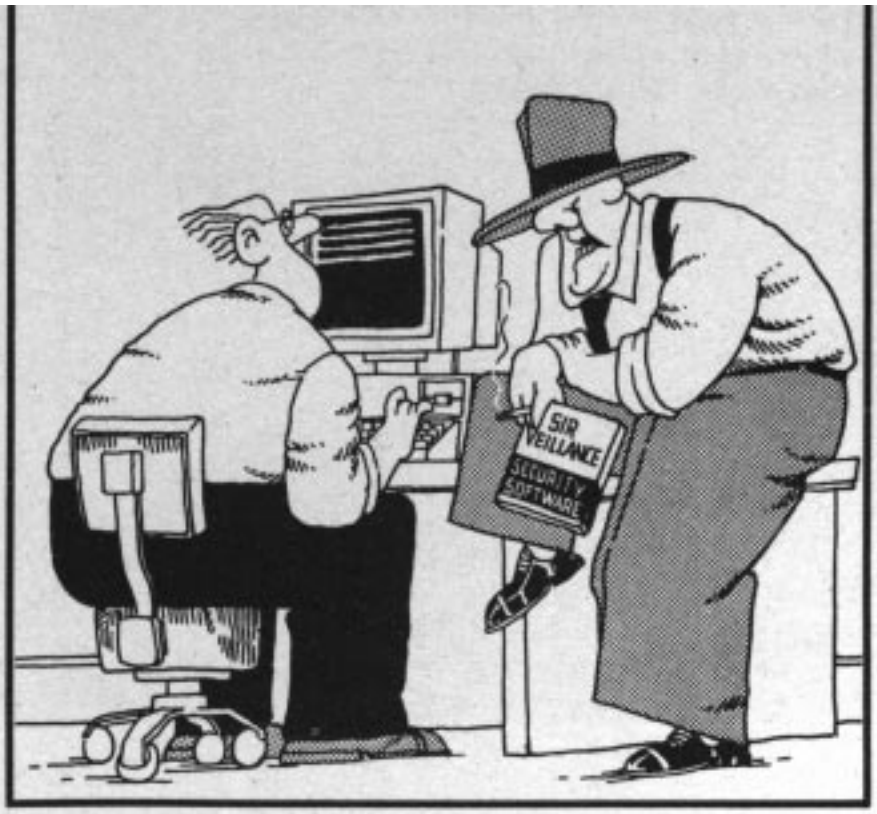
Sicherheit

auf der

Daten-Autobahn?



»Das Sicherheitsprogramm reagiert in drei Fällen: bei einem falschen Paßwort, bei einem inkorrekten Dateiwunsch und manchmal auch schon bei dem dumpfen Gefühl, daß Sie vielleicht auch nur so ein mieser Sausack sind, der gesicherte Daten klauen will.«

Inhaltsverzeichnis

1 Risikoanalyse 1

1.1 Grundschutzansatz 1

1.2 Detaillierte Risikoanalyse 1

1.3 Sicherheitskonzept erstellen 4

1.4 Literaturhinweise 5

2 Sicherheitsanforderungen 6

2.1 Absicherung der Kommunikation 6

2.2 Sichere Identifikation der Kommunikationspartner 7

2.3 Literaturhinweise 7

3 Internet-Protokolle 8

3.1 Netzwerkprotokolle 8

3.1.1 Adress Resolution Protocol (ARP) 8

3.1.1.1 Sicherheitslücken 8

3.1.2 Internet Protocol (IP) 8

3.1.2.1 Sicherheitsrisiken 9

3.1.3 Internet Control Message Protocol (ICMP) 9

3.1.3.1 Sicherheitsrisiken 9

3.2 Transportprotokolle 10

3.2.1 Port-Adressen 10

3.2.1.1 Sicherheitsrisiken 10

3.2.2 User Datagram Protocol (UDP) 10

3.2.2.1 Sicherheitsrisiken 11

3.2.3 Transmission Control Protocol (TCP) 11

3.2.3.1 Sicherheitsrisiken 11

3.3 Anwendungsprotokolle 12

3.3.1 Simple Mail Transfer Protocol (SMTP) 12

3.3.1.1 Sicherheitsrisiken 12

3.3.2 Telnet 13

3.3.2.1 Sicherheitsrisiken 13

3.3.3 File Transfer Protocol (FTP) 13

3.3.3.1 Sicherheitsrisiken 13

3.3.4 HyperText Transfer Protcol (HTTP) 13

3.3.4.1 Sicherheitsrisiken 14

3.4 Literaturhinweise 14

4 Schutzmechanismen 15

4.1 Hostabsicherung 15

4.2 Verbindungsabsicherung 15

4.2.1 Physische Verbindungssicherung 15

4.2.2 Logische Verbindungssicherung 16

4.3 Netzabsicherung 16

4.3.1 Paketfilter 16

4.3.1.1 Unterschied „normaler„ Router und Überwachungsrouter 17

4.3.1.2 Sicherheitsrisiken 18

4.3.2 Application Level Gateway – Proxy Gateways 18

4.3.2.1 Funktionsweise von Proxy-Diensten 19

4.3.2.2 Proxy-Server im Firewall-Einsatz 20

4.3.2.3 Sicherheitsrisiken 20

4.3.3 Kombinationsformen 21

4.3.4 Virtuelle Private Netzwerke (VPN) 21

4.3.4.1 Arbeitsweise 21

4.3.4.2 Protokolle im VPN 22

4.3.4.3 Methoden zur Kompromittierung von VPNs 23

4.4 Firewall-Authentifizierungsmechanismen 24

4.4.1 IP-Adressen / Ports 24

4.4.2 Anwender/Anwendungen 25

4.5 Remote Access Service 26

4.5.1 Password Authentication Protocol (PAP) 26

4.5.2 Challenge Handshake Authentication Protocol (CHAP) 26

4.5.3 PPP Encryption Control Protocol (ECP) 27

4.5.4 Remote Authentication Dial in User Service (Radius) 27

4.5.4.1 Sicherheitsbedenken 28

4.5.5 Terminal Access Control System (Tacacs+) 28

4.5.6 Sicherheitsbedenken 28

4.5.6.1 Wardialer 29

4.6 Sicherheitskonzepte gegen Viren 30

4.7 Literaturhinweise 31

5 Kryptographie 33

5.1 Grundlagen 33

5.1.1 Symmetrische Verschlüsselung 33

5.1.2 Asymmetrische Verschlüsselung 33
5.1.3 Sichere Einwegfunktionen – Hash-Algorithmen 34
5.1.4 Digitale Signaturen 34
5.2 Kryptographische Algorithmen 35
5.2.1 Data Encryption Standard (DES) 35
5.2.1.1 Zur Sicherheit von DES 36
5.2.1.2 Dreifach-DES 36
5.2.1.3 Zur Sicherheit von Dreifach-DES 37
5.2.2 International Data Encryption Algorithm (IDEA) 37
5.2.2.1 Zur Sicherheit von IDEA 38
5.2.3 RSA 38
5.2.3.1 Zur Sicherheit von RSA 39
5.2.4 Diffie-Hellman 40
5.2.5 Digital Signature Standard (DSS) 40
5.2.6 Elliptische Kurven 40
5.2.7 Blowfish 40
5.2.8 Twofish 40
5.2.9 RC 5 41
5.3 Kryptographische Protokolle 41
5.3.1 Secure Socket Layer (SSL) 41
5.3.2 Secure Shell (SSH) 41
5.3.2.1 SSH Transport Layer Protocol 42
5.3.2.2 SSH User Authentication Protocol 42
5.3.2.3 SSH Connection Protocol 42
5.3.3 Secure Hypertext Transfer Protocol (S-HTTP) 43
5.3.4 Simple Key Management for Internet Protocol (SKIP) 43
5.3.5 Email 43
5.3.5.1 Pretty Good Privacy (PGP) 44
5.3.5.2 Secure Multi Purpose Mail Extension (S/MIME) 44
5.3.6 International Protocol Security (IPSec) 45
5.4 Kryptographie im Netzwerk 45
5.4.1 Einsatz in einem VPN 45
5.4.2 Verschlüsselung bei der Dresdner Bank 46
5.5 Literaturhinweise 47
6 Sicherheitskonzept für Remote Access Lösungen 49
6.1 Remote Access via Internet 49
6.2 Remote Access via ISDN 49

6.3 Literaturhinweise 50

7 Anhänge 51

7.1 Deutsche Gesetze 51

7.1.1 Bundes-Datenschutzgesetz 51

7.1.1.1 Erster Abschnitt 51

7.1.1.2 Zweiter Abschnitt 59

7.1.1.3 Dritter Abschnitt 74

7.1.1.4 Vierter Abschnitt 86

7.1.1.5 Fünfter Abschnitt 89

7.1.2 Gesetz zur digitalen Signatur (Signaturgesetz - SigG) 90

7.2 Anschriften der Datenschutzbeauftragten des Bundes und der Länder und der Aufsichtsbehörden der Länder 98

7.2.1 Anschriften der Aufsichtsbehörden für den öffentlichen Bereich 98

7.2.2 Anschriften der Aufsichtsbehörden für den nicht-öffentlichen Bereich 101

7.3 Zugriff auf Patientendaten im Krankenhaus 105

7.3.1 Grundsätze 105

7.3.2 Daten und Patientenakten 106

7.3.3 Zugriffsrechte 108

7.3.4 Technische Absicherung der Zugriffsrechte und -einschränkungen 112

7.3.5 Typische Beispielsituationen 113

7.4 Well Known Ports 118

7.5 Netzwerkgeräte 132

7.5.1 Typische Paßwörter 132

7.5.1.1 Gängige SNMP-Community-Paßwörter 132

7.5.1.2 Switches / Router 133

7.5.2 Port-Analyse 134

7.5.2.1 Standardmäßig geöffnete Ports 134

8 Inhaltsverzeichnis 135

1 Risikoanalyse

1.1 Grundschutzansatz

Für Systeme mit geringem Schutzbedarf (z.B. Internet-Server ohne Verbindung zum eigenen Informationssystem bzw. dem eigenen Datenbestand) wird zur Erreichung eines angemessenen Sicherheitsniveaus, dem sogenannten Grundschutz, ein Abgleich zwischen den bereits vorhandenen und den auf Basis anerkannter Industriestandards empfohlenen Schutzmaßnahmen vorgenommen.

Hierfür ist in Deutschland das IT-Grundschutzhandbuch vom Bundesamt für Sicherheit in der Informationstechnik (BSI) weit verbreitet. Der Aufbau des IT-Grundschutzhandbuches gleicht einem Baukasten, mit dessen Hilfe Elemente der realen Umgebung abgebildet werden können. Für jedes identifizierte IT-System wird ein Soll-Ist-Vergleich durchgeführt. Das Ergebnis des Verfahrens ist ein Maßnahmenkatalog zr Erreichung des vorgegebenen Grundschutzes.

Der englische Standard (British Standard 7799) hat eher den Charakter einer umfangreichen Checkliste. Dieser Standard konzentriert sich wenige auf technische Grunschutzmaßnahmen. Er ist aber als Ergänzung zum IT-Grundschutzhandbuch sehr gut geeignet, da er den organisatorischen Bereich sehr umfangreich behandelt.

1.2 Detaillierte Risikoanalyse

Es gibt verschiedene Methoden zur Risikoanalyse. Qualitative Verfahren setzen die identifizierten Risiken durch eine verbale Beschreibung in Relation zueinander, quantitative Ansätze liefern eine nach dem Schadensmaß geordnete Liste aller Schwächen.

Trotz der gegensätzlichen Ergebnisdarstellung richten sich viele Ansätze zur Risikoanalyse nach der mathematischen Definition des Risikobegriffs:

$$Risiko(R) = Schadenshöhe(S) \cdot E\,\text{int}\,rittswahrscheinlichkeit(E)$$

Dadurch wird das Risiko zum Maß der Schwachstellenbewertung eines Systems. Entsprechende Sicherheitsvorkehrungen minimieren das Risiko, können es jedoch nicht vollständig ausschließen. Das verbleibende Risiko wird als Restrisiko bezeichnet und in der Regel als so gering eingestuft, daß es für den Einsatz des IT-

Systems als vernachlässigbar klein angesehen wird. In diesem Zusammenhang spricht man auch von einem Tragbaren bzw. untragbaren Risiko.

Die einzelnen Schritte einer detaillierten Risikoanalyse sind im einzelnen:

1. Bestandsaufnahme

   Bei der Bestandsaufnahme werden alle schützenswerten Objekte des Analysebereiches erfaßt, z.B. ein Web-, File- oder Mail-Server, welcher vom öffentlichen Netz (Internet) aus angegriffen werden kann

2. Bedrohungsanalyse

   Für jedes erfaßte Objekt muß nun dokumentiert werden, welche Bedrohungen und Gefahren einen maßgeblichen Einfluß auf die Geschäftstätigkeit und den laufenden Betrieb des Gesamtsystems haben, z.B. Imageverlust durch Veränderung der WWW-Seiten auf den Webserver, Geheimnisverlust durch Einbruch einer unauthorisierten Person in den Mail-Server, usw.

3. Eintrittswahrscheinlichkeit bestimmen

   Die quantitative Risikobewertung definiert für die Eintrittswahrscheinlichkeit ein Maß „Erfolgreiche Angriffe vom Typ X pro Jahr“. Dies entspricht der Jahresverlustquote. Erster und oftmals auch einziger Anhaltspunkt für derartige Auswertungen im Internet sind die Aufzeichnungen in den Protokolldateien exponierter Systeme. Das „Computer Ermergency Response Team“ (CERT) veröffentlichte eine Zusammenfassung über 4299 Meldungen, welche in den Jahren 1989 bis 1995 bei CERT eingingen:

   - 89,4 % Mißbrauch fremder User Accounts
   - 5,1 % Mitlesen vertraulicher Informationen
   - 3,1 % Integritätsverletzungen
   - 2,4 % Angriffe auf die Systemverfügbarkeit.

4. Ermittlung der Schadenshöhe

   Die Schadenshöhe ist ein Maß für die finanziellen und organisatorischen Auswirkungen bei erfolgreichem Eintritt der Bedrohungen. Eine mögliche Maßeinheit für die Schadenshöhe kann der Geldbetrag sein, der aufzubringen ist, um den Zustand vor dem Zwischenfall wieder herzustellen. Hierbei sind

neben den direkten Schäden auch die Folgeschäden zu beachten. Eine neutrale Bewertungsskala vermeidet die Ungenauigkeit, die bei der Nutzung absoluter Beträge entstehen muß. Das Verfahren vom BSI schlägt eine Bewertung von „Unbedeutend“ bis „Existenzgefährdend“ vor:

Bewertung	Bedeutung
4	Existenzgefährdend
3	Groß
2	Mittel
1	Gering
0	Unbedeutend

Abhängig davon, wie detailliert die Bedrohungsanalyse durchgeführt wurde, lassen sich mögliche Auswirkungen auch konkreter beschreiben, z.B.:

Bewertung	Bedeutung
0	Denial-of-Service-Attacke
1	interner Eindringling kann unberechtigt Lesezugriff auf Dateien/Daten erlangen
2	interner Eindringling kann unberechtigt Schreibezugriff auf Dateien/Daten erlangen
3	interner Eindringling kann unberechtigt Schreibezugriff auf Systemdateien erlangen
4	externer Eindringling aus dem lokalem Netzwerk kann unberechtigt Lesezugriff auf Dateien/Daten erlangen
5	externer Eindringling aus dem lokalem Netzwerk kann unberechtigt Schreibezugriff auf Dateien/Daten erlangen
6	externer Eindringling aus dem lokalem Netzwerk kann unberechtigt Schreibezugriff auf Systemdateien erlangen
7	externer Eindringling aus dem Internet kann unberechtigt Lesezugriff auf Dateien/Daten erlangen

8	externer Eindringling aus dem Internet kann unberechtigt Schreibezugriff auf Dateien/Daten erlangen
9	externer Eindringling aus dem Internet kann unberechtigt Schreibezugriff auf Systemdateien erlangen

5. Risikobewertung

   Abhängig von der Schadenshöhe (S) und der Eintrittswahrscheinlichkeit (E) wird nun eine Liste der einzelnen Risikopotentiale in Hinblick auf den Schaden aus finanzieller Sicht und der Abhängigkeit des Unternehmens von der Funktionsfähigkeit der untersuchten Systeme erstellt.

   Dann wird für jedes Wertepaar festgelegt, ob das damit verbundene Risiko tragbar ist, oder nicht. Alle Schwachstellen, die ein untragbares Risiko aufweisen, müssen im Sicherheitskonzept durch plattformspezifische Implementierungsvorschläge und organisatorische Sicherheitsmaßnahmen adressiert werden.

   Den ermittelten Risiken werden Prioritäten zugewiesen, die auch bei der Umsetzung der Maßnahmen berücksichtigt werden müssen.

6. Sicherheitsanforderungen

   Aus der Risikoanalyse leiten sich Sicherheitsanforderungen ab, die durch das Sicherheitskonzept und den darin beschriebenen Maßnahmen abgedeckt werden müssen. Die Anforderungen müssen in allgemeinen, unternehmensstrategischen Zielen wiedergegeben werden.

1.3 Sicherheitskonzept erstellen

Vordringlichste Aufgabe des Sicherheitskonzeptes ist es, die in der Risikoanalyse identifizierten Sicherheitslücken durch geeignete Maßnahmen zu schließen und somit den Anforderungen an die Sicherheit der Anwendung gerecht werden. Ist dies in einzelnen Fällen nicht möglich, dann müssen die Risiken zumindest vermindert werden. Zur Auswahl stehen

- präventive Maßnahmen, die Gefahren bereits im Vorfeld zu vermeiden helfen
- überwachende Maßnahmen, die Angriffe bei ihrem Eintritt erkennen und abzuwehren suchen, sowie

- reaktive Maßnahmen, die nach Eintritt der Bedrohung die Schadensfolge minimieren.

Für ein Sicherheitskonzept ist es erforderlich, daß die folgenden Punkte dokumentiert werden:

- Aufgabe und Funktion des Systems aus Anwendersicht
- Struktur des Systems
- Sicherheitsanforderungen.

Die Einführung kann eine kurze Beschreibung der Interaktionsmöglichkeiten mit dem System beinhalten. Für die Darstellung der Struktur bietet sich eine schematische Skizze an, die alle an dem System beteiligten Komponenten wiedergibt und den derzeitigen Zustand eines eventuell vorhandenen Systems erläutert. Im Anschluß hieran erfolgt die Auswahl geeigneter Abwehrmaßnahmen, die von mehreren Faktoren abhängig sind:

- Schutzwirkung der Maßnahme
- Kosten der Beschaffung, Einführung und den Betrieb
- Höhe des verbleibenden Restrisikos
- Zusammenwirken mit anderen Maßnahmen
- Benutzerfreundlichkeit.

Die geplanten Maßnahmen sollten die Arbeit mit dem System weitestgehend unbeeinträchtigt lassen, jedoch ist Sicherheit immer ein Kompromiß zwischen Funktionalität und Verbot.

1.4 Literaturhinweise

- Bundesamt für Sicherheit in der Informationstechnik
  Sicherheitsaspekte bei Electronic Commerce
  Schriftenreihe zur IT-Sicherheit, Band 10
  Bundesanzeiger Verlag, 1999
- Raepple, Martin
  Sicherheitskonzepte für das Internet, dpunkt-Verlag, 1998

2 Sicherheitsanforderungen

Die Sicherheitsanforderungen bei der Datenübertragung lassen sich zunächst ganz grob in drei Bereiche teilen:

- ✓ Absicherung der Kommunikation und Sicherheit der übertragenen Daten,
- ✓ Sicherstellung der Identität der Kommunikationspartner.

2.1 Absicherung der Kommunikation

Eine sichere Kommunikation muß mindestens den folgenden Kriterien genügen:

- Manipulation an den übertragenen Daten müssen erkannt und Sender und Empfänger mitgeteilt werden,
- die Vertraulichkeit der übertragenen Daten muß gewährleistet sein,
- der erfolgreiche Transport muß quittiert werden.

Hierzu können z.B. folgende Maßnahmen benutzt werden:

- Integritätssicherung: Um sicherzustellen, daß die übertragenen Daten nicht zufällig oder absichtlich verfälscht worden sind, können die Daten mit einer kryptographischen Prüfsumme versehen werden (z.B. Hashverfahren, Digitale Signaturen).
- Verschlüsselung: Um die Vertraulichkeit der übertragenen Daten sicherzustellen, können symmetrische (z.B. IDEA, Blowfish) oder asymmetrische (z.B. RSA, Elliptische Kurven) Verschlüsselungsverfahren benutzt werden.
- Quittierung: Zur Quittierung kann der Empfänger aus den empfangenen Daten einen Hashwert bilden und diesen anschließend digital signiert als Empfangsquittung zurücksenden. Hierdurch kann der Sender nachweisen, daß
  a) die Quittung vom Empfänger stammt (digitale Signatur) und
  b) dieser die Quittung nur durch Kenntnis der übermittelten Daten erstellen konnte (Hashwert).

- Durch Verwendung von dynamischen Schlüsseln, Transaktionsnummern oder Zeitstempeln kann sichergestellt werden, daß wiedereingespielte Nachrichten als solche erkannt und abgelehnt werden.

2.2 Sichere Identifikation der Kommunikationspartner

Zur Sicherstellung der Identität von Kommunikationspartnern werden üblicherweise sogenannte „Challenge-Response“-Verfahren eingesetzt. Das zugrundeliegende Prinzip hierbei ist wie folgt:

Person A (= Rechner A) möchte sich gegenüber Person B (Rechner B) als authentisch ausweisen. B kennt eine Eigenschaft von A, die nur A besitzt, z.B. ein nur A und B bekannter symmetrischer Schlüssel oder Person A kennt den geheimen und Person B den öffentlichen Schlüssel eines asymmetrischen Schlüsselpaares.

Im ersten Schritt sendet B an A eine neu gewählte Zufallszahl. Im zweiten Schritt verarbeitet A diese Zufallszahl mit dem symmetrischen bzw. asymmetrischen Schlüssel und sendet das Ergebnis an B zurück. B überprüft durch die Anwendung seiner Informationen, ob die von ihm gesendete Zufallszahl in der Antwort enthalten ist. Ist dies der Fall, so ist die Identität von A gewährleistet.

2.3 Literaturhinweise

- Bundesamt für Sicherheit in der Informationstechnik
  Sicherheitsaspekte bei Electronic Commerce
  Schriftenreihe zur IT-Sicherheit, Band 10
  Bundesanzeiger Verlag, 1999
- Bundesamt für Sicherheit in der Informationstechnik
  Sicherheitsaspekte bei Electronic Commerce
  Schriftenreihe zur IT-Sicherheit, Band 10
  Bundesanzeiger Verlag, 1999
- Martius, Kai
  Sicherheitsmanagement in TCP/IP-Netzen,
  Friedr. Vieweg & Sohn Verlagsgesellschaft mbH, 2000
- Raepple, Martin
  Sicherheitskonzepte für das Internet, dpunkt-Verlag, 1998

3 Internet-Protokolle

3.1 Netzwerkprotokolle

3.1.1 Adress Resolution Protocol (ARP)

IP-Adressen sind logische Zuordnungen auf der Netzwerkebene. Um den gewünschten Rechner, d.h. die dazugehörige Hardware zu erreichen, muß diese logische Zuordnung zur physikalischen Adresse aufgelöst werden. Diese Transformation zwischen IP- und physikalischer Adresse wird von ARP durchgeführt.

Die ARP-Implementierung hat hierbei zumindest zwei Aufgaben zu übernehmen:

- das Senden einer Anfrage (ARP-Request)
- die Beantwortung von Anfragen (ARP-Replys).

RARP (Reverse Adress Resolution Protocol) ist die inverse Zuordnung und wird insbesondere bei der dynamischen Vergabe von IP-Adressen beim Boot-Vorgang eines Rechners benutzt.

3.1.1.1 Sicherheitslücken

ARP- und RARP-Broadcasts werden nicht über die Grenzen eines lokalen Netzes hinweg ausgestreut, d.h. die Gefahren gehen auch nur von lokal angeschlossenen Systemen aus.

Ist es einem Rechner jedoch möglich, sich in ein lokales Netz einzuschalten („untrusted node“), kann dieser den Datenverkehr auf sich umleiten, indem er die Requests von seiner Hardwareadresse beantwortet (=“IP_Masquerading“).

3.1.2 Internet Protocol (IP)

IP ist das verbindungslose, ungesicherte Protokoll des Internets. IP bildet ein vom darunterliegenden Medium (ethernet, ISDN, ...) unabhängiges Datenpaket. Die Länge der Datenpakete ist nicht festgelegt, sondern hängt von dem benutzten Medium und seinen Übertragungseigenschaften ab. Das Paket trägt in seinem Datenkopf (= „Header“) Adressinformationen (Source- und Destination-IP-Adresse) sowie eine Vielzahl von zusätzlichen Feldern, die die Datenübertragung

beeinflussen. Mittels einer einfachen Checksumme werden Übertragungsfehler erkannt.

3.1.2.1 Sicherheitsrisiken

Da keine Authentisierungs- oder Integritätsprüfungen stattfinden, kann den Daten im IP-Header prinzipiell nicht vertraut werden. Die oben erwähnte Checksumme dient nur zum Erkennen von Übertragungsfehlern und kann von einem Angreifer leicht gefälscht werden. Hieraus folgt, daß basierend auf den Adressangaben des Headers keine sicherheitsrelevanten Entscheidungen (z.B. eine Authentisierung) getroffen werden dürfen.

Gleiches gilt natürlich für die übermittelten Nutzdaten. Sicherheit vor Fälschung bieten hier nur Maßnahmen der Kryptographie (siehe hierzu das Kapitelüber digitale Signaturen, 5.1.3). Das Ausspähen der Nutzdaten kann ebenfalls nur durch kryptographische Methoden verhindert werden (Kapitel 5 ff).

3.1.3 Internet Control Message Protocol (ICMP)

ICMP dient dazu, Fehlermeldungen, Steuerinformationen oder Statusmeldungen zu übertragen. ICMP ist kein egenständiges Übertragungsprotokoll, sondern nutzt das Datenfeld von IP zur Übertragung. ICMP-Datagramme werden wie alle anderen IP-Datagramme behandelt, sie besitzen also keine höhere Priorität.

3.1.3.1 Sicherheitsrisiken

Die durch ICMP-Botschaften („Messages“)ausgelösten Reaktionen können für Anfriffe auf ein Netz ausgenutzt werden, da die Botschaften das Verhalten der darüberliegenden Protokolle (TCP/UDP) beeinflussen.

Mittels der ICMP-Redirect-Message können Routinginformationen geändert werden. Deshalb dürfen solche Informationen nur von Endgeräten ausgewertet werden, und dies auch nur, wenn sie von einem Router desselben Subnetzes stammen.

3.2 Transportprotokolle

3.2.1 Port-Adressen

Eine IP-Adresse gibt das Ziel für meinen Datenverkehr an, nicht jedoch welche Anwendung (z.B. FTP, HTTP, ...) ich auf dem Zielrechner nutzen möchte. Um gleichzeitig mehrere Netzwerkdienste auf einem Rechner nutzen zu können, ist eine Zuordnung zwischen der Anforderung durch das IP-Datagramm und der Anwendung des Zielrechners notwendig. Dies geschieht bei TCP/IP durch sogenannte Ports.

Im Intra- bzw. Internet gibt es eine Anzahl sogenannter „wellknown“ Ports, die praktisch Ausschlieslich unter 1024 liegen. Die sogenannten „high-numbered“ Ports sind zum größten Teil verfügbar und stehen für die dynamische Vergabe zur Verfügung.

3.2.1.1 Sicherheitsrisiken

Den Daten von den wellknown-Ports wird in der Regel mehr vertraut als denen der restlichen Ports, weil diese Ports nur von Applikationen bedient werden, die entsprechende Rechte (meist Administrator- bzw. root-Rechte) auf der Maschine haben. Daher werden diese Ports auch privilegierte Ports genannt.

Auf Maschinen ohne Authentisierungsmechanismen (DOS /Windows) kann jedoch jeder diese Ports benutzen. Des weiteren ist fraglich, warum dem Administrator irgendeiner Maschine im Internet mehr vertraut werden soll als irgend einem anderem. Hieraus folgt, daß nur über die Port-Zuweisung keine gesicherte Verbindung aufgebaut werden kann.

3.2.2 User Datagram Protocol (UDP)

UDP ist eine Erweiterung des IP, die darin besteht, über die Übermittlung von Destination- und Source-Ports eine Zuordnung zu den Anwendungen auf dem Zielrechner zu erreichen. UDP-Pakete werden im Datenfeld von IP-Paketen transportiert. Jedoch enthält UDP keine Maßnahmen zur Verbindungssteuerung und ist damit ebenfalls ein verbindungsloser und ungesicherter Transportdienst.

3.2.2.1 Sicherheitsrisiken

UDP kennt weder Sequenznummern noch Prozeduren zum Verbindungsaufbau. Daher können UDP-Pakete weitaus einfacher gefälscht werden als TCP-Pakete. Die Angabe des Source-Ports ist optional, d.h. es läßt sich keine sichere Aussage über den Absender der UDP-Pakete durch die IP-Adresse oder des Ports durchführen. Daher müssen Anwendungen, die UDP zur Übertragung nutzen wollen, eigene Authentisierungsmechanismen implementieren.

3.2.3 Transmission Control Protocol (TCP)

TCP stellt im Gegensatz zu UDP einen verbindungsorientierten gesicherten Transportdienst zur Verfügung, der das IP zur Übertragung der Daten nutzt.

3.2.3.1 Sicherheitsrisiken

Oftmals wird bei Nutzung von TCP den wellknown-Ports ein hohes Vertrauen entgegengebracht. Hierbei gelten jedoch die schon zu den UDP-Sicherheitsrisiken erwähnten Bedenken.

Die Verbindungsaufbauprozedur des TCP ermöglicht einem Angreifer, eine Überlastung der Systemressourcen durchzuführen (= „Denial of Sevice“, DoS). Der Angreifer muß zu diesem Zweck nur hinreichend viele Anfragen zu einem Verbindungsaufbau senden, die Empfangsbestätigung des Zielsystems unbeantwortet lassen. Werden genügend solcher offenen Anfragen beim Zielsystem erzeugt, gehen die Systemressourcen aus und reguläre Verbindungsanfragen können nicht mehr beantwortet werden. In Reaktion auf derartige Syn-Flood-Attacken sind bei einigen Betriebssystemen (z.B. Windows NT 4.0, Windows 2000) Modifikationen der Behandlung von Verbindungsanfragen erfolgt.

Durch das Handshake-Protokoll beim TCP-Verbindungsaufbau ist es nicht ganz einfach, eine TCP-Verbindung mit einer gefälschten Source-Adresse zu etablieren. Jedoch wählen ältere Implementierungen von TCP neue Sequenznummern für den Verbindungsaufbau nicht wirklich zufällig, sondern erhalten diese durch Inkrementieren vorheriger Verbindungen. Hier muß der Angreifer lediglich eine regulären Verbindungsaufbau durchführen, um anschließend mit der inkrementierten Sequenznummer seinen Angriff zu starten.

Eine Abart der Sequenznummer-Attacke bildet das TCP-Hijacking. Hierbei steigt ein Angreifer in eine bestehende TCP-Verbindung ein und wirft einen der rechtmäßigen Teilnehmer aus der Verbindung heraus. Der Angreifer kann nun Daten an das Zielsystem senden, die für dieses von dem ursprünglichen Teilnehmer zu kommen scheinen. Schutz hiervor bietet nur eine kryptographische Verschlüsselung sämtlicher Nutzdaten, da diese unabhängig von der Rechtezuteilung seitens der TCP/IP-Verbindung besteht.

3.3 Anwendungsprotokolle

3.3.1 Simple Mail Transfer Protocol (SMTP)

SMTP ist das einem einfachen ASCII-Befehlssatz beruhende Übertragungsprotokoll für Email im Intra- / Internet.

3.3.1.1 Sicherheitsrisiken

Mit diesem ASCII-Befehlssatz kann man Mails von ei nem Email-Server abholen, aber auch volständige Mails schreiben – inklusive einer beliebigen Empfänger- und Absenderadresse. Bedingt durch diese Fälschungsmöglichkeiten kann den Adressen bei Emails daher generell nicht getraut werden.

Eine weiteres Sicherheitsrisiko besteht in der Implementierung des Programms „senmail“ auf vielen Unix-Systemen. Unabhängig von der möglichen Fehlkonfiguration (es gibt Bücher zu diesem Thema mit mehr als 500 Seiten) ist die Ausführung einiger Bestandteile des sendmail-Programmes mit root-Rechten bei vielen älteren Implementierungen, welche immer noch häufig im Einsatz zu finden sind. Oft kann hier eine Shell mit root-Privilegien eröffnet werden – welche Möglichkeiten sich hier ergeben, braucht hier wohl nicht diskutiert zu werden.

Ein weiteres Risiko sind die MIME-Erweiterungen (Multipurpose Internet Mail Extensions), welche den Inhalt einer Mail beschreiben. Über Hilfsprogramme ermöglicht die MIME-Erweiterung die Darstellung von Bildern, das Abspielen von Filmen usw. Hierbei kann es sich unter Umständen auch um ausführbare Programme handeln, daher sollten MIME-Erweiterungen nicht automatisch ausgeführt werden.

3.3.2 Telnet

Telnet bietet die Möglichkeit, sich über ein Netz auf einen entfernten Rechner anzumelden und über ein Terminal Befehle auf dem Zielrechner einzugeben. Diese Betriebsart ist nur in einem Multiuser- und Multitasking-fähigem Betriebssystem wie Unix durchzuführen.

3.3.2.1 Sicherheitsrisiken

Die Übertragung der zum Anmelden auf dem Host notwendigen User/Password-Kombination erfolgt im Klartext im Netz., d.h. es kann leicht abgehört und von einem Angreifer zu einem anderen Zeitpunkt verwendet werden.

Möglichkeiten, diese Sicherheitsrisiken zu verkleinern, bieten z.B. Einmalpasswörter wie s/Key, wobei das Passwort nur für eine einzige Sitzung gilt. In nicht vertrauenswürdigen Netzwerken sollte jedoch generell nur eine gesicherte Telnet-Sitzung (z.B. Secure Shell SSH, vgl. Kapitel 5.3.2) verwendet werden.

3.3.3 File Transfer Protocol (FTP)

FTP bietet die Möglichkeit, Daten zwischen einem FTP-Server und einem FTP-Client auszutauschen. Die Daten werden bei diesem Protokoll über einen eigenen Datenkanal übertragen. Standardmäßig verwendet ein FTP-Server die Ports 20 (Daten) und 21 (Steuerkanal).

3.3.3.1 Sicherheitsrisiken

„Anonymous ftp“ erlaubt allen Teilnehmern des Netzes Zutritt zum FTP-Server ohne Authentisierung. Die häufig verwendete Paßwortabfrage, bei welcher eine Email-Adresse einzugeben ist, kann unter dem Gesichtspunkt des Datenschutzes nicht als sicher eingestuft werden.

3.3.4 HyperText Transfer Protcol (HTTP)

Das World Wide Web (WWW) bedient sich bei der Übertragung von Informationen in Hypertext-Format dem HTTP. HTTP arbeitet auf Client/Server-Basis, wobei der HTTP-Server in der Regel auf Port 80 seinen Dienst anbietet. Für die Übertragung selbst nutzt HTTP TCP.

3.3.4.1 Sicherheitsrisiken

Eine sichere Nutzerauthentifizierung kann durch HTTP nicht gewährleistet werden. Dies kann nur durch kryptographische Verfahren (siehe Kapitel 5.3.3 über S-HTTP) erreicht werden. Daher muß der WWW-Server veifizieren können, ob ein file zum Transfer freigegeben ist. Beim Transfer von Daten mittels FTP meldet sich der HTTP-Server mit seiner IP-Adresse beim FTP-Server an, d.h. in der Regel wird diesen Anfragen vollständig vertraut.

Häufig wird eine dynamische Seitengestaltung gewünscht. Um dies zu realisieren, wird ein „Common Gateway Interface“ (CGI) implementiert, welches eine entsprechende Funktionalität bereit stellt. Mittels CGI werden mittels Scripten entsprechende Programme auf dem Server gestartet. Fehlerhafte Script-Implementierungen erlauben Angreifern die Aneignung von Zugrifsrechten auf den Server.

Clientseitig sind aktive WWW-Inhalte eine nicht zu unterschätzende Gefahr. Wird Java, Javascript, VBScript oder ActiveX im Browser ausgeführt, besteht die Gefahr der Datenmanipulation oder des Datenverlustes auf dem eigenen Rechner. ActiveX-Komponenten unterliegen, wurde Ihnen einmal Vertrauen ausgesprochen, zudem keinerlei Zugriffsbeschränkungen. Java-Programme (= „Applets“) sollten beim Aufruf durch den WWW-Browser nur in einer genau definierten Umgebung innerhalb des Client-Systems ausgeführt werden (= „Sandbox“). Implementierungsfehler führten jedoch immer wieder dazu, daß auch Java-Applets Schaden beim Anwender anrichten konnten.

3.4 Literaturhinweise

- Bundesamt für Sicherheit in der Informationstechnik
  Sicherheitsaspekte bei Electronic Commerce
  Schriftenreihe zur IT-Sicherheit, Band 10
  Bundesanzeiger Verlag, 1999
- Martius, Kai
  Sicherheitsmanagement in TCP/IP-Netzen,
  Friedr. Vieweg & Sohn Verlagsgesellschaft mbH, 2000
- Raepple, Martin
  Sicherheitskonzepte für das Internet, dpunkt-Verlag, 1998

4 Schutzmechanismen

4.1 Hostabsicherung

Ist der Rechner nicht vernetzt, kann eine Absicherung relativ leicht erfolgen, da ein Zugriff lediglich physisch erfolgen kann. Sollen mehrere Benutzer an dem REchner arbeiten, muß das eingesetzte Betriebssystem zudem über eine entsprechend sichere Benutzerverwaltung verfügen, mit welchem den einzelnen Benutzern die jeweils benötigten Rechte verliehen werden können. Der Systemverwalter (Administrator, Superuser, Root) dieses Rechners, welcher die Zugriffsrechte auf die jeweiligen Benutzer einteilt, kommt eine besondere Verantwortung zu.

Verfügt der Computer über eine Netzanbindung, so muß zusätzlich der Netzwerkzugang abgesichert werden. Generell gilt, daß alle Dienste, die über das Netzwerk bereitgestellt werden, Gefahren für die Datenintegrität und die Datensicherheit darstellen. Jeder Dienst bietet potentiell die Möglichkeit, daß sich ein Angreifer die Rechte des Systemverwalters aneignet.

4.2 Verbindungsabsicherung

Eine Vernetzung von Computern ergibt nur dann Sinn, wenn Daten zwischen den einzelnen Computern ausgetauscht werden. Um diese Daten während der Übertragung zu sichern, muß die Verbindung zwischen den vernetzten Rechnern entsprechend gesichert sein. Generelle Angriffsmöglichkeiten bietet die physische Verkabelung, die einem Angreifer das Abhören den Kommunikation erlaubt, oder genutzte Vermittlungssysteme wie Router, Switches usw.

Befinden sich alle Kabel und Vermittlungseinrichtungen in einem kontrollierten, Bereich, kann dieser Bereich gesichert werden. Normalerweise werden die Daten jedoch über öffentliche Leitungen und Vermittlungssysteme (Telefongesellschafte, Internet, etc.) übertragen und müssen daher als ungesichert gelten.

4.2.1 Physische Verbindungssicherung

Link-Verschlüsselung gewährleistet die Datensicherheit auf einer physischen Verbindung. Hierzu werden i.d.R. „Kryptoboxen“ eingesetzt, die eine für die Netzwerkschicht transparente Verschlüsselung bieten, d.h. es können sämtliche Netzwerkverbindungen (IPX, TCP/IP, AppleTalk usw.) genutzt werden. Die Sicherheit

wird hierbei natürlich nur zwischen den Kryptoboxen auf diesem einen Link gewährleistet. Der große Nachteil dieser Methode ist, daß für jede physische Leitung jeweils zwei kompatible Geräte benötigt werden und der Aufwand für größere Netze entsprechend erhöht wird.

4.2.2 Logische Verbindungssicherung

Definiert man eine Verbindung als „Virtuelle Verbindung“ auf der Netzwerkschicht, ergeben sich neue Aspekte für den Schutz der zu übertragenden Daten. Die Sicherheitsmechanismen können bereits Funktionen der Netzwerk nutzen, sind unabhängig vom physikalischen Medium und sind in der Regel ohne (teure) zusätzliche Hardware realisierbar.

Nachteilig ist jedoch, daß diese (virtuell) implementierten Sicherheitsfunktionen protokollabhängig und verbindungslose Transportdienste nicht (bzw. nur durch zusätzliche Maßnahmen) gesichert sind. Zusätzlich benötigen Protokoll-Steuerinformationen zusätzliche Sicherungen.

4.3 Netzabsicherung

Bei der Netzabsicherung sollten generell einige administrativen Probleme bedacht werden:

- eine unternehmensweite Sicherheits-Policy ist nur mit enorm hohem Aufwand durchsetzbar,
- die Administration wird sehr kompliziert, d.h. komplex und fehlerträchtig
- durch evtl. unter den Hosts bestehende Vertrauensverhältnisse kann dieses System überbrückt werden.

4.3.1 Paketfilter

Paketfilter-Systeme routen Pakete zwischen internen und externen Rechnern. Sie gehen dabei allerdings selektiv vor: sie lassen bestimmte Pakettypen passieren oder blockieren sie auf eine Art, die die Sicherheitspolitik eines Standortes widerspiegelt. Der in einem Paketfilter-Firewall verwendete Routertyp wird Überwachungsrouter genannt.

Jedes Paket besitzt eine Anzahl von Headern mit speziellen Informationen. Die wichtigsten sind:

- IP_Quelladresse
- IP-Zieladresse
- Protokoll (TCP-, UDP- oder ICMP-Paket?)
- TCP- oder UDP-Quellport
- TCP- oder UDP-Zielport
- ICMP-Nachrichtentyp.

Zusätzlich sind dem Router Informationen über das Paket bekannt, die sich nicht in den Headern zeigen, z.B.:

- die Schnittstelle, an der das Paket ankommt
- die Schnittstelle, an der das Paket herausgeht.

Da die Server bestimmter Internet-Dienste feststehende Portadressen abhören, kann der Router bestimmte Verbindungstypen blockieren oder passieren lassen. Dazu wird im Regelsatz für die Paketfilterung einfach die entsprechende Portadresse angegeben, z.B. TCP-Port 23 für Telnet-Verbindungen.

Typische Schutzmechanismen, die in den Regeln implementiert werden, sind:

- Blockieren aller Verbindungen von Systemen außerhalb des internen Netzes; lediglich eintreffende SMTP-Verbindungen dürfen passieren, damit Email empfangen werden können.
- Blockieren aller Verbindungen von und zu Systemen, die suspekt erscheinen.
- Email und FTP-Dienste aktivieren, aber riskante Dienste blockieren (z.B. TFTP, X-Window-System, RPC, r-Dienste: rlogin, rsh, rcp usw.).

4.3.1.1 Unterschied „normaler„ Router und Überwachungsrouter

Ein normaler Router sieht sich einfach die Zieladresse eines jeden Pakets an und wählt den besten ihm bekannten Weg aus, um das Paket in Richtung seines Bestimmungsortes zu senden. Wie das Paket zu behandeln ist, wird nur vom Zielort bestimmt. Wenn der Router weiß, wie er das Paket in Richtung seines

Bestimmungsortes senden kann, so tut er dies. Andernfalls gibt er das Paket mit der ICMP-Nachricht „destination unreachable„ an den Ursprungsort zurück.

Ein Überwachungsrouter dagegen sieht sich die Pakete genauer an. Er entscheidet nicht nur, ob er ein Paket in Richtung des Zielorts routen kann, sondern auch, ob er es überhaupt soll. Welche Pakete er routen soll und welche nicht, wird von der Sicherheitspolitik des Standortes bestimmt, für die der Überwachungsrouter konfiguriert ist.

Wird lediglich ein Überwachungsrouter zwischen das interne Netz und das Internet gestellt, übernimmt der „Regel-Designer„ damit eine enorme Verantwortung. Der Überwachungsrouter muß nicht nur das gesamte Routing durchführen und alle damit einhergehenden Entscheidungen treffen, sondern bildet zudem das einzige Schutzsystem. Dies ist in der Regel aber unzureichend. Außerdem kann ein einfacher Überwachungsrouter keine Dienste modifizieren. Er kann einen Dienst zulassen oder ablehnen, aber Operationen innerhalb eines Dienstes nicht einzeln schützen. Wenn ein an sich wünschenswerter Dienst unsichere Operationen enthält oder der Dienst an einem unsicheren Server angeboten wird, bieten Paketfilter allein keinen Schutz.

4.3.1.2 Sicherheitsrisiken

Ist die Anzahl der angeschlossenen Nutzer groß, wird die Konfiguration schwierig und fehlerträchtig, denn die Filtertabellen werden schnell unübersichtlich.

4.3.2 Application Level Gateway – Proxy Gateways

Proxy-Dienste sind spezielle Anwendungs- oder Serverprogramme, die auf einem Firewall-Host ablaufen: entweder auf einem Dual-Homed-Host mit einer Schnittstelle zum internen und einer zum externen Netz oder auf einem anderen Bastion-Host, der Zugang zum Internet hat und von den internen Rechnern aus angesprochen werden kann. Diese Programme greifen die Benutzeranfragen nach Internet-Diensten wie FTP oder Telnet auf und leiten sie an die eigentlichen Dienste weiter, sofern sie mit der Sicherheitspolitik des Standorts vereinbar sind. Die Proxies stellen Ersatzverbindungen her und fungieren als Gateways zu den Diensten. Deshalb werden Proxies auch manchmal als „Application-Level-Gateways„ bezeichnet.

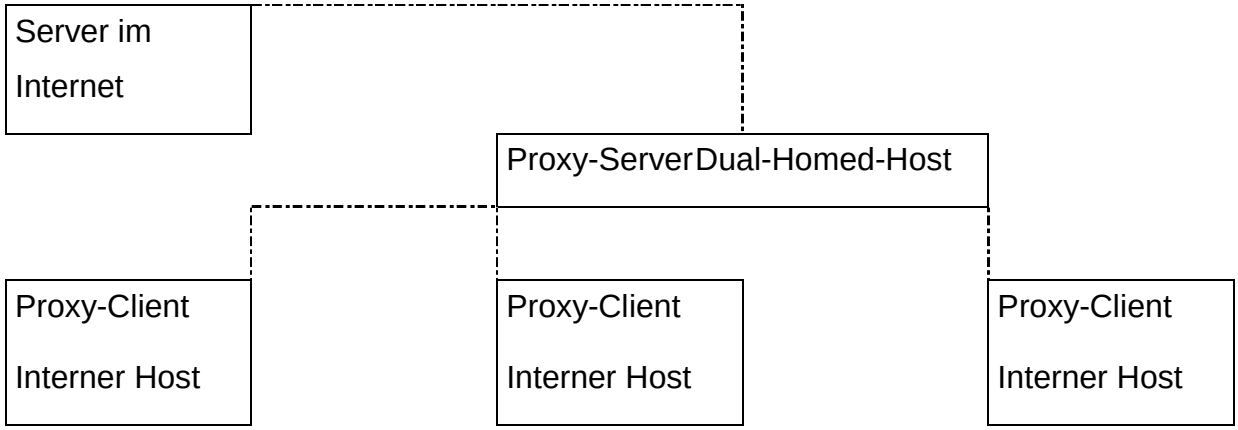
Proxy-Dienste befinden sich, mehr oder weniger sichtbar, zwischen einem Benutzer im Inneren (im internen Netz) und einem Dienst außerhalb (im Internet). Anstatt sich direkt miteinander zu unterhalten, verständigen sich Benutzer und Dienst über einen Proxy. Die Proxies steuern aus dem Hintergrund die gesamte Kommunikation zwischen Benutzern und Internet-Diensten.

Ein wesentlicher Vorteil von Proxies besteht darin, daß sie dem Benutzer gegenüber verborgen bleiben - sie sind völlig getarnt. Ein Proxy-Server vermittelt dem Benutzer den Eindruck, daß dieser direkt mit dem eigentlichen Server kommuniziert. Und gegenüber dem wirklichen Server tut der Proxy-Server so, als befände sich der Benutzer direkt auf dem Proxy-Host.

Proxy-Dienste sind jedoch nur wirksam, wenn sie in Kombination mit einem Mechanismus eingesetzt werden, der die direkte Kommunikation zwischen internen und externen Rechnern beschränkt. Dual-Homed-Hosts und Paketfilterung sind solche Mechanismen. Wenn interne und externe Computer direkt miteinander kommunizieren können, müssen Benutzer die Proxy-Dienste nicht unbedingt verwenden und tun es dann (im allgemeinen) auch nicht.

4.3.2.1 Funktionsweise von Proxy-Diensten

Ein Proxy-Dienst benötigt zwei Komponenten: einen Proxy-Server und einen Proxy-Client. Der Proxy-Server kann beispielsweise auf einem Dual-Homed-Host laufen. Ein Proxy-Client ist die spezielle Fassung eines normalen Client-Programmes, d.h. eines Telnet- oder FTP-Clients, der sich statt mit dem wirklichen Server im Internet mit dem Proxy-Server unterhält.



Proxy-Dienste bei einem Dual-Homed-Host

Oft können normale Client-Programme als Proxy-Clients eingesetzt werden, sofern Benutzer eine spezielle Anleitung erhalten. Der Proxy-Server wertet die Anfragen vom Proxy-Client aus und entscheidet, welche zu bestätigen und welche abzulehnen sind. Nach Bestätigung der Anfrage nimmt der Proxy-Server anstelle des Clients Kontakt zum eigentlichen Server auf (Proxy = Stellvertreter) und übermittelt nachfolgende Anfragen und Antworten zwischen Proxy-Client und dem eigentlichen Server.

4.3.2.2 Proxy-Server im Firewall-Einsatz

Ein Proxy-Dienst ist eine Software-Lösung und nicht schon an sich eine Firewall-Architektur. Allerdings können Proxy-Dienste in Kombination mit allen Firewall-Architekturen eingesetzt werden.

Der Proxy-Server leitet die Anfragen vom Benutzer nicht immer einfach an die eigentlichen Internet-Dienste weiter. er kann die Aktionen der Benutzer steuern, da er über die von ihm bearbeiteten Anfragen entscheiden kann. Entsprechend der Sicherheitspolitik des Standortes können Anfragen zugelassen oder abgelehnt werden. Der FTP-Proxy könnte beispielsweise unterbinden, daß Benutzer Dateien exportieren oder den Import von Dateien nur von bestimmten Standorten gestatten. Komplizierte Proxy-Dienste sind in der Lage, rechnerspezifisch unterschiedliche Aktionen zu erlauben, so daß eine Einschränkung nicht für alle Rechner gelten muß.

SOCKS (ftp://ftp.nec.com/pub/security/socks.cstc/ bzw. ftp://coast.cs.purdue.edu/pub/tools/unix/socks/) ist ein Toolkit für den Aufbau von Proxies, das eigens dafür entworfen wurde, die Umwandlung bestehender Client-/Server-Anwendungen in Proxy-Versionen zu erleichtern. Das „Trusted Information Systems Internet Firewall Toolkit„ (TIS FWTK, ftp://ftp.tis.com/pub/firewalls/toolkit/) enthält Proxy-Server für zahlreiche gängige Internet-Protokolle, darunter Telnet, FTP, HTTP, rlogin und X11. Diese Proxy-Server sind so konzipiert daß sie in Kombination mit eigens für die Benutzer erstellten Prozeduren verwendet werden können.

4.3.2.3 Sicherheitsrisiken

Der Einsatz von Application-Level-Gateways wie dem Microsoft Proxy-Server bedingt den Einsatzmodifizierter Clientprogramme, da eine direkte Verbindung zum Server

nicht möglich ist, sondern über das Gateway geleitet wird. D.h. die Clients müssen Kenntnis von diesem Gateway haben und die Anfragen über dieses Gateway leiten.

4.3.3 Kombinationsformen

Die „richtige„ Lösung für den Aufbau eines Firewalls besteht selten aus einer einzigen Technik; es ist meist eine geschickt gewählte Kombination zur Lösung unterschiedlicher Probleme. Für welche Probleme Lösungen gefunden werden müssen, hängt davon ab, welche Dienste den Benutzern angeboten werden sollen und in welchem Maße dabei Risiken in Kauf genommen werden können.

Einige Protokolle wie z.B. Telnet und SMTP eignen sich gut für die Paketfilterung. Andere wie z.B. Archie, Gopher und WWW lassen sich effektiver mit Proxies bearbeiten. Die meisten Firewalls verwenden eine Kombination aus Proxy-Diensten und Paketfilterung.

4.3.4 Virtuelle Private Netzwerke (VPN)

Moderne Unternehmensstrukturen und neue Arbeitsformen wie Telearbeit und Mobile Computing benötigen eine anpassungsfähige Informationstechnologie, welche die Sicherheit der Daten des Unternehmens gewährleisten und zugleich die Kommunikationsanforderungen der miteinander kooperierenden Organisationseinheiten erfüllen muß. Vor diesem Hintergrund bieten sogenannte „Virtuelle Private Netzwerke“ eine Möglichkeit zur Realisierung der Anforderungen. VPNs ermöglichen die transparente Kopplung zwischen dem LAN im Unternehmen und seinen Außenstellen bzw. Geschäftspartnern.

4.3.4.1 Arbeitsweise

Ein virtuelles privates Netz ist ein Verfahren, in einem öffentlichem Netz wie dem Internet ein privates Netz zu simulieren. Es wird virtuell genannt, weil es sich auf eine virtuelle Verbindung stützt, d.h. die Verbindung stützt sich nicht auf ein physisches Vorhandensein, sondern sie besteht aus Paketen, die über verschiedene Rechner im Internet ohne fest vorgegebene Route übertragen werden. Sichere virtuelle Verbindungen können zwischen zwei Rechnern, zwischen einem Rechner und einem Netz oder zwischen zwei Netzen aufgebaut werden.

Mit virtuellen privaten Netzen läßt sich die Reichweite eines Intranet vergrößern. Da Intranets normalerweise für firmeninterne Informationen verwendet werden, sollen sie in der Regel vom Internet aus nicht sichtbar sein. In manchen Fällen ist es aber wünschenswert, Daten auch mit weit verstreuen Filialen zu nutzen oder fernen Benutzern über das Internet Zugang zum Intranet zu erlauben.

In einem VPN können verschiedene Techniken zum Schutz der Datenübertragung eingesetzt werden:

- Firewalls
- Benutzer- / Rechnerauthentifizierung
- Verschlüsselung
- Tunneling.

Durch Tunneling läßt sich ein IP-Paket in ein anderes IP-Paket kapseln. Dies bietet die Möglichkeit, Pakete mit beliebigen Ziel- und Quelladressen im Internet zu verschicken, da diese wiederum in Pakete untergebracht sind, deren Ziel- und Quelladressen geroutet werden können. So kann auch der reservierte, im Internet nicht-routingfähige IP-Adressbereich verwendet werden.

4.3.4.2 Protokolle im VPN

4.3.4.2.1 IPSec

Das Internet Security Protocol (IPSec, siehe Kapitel 5.3.6) bietet ein Grundgerüst, welches verschiedene Sicherheitsdienste für das Internet Protocol (IP) – sowohl für IPv4, den aktuellen Standard, als auch für IPv6 – bereitstellen soll. IPSec definiert keine speziellen Verschlüsselungsalgorithmen oder Schlüsselaustauschverfahren, sondern liefert nur den Rahmen für eine modulare Sicherheitsstruktur.

Da IPSec zur Absicherung des zugrundeliegenden Netzes dient, können Anwendungen unverändert ausgeführt werden. Bei IPSec gibt es zwei Verschlüsselungsmodi. Im Transportmodus wird nur der Nachrichtentext, im Tunnelmodus dagegen sowohl der Nachrichtentext als auch der Header des Pakets geschützt. Damit IPSec funktioniert, müssen alle beteiligten Geräte über einen gemeinsamen Schlüssel verfügen.

Zum Aufbau eines Tunnels zwischen zwei Netzen mit IPSec müssen beide Gateways ähnliche Sicherheitsstrategien verfolgen. Bei unterschiedlichen Strukturen besteht die Gefahr, daß eines der Netze weniger sicher ist und nach einem erfolgreichen Angriff das andere Netz kompromittiert.

4.3.4.2.2 Point-to-Point Tunneling Protocol (PPTP)

Das PPTP stellt eine Erweiterung des Point-to-Point Protocol (PPP) dar. Die Tunneling-Dienste von PPTP sind über der IP-Schicht angesiedelt, während das traditionelle PPP unter IP liegt. Bei PPTP handelt es sich am ehesten um einen rechnerorientierten Kommunikationskanal, d.h. es wird eine gesicherte Rechner-zu-Rechner Verbindung hergestellt.

4.3.4.3 Methoden zur Kompromittierung von VPNs

Es gibt bisher nur wenige Untersuchungen bezüglich des Einsatzes von VPNs in produktiven Umgebungen. Entsprechend wenig Gelegenheiten gab es bisher, die Sicherheit von VPNs „in the wild“, d.h. im reellen Einsatz zu testen.

Ein Beispiel einer solchen Analyse ist jedoch die aus dem Juni 1998 stammende Kryptoanalyse von Bruce Schneider und Peter Mudge (Letzterer Mitglied der Hacker-Gruppe L0pht, heute L0pht Heavy Industries) der Implementierung von PPTP durch die Firma Microsoft.

AlephOne, der die Mailingliste Bugtraq leitet, entdeckte weitere Sicherheitslücken von PPTP, einschließlich der Idee, einen PPTP-Server zu imitieren (=“spoofen“), um die Beglaubigungsinformationen abzufangen.

Obwohl sich diese Veröffentlichung von Schneider/Mudge lediglich auf die Microsoft-spezifische Implementierung von PPTP bezieht, zeigen die Bemühungen doch deutlich, was die Kombination eines guten Kryptoexperten (Schneider) und einem gewieften Hacker (Mudge) bei einem als sicher geltendem Protokoll leistet. Draußen im Internet gibt es fähige Hacker, die gewillt und in der Lage sind, VPN-Technologien trotz der guten Sicherheitsvorkehrungen zu kompromittieren.

4.4 Firewall-Authentifizierungsmechanismen

Um innerhalb eines Paketfilters bzw. eines Application Level Gateways zu entscheiden, welche Filterregel angewendet werden muß, ist eine Identifizierung des Zugreifenden erforderlich.

4.4.1 IP-Adressen / Ports

Am häufigsten erfolgt die Identifizierung des Zugreifenden anhand der IP-Adresse, d.h. die Regeln basieren auf die Source- und Destination- Adresse. Diese Lösung weist jedoch einige Sicherheitslücken auf:

- IP-Adressen können gefälscht werden. An Rechnern ohne abgestufte Zugangsberechtigungen kann jeder die eigene IP-Adresse zu Gunsten einer anderen, basierend auf den Regeln der Firewall höher gestellten IP-Adresse abändern. Ist der Rechner mit der „gestohlenen“ IP-Adresse nicht in Betrieb oder wird mittels einer „Denial of Service“-Attacke außer Betrieb gesetzt, fällt diese Manipulation zunächst nicht auf. Weiterhin kann die Source-Adresse im IP-Paket manipuliert werden, so daß die IP-Adresse des eigentlichen Senders nicht mehr zu erkennen ist.
- Auf den wellknown-Ports werden in der Regel fest definierte Dienste bereitgestellt, wie z.B. Port 80 für das WWW. Diese Zuordnung kann jedoch beliebig verändert werden, so daß auf diesen „privilegierten“ Ports dann nicht die erwarteten Dienste zu finden sind. Noch schwieriger wird die Filterung an Hand der vom Client eingesetzten Ports. Diese sind bei vielen Diensten nicht vorher bestimmbar, da ein Client den eigenen Port häufig zufällig auswählt. Daher müssen in den Filterregeln dann ganze Bereiche bereitgestellt werden.
- Die Verwendung dynamischer IP-Adressen läßt die Filterung basierend auf die IP-Adresse praktisch völlig versagen, da heute fast keines der kommerziell erhältlichen Router und Application Level Gateways dynamische Filterregeln unterstützen.
- Der Einsatz von symbolischen Namen statt IP-Adressen zwingt zur Verwendung eines DNS-Servers, was die ganze Angelegenheit jedoch noch um einen weiteren Faktor unsicherer macht. Der Angreifer muß nur den

DNS-Server manipulieren, um eine falsche Zuordnung zwischen Namen und IP-Adresse zu erreichen.

Die hier aufgeführten Filterregeln berücksichtigen nur IP-Adressen und Ports, nicht jedoch den darauf angemeldeten Benutzer. Auf Multiuser-Betriebssystemen wie Unix oder Windows NT kann ein Router oder ein Application Level Gateway jedoch nicht festgestellt werden, welcher Benutzer angemeldet ist und den gewünschten Dienst nutzen will.

4.4.2 Anwender/Anwendungen

Auf der Anwendungsebene ist eine Nutzeridentifizierung möglich, was von reinen Paketfiltern nicht gewährleistet werden kann. Firewall-Systeme stellen aus diesem Grund häufig Mechanismen bereit, die eine Nutzerauthentifizierung gegenüber dem Firewall-System ermöglichen. Hierzu wird heute im Prinzip ausschließlich das Private-Key-Verfahren eingesetzt. Als Paradebeispiel für das Private-Key-Verfahren wird häufig das Kerberos-System angeführt, dessen Einsatz sich nicht auf die Authentifizierung in Firewall-Systemen beschränkt. Mittlerweile existiert auch eine Public-Key-Variante des Kerberos-Systems. Das Kerberos-Protokoll basiert auf dem Client-Server-Prinzip und benötigt einen vertrauenswürdigen Kerberos-Server (= „Trusted Third Party“), der eine Datenbank mit den Clients und deren geheimen (private) Keys unterhält. Kerberos besitzt jedoch einige Sicherheitsmängel:

- Die Gültigkeitsdauer eines sogenannten „Tickets“ (= Zulassung eines bestimmten Clients zu einem Server) beträgt im Allgemeinen acht Stunden, d.h. benutzte Tickets können von einem Angreifer benutzt werden, um einen unberechtigten Zugriff auf den Server zu erlangen.
- Die Sicherheit von Kerberos hängt durch die Verwendung von Zeitstempeln stark von einer synchronisierten, sicheren Zeit zwischen Clients, Servern und dem Kerberos-Server ab. Durch das Network Time Protocol, welches Systemzeiten im Netzwerk synchronisiert, ist es einem Angreifer relativ einfach möglich, die Zeit zu fälschen.
- Einige Tickets werden ohne Zufallsanteil erstellt, dadurch ist es einem Angreifer, der genügend Tickets gesammelt hat, möglich, ein neues Ticket zu erraten.

Public-Key-Verfahren zur Authentifizierung sind wesentlich flexibler und bei richtigem Einsatz auch sicherer als Private-Key-Verfahren. Der Einsatz von Public-Key-Verfahren ist im Umfeld von Firewall-Systemen zur Zeit jedoch noch nicht weit verbreitet.

4.5 Remote Access Service

Das klassische Remote-Access-Verfahren ermöglicht eine Zugangsmöglichkeit in ein Unternehmensnetz über öffentlich nutzbare Leitungen, wie z.B. das analoge Telefonnetz, ISDN oder ADSL. Als Einwahlknoten werden Modem-Pools oder ISDN-Router (= „RAS-Server „) installiert. In eine RAS-Server müssen Sicherheitsmechanismen wirken, die eine sichere Authentifizierung des Anrufenden gewährleisten. Erste Schritte zur Remote-Access-Sicherheit sind

a) Rufnummernüberprüfung,

b) genutzte Dienstmerkmale im ISDN,

c) Callback-Funktionen.

Mit diesen Möglichkeiten wird zunächst nur der jeweilige Telefonanschluß identifiziert (analog der Identifizierung des Rechners an Hand seiner IP-Adresse), nicht jedoch der Anrufer selbst.

4.5.1 Password Authentication Protocol (PAP)

PAP überträgt die Anmeldeinformationen (Nutzername, Paßwort) im Klartext und ohne eine weitere Sicherung zum Server, welcher die Daten mit seinen gespeicherten Informationen vergleicht und die Verbindung entsprechend des Vergleichsergebnisses zuläßt oder ablehnt. PAP bietet keinerlei Schutz gegen Abhören, Wiedereinspielen von Authentisierungsinformationen, Datenfälschung usw.

4.5.2 Challenge Handshake Authentication Protocol (CHAP)

CHAP führt zur Authentifizierung einen „3-Wege-Handshake“ durch. Dabei wird zunächst nur eine einseitige Authentifizierung durchgeführt, grundsätzlich kann das Protokoll jedoch auch für eine gegenseitige Authentifizierung genutzt werden.

Die Sicherheitsfunktion von CHAP ist im Prinzip sehr einfach gehalten: ein vom RAS-Server bereitgestellter Zufallswert und ein Passwort werden zusammen von einer

Hash-Funktion auf dem Client verarbeitet. Die Hash-Funktion garantiert, daß das geheime Paßwort aus den übertragenen Daten nicht mehr zurückgewonnen werden kann. Stimmen Hashwert von Client und Server überein, ist die Identifikation des Client sichergetsellt.

4.5.3 PPP Encryption Control Protocol (ECP)

Das Encryption Control Protocol stellt ein Verfahren zur Verschlüsselung von Nachrichten bzw. Verbindungen via PPP dar. Zunächst werden die Übertragungsparameter durch das Link Control Protocol konfiguriert. Anschließend werden auf beiden Seiten der Verbindung die zu verwendenden Algorithmen und Schlüssellängen abgestimmt. Prinzipiell ist es möglich, unterschiedliche kryptographische Verfahren für jede Verbindungsrichtung zu benutzen.

Entsprechend dem RFC 1968 werden den Algorithmen eindeutige Bezeichner zugeordnet. Der Empfänger der Nachrichten führt – entsprechend seinen Präferenzen – eine Liste der von ihm unterstützten Algorithmen, welche er dem Sender in Form einer configure-request-Anfrage schickt. Aus dieser Liste wählt der Sender den von ihm bevorzugten Algorithmus aus und schickt die Nachricht mit seiner Wahl zurück an den Empfänger als configure-Ack-Nachricht. Findet der Sender kein geeignetes oder unterstütztes Verfahren, erfolgt ein Verbindungsabbruch durch den Sender mittels einer configure-reject-Nachricht.

4.5.4 Remote Authentication Dial in User Service (Radius)

Radius definiert den Nachrichtenaustausch zwischen RAS und einem Administrationsrechner, dem Radius-Server. Der Radius-Server verwaltet alle Benutzer- und Konfigurationsdaten (zentralisierte Datenverwaltung). Das in RFC 2138 beschriebene Protokoll hat sich mittlerweile zum de-facto-Standard für die Anbindung von Heimarbeitsplätzen in Firmen etabliert. Insbesondere die Möglichkeit des zentralen Accounting bietet den Arbeitgeber die Möglichkeit der Protokollierung aller Verbindungen und der entsprechenden Onine-Zeiten entsprechend den Benutzerkonten. Ein Radius-Accounting-Protokoll benhaltt unter anderem den Benutzernamen, die IP-Adresse des RAS sowie de Dauer der Sizung in Sekunden. Eine Implementierung des Radius-Server ist für viele Unix-Plattformen und Windows NT kostenlos im Internet verfügbar.

Das Client/Server-Modell bietet eine skalierbare Lösung für die in einem Unternehmen ansteigende Benutzerzahl. Ebenso werden die zwischen Kommunikations- und Radius-Server übertragenen Daten verschlüsselt. Hierzu ist jedem RAS ein eigener symmetrischer Schlüssel zugeordnet, welcher zur Codierung der Nachrichten und zugleich zur Identifikation der RAS-Station gegenüber dem Radius-Server benutzt wird. Hierbei unterstützt das Protokoll eine Vielzahl von Mechanismen zur Authentifikation der Benutzer bzw. der RAS-Clients, wobei die Offenheit gegenüber neuen Verfahren gewahrt bleibt. Zur Zeit reicht das Spektrum von wiederverwendbaren Paßwörtern bis zu ausgereiften Challenge-Response-Verfahren, wo mitunter Soft- und Hardware von Drittanbietern genutzt werden.

4.5.4.1 Sicherheitsbedenken

Nicht nur der RAS-Zugang selbst sondern auch der Radius-Server muß gegen interne und externe Angriffe abgesichert werden, um die Gesamtsicherheit des Systems zu gewährleisten. Insbesondere ist auf eine sorgfältige Vergabe von Lese- und Schreib-Rechten für die Dateien der Datenbank zu achten. Da diese Dateien im Kartext (Benutzername, RAS-Paßwort) im Klartext vorliegen, darf nur der Administrator des Radius-Server darauf Zugriff haben.

4.5.5 Terminal Access Control System (Tacacs+)

Tacacs arbeitet ähnlich wie Radius und wird hauptsächlich von Cisco-Routern verwendet. Auch hier wird die Benutzerverwaltung auf einen xternen Server verlagert, auf welchem eine Software (typischerweise der frei erhältliche „tacacsd“ für Unix-Systeme) läuft.

Hintergrundinformationen hierzu findet amn im RFC 1492. Eine kommerzielle Implementierung von Tacacs+ und Radius ist CiscoSecure Server von Cisco.

4.5.6 Sicherheitsbedenken

Der Angriff auf Einwahlknoten wird weitestgehend wie jeder andere Angriff vorbereitet: Footprint erstellen (d.h. Identifizierung der Rufnummern), Scannen, Auswet´rten und Ausbeuten. Dieser ganze Vorgang kann mit traditionellen Hacking-Tools, den sogenannten Wardialer oder Demon-Dialer automatisiert werden.

Bei der Wahl einer Standard-Zeitüberschreitung von 45 bis 60 Sekunden – eine geringere Zeitwahl bedeutet, daß eventuell Leitungen auf Grund von Belegung oder schlechter Leitungsqualität übersehen werden – schafft ein Wardialer im Durchschnitt etwa einen Anruf je Minute und Modem. Ein Nummernblock aus 10 000 Telefonnummern kann daher von einem Modem in etwa 7 Tagen durchgescannt werden. Die Erkennung von „Voice“-Leitungen geben der Wardialer-Software die Möglichkeit, direkt aufzulegen, ohne eine bestimmte Zeitüberschreitung (45 bis 60 Sekunden) abzuwarten. Da es sich in der Regel bei einem großen Teil der angewählten Leitungen um Voice-Leitungen handelt, wird die Gesamtdauer der Wardialer-Attacke stark verkürzt.

4.5.6.1 Wardialer

Bei Wardialern geht es in erster Linie um die Auswahl der Tools. Als Freeware sind ToneLoc, THC-Scan oder der deutsche Modem-Hunter verfügbar. Die Freeware-Tools laufen unter Dos und setzen für komplexere Konfigurationen Kenntnisse im Umgang mit COM-Schnittstellen voraus. Desweiteren funktionieren die Tools auch nicht in jeder Konfiguration. Die Verwendung einer PCMCIA-Kombokarte in einem Notebook wird eventuell nicht unterstützt.

Die kommerzielle Software PhoneSweep bietet eine graphische Benutzeroberfläche, eine automatische Zeitplanung, automatische Träger-Infiltrierung mit gleichzeitiger Unterstützung von mehreren Modems und eleganten Berichtsfunktionen. PhoneSweep erkennt automatisch etwa 120 unterschiedliche Marken und Modelle von Remote-Access-Geräten. Desweiteren unterstützt PhoneSweep einen Wortlisten-Angriff auf die identifizierten Modems. Eine integrierte SQL-Datenbank, in welcher die Ergebnisse der Anrufe der benutzten Modems protokolliert werden, erleichtert die spätere Auswertung. Nähere Informationen zu PhoneSweep erhält man unter http://www.sandstorm.net/phonesweep/sysids.shtml.

Die Auswertung der Wardialer-Attacke durch die Ergebnisprotokolle erlaubt dann eine weitere Attacke. Ersieht man aus dem Ereignisprotokoll eine Meldung wie

```
17-03-2000 17:37:33 Dialing... 08 15 47 11
CONNECT 57600
HP995-400:_
Expected a HELLO command. (CIERR 6057)
```

so ist schnell der HP-Server im Hintergrund („HP995-400“) entlarvt. Kennt sich der Eindringling nun auch noch mit den MPE-XL MDT-Systemen von Hewlett-Packard aus, weiß er, daß die Login-Sequenz „HELLO USER.ACCT“ lautet, gefolgt von einem Paßwort bei Erscheinen der Eingabeaufforderung. Mit den Kenntnissen über typische Standartkonten und Paßwörter bei HP (z.B. „FIELD.SUPPORT“ und „TeleSup“) kann er nun einen Login versuchen:

```
17-03-2000 17:37:33 Dialing... 08 15 47 11
CONNECT 57600
HP995-400: HELLO FIELD.SUPPORT
PASSWORD= TeleSup
```

4.6 Sicherheitskonzepte gegen Viren

Die aus einem Virenbefall resultierenden Kosten lassen sich nur schwer beziffern. Sie sind maßgeblich von der Verbreitung der Infektion abhängig, die um so geringer ausfällt, je eher sie entdeckt wird. Im Idealfall wird ein Virus frühzeitig beim Eintritt in das Unternehmensnetzwerk automatisch von einer speziellen Software erkannt und entfernt.

Ein umfassender Ansatz für ein Sicherheitskonzept gegen Viren in betrieblichen Umgebungen sollte alle möglichen Verbreitungskanäle berücksichtigen, um einen wirkungsvollen Schutz zu gewährleisten. Hierzu müssen vor allem die von den Viren bedrohten Güter identifiziert werden, in der Regel die lokalen Anwendungen und Daten auf Intel-basierten Workstations im Unternehmensnetz. Durch die Verbreitung der plattformunabhängigen Javaviren bzw. der Makroviren sind auch zunehmend Unix- und Macintosh-Workstations betroffen.

Zum Schutz gegen Viren bieten eine ganze Reihe von Herstellern Anti-Viren-Programme an, welche die unerwünschten Eindringlinge nach unterschiedlichen Methoden erkennen sollen:

- Virenscanner greifen auf umfangreiche Datenbanken zu, die Informationen über typische Bytemuster (= „Signaturen“) bekannter Viren enthalten. Um die Effektivität der Scanner zu gewährleisten, müssen diese Datenbanken immer aktuell gehalten werden (= regelmäßige Updates der Viren-Signaturen notwendig).

- Integritätsprüfer berechnen Prüfsummen auf potentiell gefährdeten Dateien, um nachträgliche Veränderungen durch eine Infektion feststellen zu können. So können auch ohne entsprechende Signaturen neuere Virenarten erkannt werden. Leider führen Manipulationen der Benutzer an den Dateien häufiger zu Fehlalarmen, die mit unnötiger Arbeit und Kosten verbunden sind.
- Heuristische Analysetools reagieren im laufenden Betrieb auf typische Strukturen und Verhaltensmuster, wie z.B. verdächtige Dateioperationen. Auch hier werden des öfteren Fehlalarme ausgelöst.

4.7 Literaturhinweise

- Bundesamt für Sicherheit in der Informationstechnik
  Sicherheitsaspekte bei Electronic Commerce
  Schriftenreihe zur IT-Sicherheit, Band 10
  Bundesanzeiger Verlag, 1999
- Chapman, D. Brent; Zwicky, Elizabeth D.
  Einrichten von Internet Firewalls
  O'Reilly Verlag, 1997
- Friedl, Wolfgang J.
  Rechenzentrumssicherheit
  Springer-Verlag Berlin Heidelberg New York, 1998
- Kuppinger, Martin
  Internet- und Intranet-Sicherheit
  Microsoft Press Deutschland, 1998
- Kurtz, Georg; McClure, Stuart; Scambray, Joel
  Das Anti-Hacker Buch
  MITP-Verlag GmbH, Bonn, 2000
- Martius, Kai
  Sicherheitsmanagement in TCP/IP-Netzen,
  Friedr. Vieweg & Sohn Verlagsgesellschaft mbH, 2000
- Microsoft Proxy Server – Original Microsoft Training
  Microsoft Press Deutschland, 1998

- Raepple, Martin
  Sicherheitskonzepte für das Internet, dpunkt-Verlag, 1998
- Scott, Charlie; Wolfe, Paul; Erwin, Mike
  Virtuelle Private Netzwerke, O'Reilly Verlag, 1999
- Strobel, Stefan
  Firewalls: Einführung, Praxis, Produkte, dpunkt-Verlag, 1999

5 Kryptographie

5.1 Grundlagen

5.1.1 Symmetrische Verschlüsselung

Die symmetrische Verschlüsselung, auch Secret-Key-Verfahren genannt, verdankt ihren Namen der Tatsache, das Sender und Empfänger im Besitz des gleichen, für alle anderen geheimen Schlüssels sein müssen, um vertraulich miteinander zu kommunizieren. Der Sender verschlüsselt die Nachricht mit dem gemeinsamen Schlüssel, schickt sie über das unsichere Medium zum Empfänger, der das Chiffrat unter Verwendung des gleichen Schlüssel wieder entschlüsselt.

Symmetrische Verfahren lassen sich in Block- und Stromchiffren klassifizieren. Blockchiffren führen eine gleichbleibende mathematische Operation auf Blöcken fester Länge in der Originalnachricht aus. Im Gegensatz dazu interpretieren Stromchiffren den Klartext als eine endliche Folge von Zeichen, auf die in jedem Verschlüsselungsschritt eine andere Verschlüsselungsfunktion angewendet wird.

Zu den heute am weitesten verbreiteten symmetrischen Verfahren gehört der „International Data Encryption Algorithm“ (IDEA), der allgemein als relativ schnell und sicher gilt. Bedingt durch die Lizenzbestimmungen wird IDEA heute jedoch mehr und mehr durch den von Bruce Schneider entwickelten Blowfish-Algorithmus ersetzt.

5.1.2 Asymmetrische Verschlüsselung

Die asmmetrische Verschlüsselung wird oft auch als Public-Key-Verfahren bezeichnet. Hierbei werden zwei komplementäre, mathematisch aber miteinander in Beziehung stehende Schlüssel verwendet.

Der nach den drei Anfangsbuchstaben seiner Entwickler (Ron Rivest, Adi Shamir, Leonard Adleman) benannte RSA-Algorithmus zählt zu den bekanntesten Vertretern der asymmetrischen Kryptographie. Er sieht für jeden Teilnehmer ein Schlüsselpaar vor, bestehend aus einem öffentlichen (= „public key“) und einem vertraulichen, privaten Schlüssel (= „private key“). Seinem Namen nach wird der öffentliche Schlüssel jedem zur Verfügung gestellt, der eine vertrauliche Nachricht an den Besitzer des Schlüsselpaars schicken möchte.

Die Schlüssel sind so gewählt, daß eine mit dem öffentlichen Schlüssel chiffrierte Nachricht nur mit dem passenden privaten Schlüssel dechiffriert werden kann. Umgekehrt gilt das gleiche: mit dem privaten Schlüssel kodierte Daten lassen sich nur mit dem öffentlichen Schlüssel dekodieren.

Obwohl bei Public-Key-Verfahren das Schlüsselpaar einen mathematischen Bezug aufweist, sorgen – bis jetzt – die komplexen Zusammenhänge dafür, daß ein Außenstehender, der im Besitz des öffentlichen Schlüssels ist, nicht auf den passenden privaten Schlüssel schließen kann.

5.1.3 Sichere Einwegfunktionen – Hash-Algorithmen

Sichere Einwegfunktionen dienen zum Schutz vor Integritätsverletzungen. Sie akzeptieren als Eingabe eine Nachricht beliebiger Größe und liefern als Ergebnis genau einen Wert mit fester Länge (= „Hashwert“) zurück.

Gemäß ihrem Namen existiert für eine Einwegfunktion keine Umkehrvorschrift, die aus dem Hash wieder die Originalnachricht reproduzieren könnte. Um einen sicheren Schutz gegen beabsichtigte oder ungewollte Manipulationen zu bieten, muß die Funktion schon für einzelne Bitfehler in der Originalnachricht einen vollkommen anderen Wert liefern. Außerdem muß sichergestellt werden, daß es für einen gegebenen Hashwert H basierend auf der Nachricht N keine Nachricht N‘ gibt, so daß $H(N) = H(N')$ gebildet werden kann. Kryptographische Einwegfunktionen, welche diese Forderungen erfüllen, werden als kollisionsfrei bezeichnet.

5.1.4 Digitale Signaturen

Die digitale Signatur bildet im Internet die Eigenschaften der handschriftlichen Unterschrift ab. Diese Eigenschaften sind

- Authentifikation: Die papiergebundene Unterschrift (elektronische Signatur) identifiziert den Unterzeichnenden durch ein typisches Schriftbild
- Verbindlichkeit: Der Unterzeichnende kann nach geleisteter Unterschrift (elektronische Signatur) nicht mehr abstreiten, den Inhalt des Dokuments nicht gekannt und durch seine Unterschrift (elektronische Signatur) bestätigt zu haben

- Fälschungssicherheit: Nur die mit der Unterschrift (elektronische Signatur) identifizierte Person kann unterschrieben (signiert) haben
- Einmalige Verwendung: Die geleistete Unterschrift (elektronische Signatur) ist an das Dokument gebunden. Sie kann kein weiteres Mal verwendet werden
- Integrität: Der Inhalt eines einmal unterschriebenen (signierten) Dokuments kann nachträglich nicht mehr geändert werden.

Zur Erstellung einer digitalen Signatur auf einem elektronischen Dokument kommt das Public-Key-Verfahren in entgegengesetzter Richtung zum Einsatz: die Verschlüsselung erfolgt bei der digitalen Signatur mit dem privaten Schlüssel, dechiffriert wird demnach mit dem öffentlichen Schlüssel.

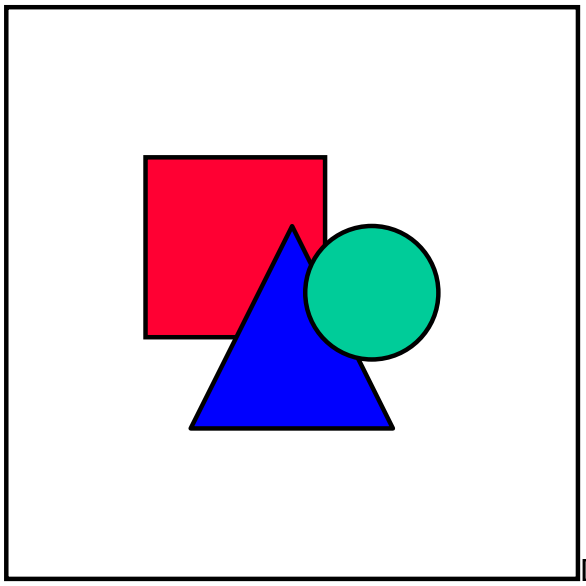
Das Verschlüsseln ganzer Nachrichten würde aufgrund der Komplexität asymmetrischer Verfahren oft zu lange dauern. Daher wird das zur Signatur vorgesehene Dokument durch eine Einwegfunktion (siehe Kapitel 5.1.3) auf wenige Bytes verdichtet. Der Hashwert wird anschließend mit dem privaten Schlüssel des Anwenders signiert und der chiffrierte Wert der Nachricht beigefügt.

5.2 Kryptographische Algorithmen

5.2.1 Data Encryption Standard (DES)

Das DES-Verfahren, das 1976 als amerikanischer Standard entwickelt wurde, wird heute am häufigsten eingesetzt.

Das DES-Verfahren teilt einen Text in 64-Bit-Binärworte, also 8-Byte-Blöcke, und verschlüsselt sie mit einem 56-Bit-Schlüssel.



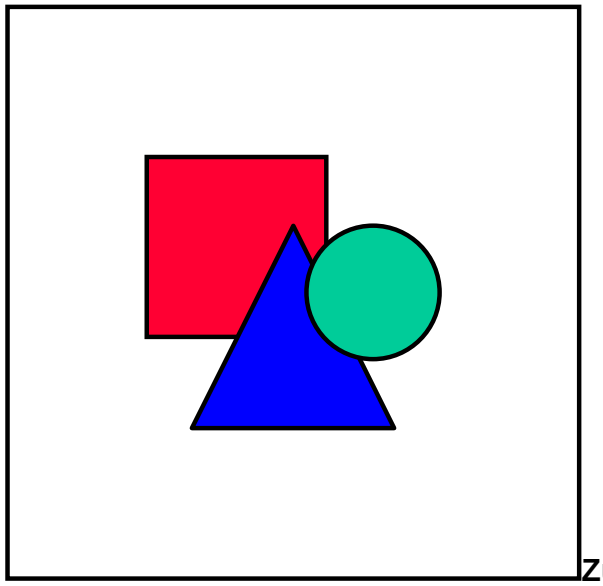
DES ist eine komplexe Funktion, die auch Permutationen verwendet und mit sechzehn Iterationen ein Ergebnis liefert. Dabei ist der Ausgabewert des einen Schrittes der Eingabewert für den nächsten Schritt, der mit einer Permutation bestimmter Schlüsselbits zuvor verändert wird. Diese Permutationen werden auch Teilschlüssel genannt. Zur Entschlüsselung werden die Teilschlüssel in umgekehrter Reihenfolge verwendet.

5.2.1.1 Zur Sicherheit von DES

Die Sicherheit dieses Verfahrens ist bislang sehr hoch, da bis heute noch kein Algorithmus veröffentlicht wurde, der den DES knackt. Der DES ist aber nicht unknackbar. Der Angreifer hat heute die Möglichkeit mit leistungsfähigen Rechnern diese Möglichkeiten zu probieren. Es ist daher anzunehmen, daß DES bisher ein guter Verschlüsselungsalgorithmus ist.
Viel größere Bedeutung kommt der Schlüssellänge zu. Bei einer Schlüssellänge von 56 Bit gibt es 2^{56} Schlüssel (ca. 7,6&middot10^{10} Schlüssel).

5.2.1.2 Dreifach-DES

Zur weiteren Erhöhung der Sicherheit entwickelte man den Dreifach-DES, der das DES-Verfahren und verschiedene Schlüssel k_1 und k_2 verwendet. Dabei wird das DES- Verfahren drei mal hintereinander durchgeführt. Es wird mit k_1 verschlüsselt, mit k_2 entschlüsselt und schließlich mit k_1 wieder verschlüsselt.



5.2.1.3 Zur Sicherheit von Dreifach-DES

Diese Methode erlaubt es auch, Texte die nach dem ursprünglichen DES-Verfahren verschlüsselt wurden, zu entschlüsseln. Obwohl nur zwei Schlüssel benutzt werden, wird der DES- Algorithmus dreimal angewendet, denn es hat sich herausgestellt, daß man bei nur zweimaliger Anwendung relativ leicht mit einem Frontalangriff die Schlüssel herausfinden kann. Bei drei Iterationen der DES- Funktion ist die effektive Schlüssellänge 112 Bits und damit im Moment relativ sicher.

5.2.2 International Data Encryption Algorithm (IDEA)

IDEA ist ein blockorientierter Verschlüsselungsalgorithmus, der 1990 von Xuejia Lai und James Massey entwickelt wurde.

Mit einem Schlüssel von 128 Bit Länge werden Blocks von 64 Bit Länge verschlüsselt. Dabei wird jeder Block achtmal hintereinander und abschließend mit einer Transformation bearbeitet.

Der Algorithmus teilt die 64 Eingabe-Bits in vier 16-Bit-Blöcke auf. In jedem Schritt werden die vier 16-Bit-Blöcke bearbeitet und vier neue 16-Bit- Blöcke erzeugt.

Jede Iteration des IDEA-Algorithmus verwendet drei verschiedene mathematische Operationen, bei denen jeweils zwei 16-Bit-Blöcke auf 16 Bit abgebildet werden. Diese drei Operationen sind:

- bitweises exklusives ODER
- Addition zweier ganzer Zahlen modulo * 2^{16} (=65536), die man als vorzeichenlose ganze Zahl behandelt, ebenso wie das Ergebnis. D.h. die

Funktion addiert zwei 16-Bit-Zahlen und gibt eine 16-Bit-Zahl aus. Der Überlauf im 17. Bit wird "weggeworfen".

- Multiplikation zweier Zahlen modulo $2^{16} + 1$ (=65537), wobei die Multiplikatoren als vorzeichenlose 16-Bit-Zahlen behandelt werden. Die einzige Ausnahme ist die Folge von 16 Nullen, die 2^{16} repräsentiert.

5.2.2.1 Zur Sicherheit von IDEA

Zusammen ergeben diese drei unterschiedlichen Operationen einen Eingabewert für die komplexe Transformation. Kryptoanalyse ist hier viel schwieriger als bei einem Algorithmus wie DES, der ausschließlich auf einfachen Bit-Masken und Permutationen besteht.

IDEA hat somit einige Vorteile gegenüber DES und sogar im Vergleich zu Dreifach-DES. Erstens macht die Schlüssellänge von 128 Bit einen direkten Angriff fast unmöglich. Zweitens widersteht die innere Struktur von IDEA einer Kryptoanalyse besser. Und schließlich wurde IDEA so entwickelt, daß Hard- und Softwareimplementationen möglich sind. Bei Vergleichen der Implementationen von IDEA und Dreifach-DES benötigt IDEA weniger Zeit zur Ausführung.

5.2.3 RSA

(entwickelt 1977, von Ron **R**ivest, Adi **S**hamir und Leonard **A**dleman)

RSA ist einer der frühesten Algorithmen, die öffentliche Schlüssel verwenden. Der RSA-Algorithmus gilt seitdem als der einzige weitverbreitete und implementierte Ansatz der Verschlüsselung mit öffentlichen Schlüsseln.

Ein nichtmathematisches Beispiel (nach Alfred Beutelspacher)

Vergleichbar ist dieser Algorithmus mit dem Kochen einer geheimen Suppe durch zwei Köche A und B. Beide benutzen die gleiche bekannte Ausgangssuppe. Beide Köche haben jeweils geheime Gewürze. Sogar A kennt die Gewürze von B nicht und umgekehrt. Jeder nimmt zum Beispiel die Hälfte der Ausgangssuppe und fügt seine geheimen Gewürze dazu. Die halbfertigen Suppen werden jetzt ausgetauscht. Sie sind also öffentlich, d. h. jeder könnte sie probieren. Jetzt versetzt B die von A erhaltene Suppe mit seinem Gewürz und A fügt der Suppe von B sein Gewürz hinzu. Nun haben beide die gleiche Suppe mit der richtigen Menge an Gewürzen.

RSA ist eine Verschlüsselungstechnik, bei der Klartext und verschlüsselter Text ganze Zahlen zwischen 0 und n-1 für ein beliebiges n sind. Bei langen Nachrichten wird der Text in einzelne Blöcke aufgeteilt. Jeder dieser Blocks hat eine Länge von $\log_2 n$ Bit.
Der öffentliche und der dazugehörige geheime Schlüssel sind Funktionsergebnisse einer Funktion über große Primzahlen (wobei ,,groß" hier mindestens 100 bis 200 Stellen bedeutet). Es wird angenommen, daß es ebenso aufwendig ist, aus dem verschlüsselten Text mit Hilfe des öffentlichen Schlüssels den Klartext zu gewinnen, wie die Zerlegung eines Produkts großer Primzahlen zu finden. Um die zwei Schlüssel, den geheimen und den öffentlichen, zu berechnen, nimmt man zwei große Primzahlen p und q, die etwa gleich viele Stellen haben sollten, da dies die Sicherheit erhöht.

Damit berechnet man das Produkt $n=p \cdot q$ und $\varnothing(n)=(p-1) \cdot (q-1)$.

Nun wählt man eine Zahl e, die anschließend zur Verschlüsselung verwendet wird. Der größte gemeinsame Teiler von e und $\varnothing(n)$ sollte 1 sein ($ggT(e, \varnothing(n))=1$) .

Damit berechnet man den Schlüssel d, der später zur Entschlüsselung verwendet wird:

$e \cdot d=1 \bmod \varnothing(n)$, $d=e^{-1} \cdot \bmod \varnothing(n)$

Für d und n gilt auch, dass ihr größter gemeinsamer Teiler 1 ist ($ggT(n,e)=1$).

Das Zahlenpaar (e,n) bildet den öffentlichen Schlüssel, (d,n) ist der geheime. Die Primzahlen p und q werden nun nicht mehr benötigt und sollten gelöscht, aber auf keinen Fall veröffentlicht werden.

5.2.3.1 Zur Sicherheit von RSA

Die Sicherheit dieses Algorithmus liegt in der Größe der verwendeten Schlüssel. Um aus dem öffentlichen Schlüssel den geheimen zu berechnen, muß man n in seine Primfaktoren zerlegen. Bei einer Zahl wie 91 mag das noch sehr einfach erscheinen, allerdings wird das bei 2091 ($=51 \cdot 41$) schon schwieriger und bei RSA-Schlüsseln mit 200-stelliger Zahl n scheint das unmöglich zu sein.

Damit n geheim bleibt, müssen natürlich auch p und q geheim bleiben. Diese zwei Zahlen können nach der Berechnung des Schlüssels auch gelöscht werden.

Darin liegt aber auch der Nachteil von RSA. Je größer n ist, desto länger ist der verwendete Schlüssel. Die Ver- und Entschlüsselung dauert dadurch lange. Im Vergleich zu IDEA benötigt eine Ver- und Entschlüsselung mit RSA etwa tausendmal soviel Zeit. Welche Schlüssellänge allerdings hundertprozentige Sicherheit bietet, ist schwer zu sagen.

5.2.4 Diffie-Hellman

Diffie-Hellmann ist ein weit verbreiteter Algorithmus zum Schlüsselaustausch, da er bei Verwendung von genügend langen Schlüsseln (entsprechend guter Generator vorausgesetzt) als sicher bezeichnet wird.

Die Sicherheit beruht auf dem *diskreten Logarithmus Problem*, welches als aquivalent zum Faktorisierungsproblem von ganzen Zahlen angesehen wird. Diffie-Hellmann ist in den USA patentiert, wobei das Patent jedoch bald abläuft.

5.2.5 Digital Signature Standard (DSS)

Ein Verfahren, welches nur zum Erzeugen von Signaturen gedacht ist. DSS wurde von der US Regierung entwickelt, das Design von DSS wurde jedoch nie veröffentlicht und viele Personen haben potentielle Probleme von DSS aufgezeigt. Die US Regierung hat das Patent auf DSS, wobei die Benutzung jedoch frei ist

5.2.6 Elliptische Kurven

Public Key Verfahren, welche auf Basis von elliptischen Kurven funktionieren sind erst vor einiger Zeit ins Rampenlicht gerückt worden. Bisher war eine praktikable Anwendung aufgrund des relativ hohen Rechenaufwandes nur schwer möglich

5.2.7 Blowfish

Der Blowfish Algorithmus wurde von Bruce Schneier entwickelt und ist ein Blockalgorithmus. Blockgröße ist 64 bit mit einer Schlüsselkgröße von bis zu 448 bit.

5.2.8 Twofish

Der Twofish Algorithmus wurde von dem Counterpane Team (Bruce Schneier u.a.) entwickelt und ist ein Blockalgorithmus. Blockgröße ist 128 bit mit einer Schlüsselkgröße von bis zu 256 bit über 16 Runden.

5.2.9 RC 5

RC5 wurde von Ron Rivest für RSA Data Security, Inc. entwickelt (April 1995).

RC5 ist ein Blockverschlüsselungsalgorithmus und ist als möglicher Nachfolger von DES gedacht. Im Gegensatz zu DES bietet RC5 eine variable Schlüssel-, Wortlänge und eine variable Anzahl von Durchläufen. RC5 ist sowohl für Software wie auch Hardware Implementierungen geeignet.

5.3 Kryptographische Protokolle

5.3.1 Secure Socket Layer (SSL)

SSL bietet einen recht allgemeinen Ansatz für die Absicherung von virtuellen Verbindungen (= TCP-Verbindungen) im Internet auf Transportebene. SSL kann im OSI-Schichtenmodell über der Transportschicht eingeordnet werden. Im TCP/IP-Stak liegt es dann zwischen TCP und der Anwendungsebene.

Die meisten Anwendungen nutzen die Socket-Schnittstelle als programmtechnischen Zugang zu einem TCP/IP-Netzwerk. SSL bedient sich dieser Schnittstelle u. a. zur Übertragung der verschlüsselten Daten. Um die SSL-Sicherheitsfunktionen nutzen zu können, muß eine Anwendung explizit die SSL-Funktionen statt der Socket-Aufrufe ansprechen. Die SSL-Schicht baut dann selbständig eine TCP-Verbindung zur SSL-Schicht des Server auf und führt eine Handshake-Prozedur durch.

SSL bietet

- eine flexible kryptographische Authentisierung und Verschlüsselung für eine verbindungsorientierte Kommunikation,
- eine Ende-zu-Ende-Sicherheit.

Notwenig für den Einsatz von SSL sind:

- eine explizite Nutzung durch die Anwendung,
- Zertifikate und eine entsprechende Infrastruktur.

5.3.2 Secure Shell (SSH)

SSH ist zunächst als ein Ersatz für die Remote Shell (rsh) und Telnet entstanden, um deren Sicherheitslücken auszugleichen. Mittlerweile ist SSH ein eigenständiges

Protokoll, welches sichere Kanäle für beliebige verbindungsorientierte Dienste bereitstellen kann. Standardmäßig wird eine interaktive Shell und Tunneling unterstützt. Entsprechend seiner erweiterten Funktionalität ist SSH in drei Teilprotokolle untergliedert:

1) SSH Transport Layer Protocol
2) SSH User Authentication Protocol
3) SSH Connection Protocol.

5.3.2.1 SSH Transport Layer Protocol

Das Transport Layer Protocol setzt auf eine gesicherte Datenverbindung (i. a. TCP) auf. Es gewährleistet eine einseitige Host-Authentisierung, d.h. der Server authentisiert sich zunächst gegenüber dem Client.

Weiterhin werden die kryptographischen Möglichkeiten abgeglichen sowie geheime Schlüssel zur nachfolgenden Kanalverschlüsselung ausgetauscht. Die Kanalverschlüsselung basiert auf symmetrischen Verfahren der Kryptographie. In der aktuellen (Januar 2000) Protokollversion wird das Diffie-Hellman-Verfahren als Public-Key-Verfahren eingesetzt, da RSA patentrechtlich in einigen Staaten geschützt ist.

5.3.2.2 SSH User Authentication Protocol

Über den kryptographisch gesicherten Kanal kann nun eine Nutzerauthentifizierung durchgeführt werden. Die Authentifizierung beruht auf Public-Key-Verfahren; meist wird zusätzlich noch das herkömmliche Paßwort-Verfahren angeboten. Durch das Public-Key-Verfahren muß der Server nur den öffentlichen Schlüssel kennen, um an Hand einer Signatur eine Client-Nachricht zu verifizieren.

Eine Verwendung von Zertifikaten ist nicht zwingend vorgesehen, daher kann das Verfahren ohne große Infrastrukturanforderungen eingesetzt werden – bietet dann aber auch gewisse Angriffspunkte.

5.3.2.3 SSH Connection Protocol

Das Connection Protocol besitzt bezüglich des gesamten SSH-Protokolls keine weitere Sicherheitsrelevanz, sondern setzt auf die vorherigen Protokolle auf und

„verläßt“ sich damit auf den gesicherten kryptographischen Kanal und die durchgeführte Authentifizierung.

Das Protokoll erweitert den ursprünglichen Ansatz von SSH um die Möglichkeit, beliebige Verbindungen über den gesicherten Kanal zu multiplexen. Es stellt dazu Mechanismen und Nachrichten bereit, die eine Anforderung von Diensten und deren Zuordnung unterstützen.

5.3.3 Secure Hypertext Transfer Protocol (S-HTTP)

Mit dem S-HTTP wurde speziell für das im World Wide web eingesetzte HTTP eine Sicherheitserweiterung geschaffen. S-HTTP besitzt folgende Eigenschaften:

- Abwärtskompatibilität zu HHTP
- Kann wie SSH auch ohne clientseitige Zertifikate genutzt werden (Der Server muß ein Zertifikat besitzen!)
- Kann echte digitale Signaturen für die übertragenen Dokumente/Daten bereitstellen
- Flexibler Einsatz kryptographischer Mechanismen:
  - Soll Request und/oder Reply verschlüsselt und/oder signiert werden?
  - Welche kryptographischen Methoden sollen eingesetzt werden?
  - Welches Zertifikat, welcher Schlüssel soll verwendet werden?
- Sicherheitsanforderungen können dynamisch bei Abruf einer Seite vom Server gegenüber dem Client definiert werden.

5.3.4 Simple Key Management for Internet Protocol (SKIP)

SKIP wurde von Sun Microsystems entwickelt und dient dem Schlüsselmanagement. SKIP ermöglicht eine sitzungsbezogene Schlüsselabsprache zwischen Kommunikationspartnern nach der Diffie-Helman-Methode.

5.3.5 Email

Da mit dem Standard-Protokoll SMTP der Inhalt einer Mail weder vertraulich noch gesichert übertragen wird und auch der Absender nicht eindeutig identifiziert werden kann, sind einige Tools für die Sicherung von Email entstanden. Phil Zimmermann

entwickelte „Pretty Good Privacy“ (PGP), ein Freeware-Tool, welches weltweit eingesetzt wird und mit starker Verschlüsselung arbeiten kann.

Die andere Hauptentwicklung im Internet-Umfeld ist die Erweiterung des MIME-Standards um Sicherheitsfunktionen zu S/MIME, hauptsächlich von der Firma RSA Data Security Inc. vorangetrieben.

5.3.5.1 Pretty Good Privacy (PGP)

PGP ist kein Kryptographieverfahren oder -Algorithmus, sondern ein Programm, welches vorhandene Verfahren benutzt bzw. kombiniert um die Möglichkeit zu bieten zwischen verschiedenen Systemen verschlüsselte Daten austauschen zu können.

In erster Linie ist PGP zum Verschlüsseln von E-Mail gedacht. Allerdings kann es auch benutzt werden, um Dateien vor dem Zugriff anderer Personen zu schützen.

PGP benutzt den RSA-Algorithmus um das Public-Key-Prinzoip umzusetzen, wobei jedoch nicht die gesamte Nachricht mittels RSA verschlüsselt wird. Hierfür wird das IDEAVerfahren benutzt und lediglich der IDEA-Schlüssel wird mittels RSA bzw. dem entsprechenden öffentlichen Schlüssel des Empfängers verschlüsselt. Im E-Mail-Bereich ist PGP mittlerweile zu einem Quasi-Standard geworden und wird von sehr vielen Leuten eingesetzt.

5.3.5.2 Secure Multi Purpose Mail Extension (S/MIME)

Hinter S/MIME steht eine Sicherheitserweiterung für Emails im MIME-Format, welche unter der Federführung von RSA Data Security Inc. entwickelt wird.

Im Vergleich zu PGP bietet die Spezifikation keine zusätzliche Sicherheitsfun ktionen für den elektronischen Datenaustausch. Die Vertraulichkeit wird durch ein hybrides Verschlüsselungsverfahren sichergestellt, die Authentizität und Integrität über die digitale Signatur des Absenders.

Unter den Symmetrischen Verfahren unterstützt S/MIME DES, Triple-DES und RC2. Als Public-Key-Verfahren kommt RSA zum Einsatz. Im Gegensatz zu PGP setzt S/MIME bei den Zertifikaten auf vorhandene Standards. Verwendet wird das im Internet weit verbreitete X.509-Format.

Die Teilnahme am international sicheren Briefverkehr mit S/MIME setzt ein beglaubigtes Schlüsselzertifikat von einer der kostenpflichtigen CAs wie VeriSign

oder GTE voraus. Die Kosten für den Einsatz von S/MIME sind sicherlich mit daran Schuld, daß der Einsatz von S/MIME im Vergleich zum kostenlosen PGP noch recht dünn gesät ist.

5.3.6 International Protocol Security (IPSec)

IPSec wird in RFC 1825ff beschrieben und stellt Verfahren zur Integration von Security-Diensten (Verschlüsselung, Integritätprüfung und Authentifikation) in der Netzwerkschicht vor Sie gelten in gleicher Weise für die nächste Generation des IP-Protokolls (IPv6) als auch für die derzeitige Version (IPv4).

Umgesetzt werden die neuen Sicherheitsfunktionen durch die Einführung von zwei Erweiterungen: dem IP Authentication Header (AH) und der Encapsulation Security Payload (ESP). Beide können getrennt oder gemeinsam eingesetzt werden. Der AH gewährleistet die Authentifikation und Integrität von Datagrammen, die ESP sorgt für die Integrität und Verschlüsselung.

Nach wie vor ungeschützt bleiben Informationen über die Paketgröße, die Anzahl der Verbindungen zwischen zwei Stationen sowie bestimmte Daten in den Protokollfeldern, die im Rahmen von Netzwerkanalysen ausgewertet werden können.

5.4 Kryptographie im Netzwerk

Asymmetrische Verfahren sind – bedingt durch ihre Komplexität – recht langsam. Bei der Verschlüsselung größerer Datenmengen kommen also nur symmetrische Verfahren bzw. Algorithmen in Frage.

Die langsamen asymmetrischen Verfahren können dann immer noch zum Austausch des geheimen Schlüssels dienen, bedingen dann jedoch den administrativen Aufwand zur Pflege eines Verwaltungs-Servers für die öffentlichen Schlüssel.

5.4.1 Einsatz in einem VPN

Scott et al. untersuchten 1999 die Effizienz der Verschlüsselungsalgorithmen beim Einsatz in einem VPN, welches mit SSH realisiert wurde:

Verbindungsart	Effizienz vs. FTP bei VPN-Nutzung (in %)	Effizienz vs. VPN ohne VPN-Nutzung (in %)

FTP	100	233
VPN (nur SSH)	43	100
Blowfish mit SSH	36	85
IDEA mit SSH	26	60
3DES mit SSH	20	47

Wie sich zeigt, vermindert sich die Leistung bereits durch die Nutzung der SSH und dem damit einhergehenden Protokoll-Overhead beträchtlich. Es ist an dieser Stelle interessant, daß durch das Hinzufügen der Verschlüsselungen mit Blowfish und IDEA keine wesentlichen Leistungseinbußen mehr hinzukommen.

5.4.2 Verschlüsselung bei der Dresdner Bank

Die Dresdner Bank benutzt SafeGuard Easy, um ihre Rechner durch kryptographische Verfahren zu schützen. SafeGuard Easy kann dabei den ganzen PC, einzelne Partitionen, Dateien oder auch Disketten verschlüsseln.

Als Algorithmen kommen XOR, Stealth-40, Blowfish-16, DES oder Idea zum Einsatz. XOR ais zwar ein extrem schneller Algorithmus, die von ihm gebotene Sicherbeit besteht jedoch lediglich darin, das Gewissen seines Benutzers zu beruhigen. („Ich habe meine Daten ja durch Kryptographie geschützt!“) Ähnliches gilt für Stealth-40. Beide Algorithmen sind von Experten sehr schnell zu knacken. Auch DES gilt heute von der Struktur des Algorithmus her nicht mehr als sicher.

IDEA und Blowfish sind relativ schnelle Algorithmen und gelten als sehr sicher. IDEA für den professionellen bzw. kommerziellen Einsatz jedoch lizensiert werden, während Blowfish frei verfügbar ist.

Die folgende Tabelle zeigt die Verzögerung von Arbeitsabläufen bei der PC-Benutzung durch den Einsatz kryptographischer Verfahren, wobei der unverschlüsselte Wert zwecks Standardisierung auf 100 % gesetzt wurde:

Algorithmus	Unverschlüsselt	XOR	Stealth-40	Blowfish-16	DES	IDEA
Bootendes PC	100	118	120	129	171	135
Starten von	100	100	100	111	244	155

Excel						
Starten von Word	100	100	100	117	183	133
Laden einer Excel-Datei	100	100	100	113	175	113
Laden Textdatei	100	100	100	107	133	120
10 MB kopieren	100	320	328	336	504	352

5.5 Literaturhinweise

- Bundesamt für Sicherheit in der Informationstechnik
  Sicherheitsaspekte bei Electronic Commerce
  Schriftenreihe zur IT-Sicherheit, Band 10
  Bundesanzeiger Verlag, 1999
- Görtz, Horst; Stolp, Jutta
  Informationssicherheit im Unternehmen,
  Addison-Wesley-Longman GmbH, 1999
- Martius, Kai
  Sicherheitsmanagement in TCP/IP-Netzen,
  Friedr. Vieweg & Sohn Verlagsgesellschaft mbH, 2000
- Raepple, Martin
  Sicherheitskonzepte für das Internet, dpunkt-Verlag, 1998
- Schneier, Bruce
  Angewandte Kryptographie
  Addison-Wesley-Longman GmbH, 1999
- Scott, Charlie; Wolfe, Paul; Erwin, Mike
  Virtuelle Private Netzwerke
  O'Reilly Verlag, 1999

- Welschenbach, Michael
  Kryptographie in C und C++
  Springer-Verlag Berlin Heidelberg New York, 1998

6 Sicherheitskonzept für Remote Access Lösungen

6.1 Remote Access via Internet

Die Benutzerauthentisierung kann nach einem modifizierten CHAP-Verfahren (siehe Kapitel 4.5.2) durchgeführt werden.

Der Benutzer generiert eine Zufallszahl, z.B. durch Mausbewegungen in einem vorgegebenen Feld, die Punkte im Feld Zahlen darstellen. Jeder Punkt, auf den der Mauszeiger weist repräsentiert so eine Zahl. Durch Produktbildung erhält der Programmierer so schnell eine hinreichend große Zufallszahl. Mit dem geheimen Schlüssel wird diese Zahl kodiert und zum Server geschickt. Der Server entschlüsselt diese Zahl mit dem bei ihm hinterlegten öffentlichen Schlüssel, wobei öffentlich in diesem Falle bedeutet: nur dem Server bekannt.

Analog identifiziert sich der Server gegenüber dem Client durch die Zurücksendung der empfangenen Zufallszahl, welche mit dem privaten Schlüssel des Servers verschlüsselt wurde. Mit dem öffentlichen Schlüssel des Servers entziffert der Client die gesendete Zahl und vergleicht sie mit der von ihm gesendeten. Stimmen beide überein, hat sich der Server ebenfalls legitimiert.

Die Verschlüsselung der Daten der eigentlichen Kommunikation erfolgt dann nach einem schnellen, aber sicheren symmertrischen Algorithmus, z.B. Blowfish.

6.2 Remote Access via ISDN

Eine mögliche Lösung ist der Einsatz von SafeGuard VPN. SafeGuard kombiniert die starke Verschlüsselung der Daten mit einer administrativen Firewall-Funktionalität. SafeGuard VPN benutzt Simple Key Management for Internet Protocol (SKIP) zur Schlüsselvereinbarung und den IDEA-Algorithmus zur Datenverschlüsselung. SafeGuard VPN ermöglicht End-to-End-, End-to-Site- und Site-to-Site-Verbindungen.

Eine End-to-Site-Verbindung bedeutet hier eine Verbindung zwischen einem entfernten Client (PC, Laptop unter Windows NT 4.0) und dem Windows NT-Server. Die anderen Methoden erlauben Verschlüsselung zwischen zwei Terminals (End-to-End) oder zwischen zwei Servern (Site-to-Site).

Die NDIS-Schnittstelle von Windows NT deckt die Kommunikation über Netzwerkkarten wie auch über Modem ab, d.h. die Implementierung eines NDIS-Filters gewährleistet, daß kein Netzwerktreiber verändert werden muß.

Als Algorithmus für die Verschlüsselung der IP-Pakete wird IDEA mit einer Schlüssellänge von 128 BIt verwendet, was heute als sicher eingestuft werden muß. SKIP ermöglicht eine sitzungsbezogene Schlüsselabsprache zwischen Kommunikationspartnern nach der Diffie-Hellman-Methode.

6.3 Literaturhinweise

- Buchmann, Johannes
  Einführung in die Kryptographie
  Springer-Verlag Berlin Heidelberg New York, 1999
- Bundesamt für Sicherheit in der Informationstechnik
  Sicherheitsaspekte bei Electronic Commerce
  Schriftenreihe zur IT-Sicherheit, Band 10
  Bundesanzeiger Verlag, 1999
- Creutzig, Christopher; Buhl, Andreas; Zimmermann, Philipp
  PGP – Pretty Good Privacy
  Art d'Ameublement, Bielefeld, 1999
- Görtz, Horst; Stolp, Jutta
  Informationssicherheit im Unternehmen,
  Addison-Wesley-Longman GmbH, 1999
- Martius, Kai
  Sicherheitsmanagement in TCP/IP-Netzen,
  Friedr. Vieweg & Sohn Verlagsgesellschaft mbH, 2000
- Smith, Richard E.
  Internet-Kryptographie
  Addison Wesley Longman Verlag, 1998

7 Anhänge

7.1 Deutsche Gesetze

7.1.1 Bundes-Datenschutzgesetz

7.1.1.1 Erster Abschnitt

Allgemeine Bestimmungen

§1 Zweck und Anwendungsbereich des Gesetzes

(1) Zweck dieses Gesetzes ist es, den einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch

1. öffentliche Stellen des Bundes,

2. öffentliche Stellen der Länder, soweit der Datenschutz nicht

durch Landesgesetz geregelt ist und soweit sie

a) Bundesrecht ausführen oder

b) als Organe der Rechtspflege tätig werden und es sich

nicht um Verwaltungsangelegenheiten handelt,

3. nicht-öffentliche Stellen, soweit sie die Daten in oder aus

Dateien geschäftsmäßig oder für berufliche oder gewerbliche Zwecke verarbeiten oder nutzen.

(3) Bei der Anwendung dieses Gesetzes gelten folgende Einschränkungen:

1. Für automatisierte Dateien, die ausschließlich aus verarbeitungstechnischen Gründen vorübergehend erstellt und nach ihrer verarbeitungstechnischen Nutzung automatisch gelöscht werden, gelten nur die §§5 und 9.

2. Für nicht-automatisierte Dateien, deren personenbezogene Daten nicht zur Übermittlung an Dritte bestimmt sind, gelten nur die §§5, 9, 39 und 40. Außerdem

gelten für Dateien öffentlicher Stellen die Regelungen über die Verarbeitung und Nutzung personenbezogener Daten in Akten. Werden im Einzelfall personenbezogene Daten übermittelt, gelten für diesen Einzelfall die Vorschriften dieses Gesetzes uneingeschränkt.

(4) Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(5) Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes

vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

§2 Öffentliche und nicht-öffentliche Stellen

(1) Öffentliche Stellen des Bundes sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. Als öffentliche Stellen gelten die aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz oder dem Gesetz über Fernmeldeanlagen zusteht.

(2) Öffentliche Stellen der Länder sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes und sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie derer Vereinigungen ungeachtet ihrer Rechtsform.

(3) Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeachtet der Beteiligung nicht-öffentlicher Stellen als öffentliche Stellen des Bundes, wenn

1. sie über den Bereich eines Landes hinaus tätig werden oder

2. dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht.

Andernfalls gelten sie als öffentliche Stellen der Länder.

(4) Nicht-öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen. Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

§3 Weitere Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

(2) Eine Datei ist

1. eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (automatisierte Datei), oder
2. jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann (nicht-automatisierte Datei).

Nicht hierzu gehören Akten und Aktensammlungen, es sei denn, daß sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können.

(3) Eine Akte ist jede sonstige amtlichen oder dienstlichen Zwecken dienende Unterlage; dazu zählen auch Bild- und Tonträger. Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

(4) Erheben ist das Beschaffen von Daten über den Betroffenen.

(5) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung,

2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,

3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten (Empfänger) in der Weise, daß

a) die Daten durch die speichernde Stelle an den Empfänger weitergegeben werden oder

b) der Empfänger von der speichernden Stelle zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,

4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,

5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

(6) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

(7) Anonymisieren ist das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

(8) Speichernde Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst speichert oder durch andere im Auftrag speichern läßt.

(9) Dritter ist jede Person oder Stelle außerhalb der speichernden Stelle. Dritte sind nicht der Betroffene sowie diejenigen Personen und Stellen, die im Geltungsbereich dieses Gesetzes personenbezogene Daten im Auftrag verarbeiten oder nutzen.

§4 Zulässigkeit der Datenverarbeitung und -nutzung

(1) Die Verarbeitung personenbezogener Daten und deren Nutzung sind nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat.

(2) Wird die Einwilligung bei dem Betroffenen eingeholt, ist er auf den Zweck der Speicherung und einer vorgesehenen Übermittlung sowie auf Verlangen auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich

erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.

(3) Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Absatz 2Satz 2auch dann vor, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind der Hinweis nach Absatz 2 Satz 1 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszweckes ergibt, schriftlich festzuhalten.

§5 Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§6 Unabdingbare Rechte des Betroffenen

(1) Die Rechte des Betroffenen auf Auskunft (§§19, 34) und auf Berichtigung, Löschung oder Sperrung (§§20, 35) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

(2) Sind die Daten des Betroffenen in einer Datei gespeichert, bei der mehrere Stellen speicherungsberechtigt sind, und ist der Betroffene nicht in der Lage, die speichernde Stelle festzustellen, so kann er sich an jede dieser Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die speichernde Stelle weiterzuleiten. Der Betroffene ist über die Weiterleitung und die speichernde Stelle zu unterrichten. Die in §19 Abs. 3 genannten Stellen, die Behörden der Staatsanwaltschaft und der Polizei sowie öffentliche Stellen der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, können statt des Betroffenen den Bundesbeauftragten für den Datenschutz unterrichten. In diesem Fall richtet sich das weitere Verfahren nach §19 Abs. 6.

§7 Schadensersatz durch öffentliche Stellen

(1) Fügt eine öffentliche Stelle dem Betroffenen durch eine nach den Vorschriften dieses Gesetzes oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige automatisierte Verarbeitung seiner personenbezogenen Daten einen

Schaden zu, ist sie dem Betroffenen unabhängig von einem Verschulden zum Ersatz des daraus entstehenden Schadens verpflichtet.

(2) Bei einer schweren Verletzung des Persönlichkeitsrechts ist dem Betroffenen der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen.

(3) Die Ansprüche nach den Absätzen 1 und 2 sind insgesamt bis zu einem Betrag in Höhe von zweihundertfünfzigtausend Deutsche Mark begrenzt. Ist auf Grund desselben Ereignisses an mehrere Personen Schadensersatz zu leisten, der insgesamt den Höchstbetrag von zweihundertfünfzigtausend Deutsche Mark übersteigt, so verringern sich die einzelnen Schadensersatzleistungen in dem Verhältnis, in dem ihr Gesamtbetrag zu dem Höchstbetrag steht.

(4) Sind bei einer Datei mehrere Stellen speicherungsberechtigt und ist der Geschädigte nicht in der Lage, die speichernde Stelle festzustellen, so haftet jede dieser Stellen.

(5) Mehrere Ersatzpflichtige haften als Gesamtschuldner.

(6) Auf das Mitverschulden des Betroffenen und die Verjährung sind die §§254 und 852 des Bürgerlichen Gesetzbuches entsprechend anzuwenden.

(7) Vorschriften, nach denen ein Ersatzpflichtiger in weiterem Umfang als nach dieser Vorschrift haftet oder nach denen ein anderer für den Schaden verantwortlich ist, bleiben unberührt.

(8) Der Rechtsweg vor den ordentlichen Gerichten steht offen.

§8 Schadensersatz durch nicht-öffentliche Stellen

Macht ein Betroffener gegenüber einer nicht-öffentlichen Stelle einen Anspruch auf Schadensersatz wegen einer nach diesem Gesetz oder anderen Vorschriften über den Datenschutz unzulässigen oder unrichtigen automatisierten Datenverarbeitung geltend und ist streitig, ob der Schaden die Folge eines von der speichernden Stelle zu vertretenden Umstandes ist, so trifft die Beweislast die speichernde Stelle.

§9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Geset-zes, insbesondere die in der Anlage zu diesem Gesetz genannten

Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

§10 Einrichtung automatisierter Abrufverfahren

(1) Die Einrichtung eines automatisierten Verfahrens, das die Übermittlungpersonenbezogener Daten durch Abruf ermöglicht, ist zulässig, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben oder Geschäftszwecke der beteiligten Stellen angemessen ist. Die Vorschriften über die Zulässigkeit des einzelnen Abrufs bleiben unberührt.

(2) Die beteiligten Stellen haben zu gewährleisten, daß die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Hierzu haben sie schriftlich festzulegen:

1. Anlaß und Zweck des Abrufverfahrens,

2. Datenempfänger,

3. Art der zu übermittelnden Daten,

4. nach §9 erforderliche technische und organisatorische Maßnahmen.

Im öffentlichen Bereich können die erforderlichen Festlegungen auch durch die Fachaufsichtsbehörden getroffen werden.

(3) Über die Einrichtung von Abrufverfahren ist in Fällen, in denen die in §12 Abs. 1 genannten Stellen beteiligt sind, der Bundesbeauftragte für den Datenschutz unter Mitteilung der Festlegungen nach Absatz 2zu unterrichten. Die Einrichtung von Abrufverfahren, bei denen die in §6 Abs. 2 und in §19 Abs. 3 genannten Stellen beteiligt sind, ist nur zulässig, wenn der für die speichernde und die abrufende Stelle jeweils zuständige Bundes- oder Landesminister oder deren Vertreter zugestimmt haben.

(4) Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Empfänger. Die speichernde Stelle prüft die Zulässigkeit der Abrufe nur, wenn dazu Anlaß besteht. Die speichernde Stelle hat zu gewährleisten, daß die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann. Wird ein Gesamtbestand personenbezogener Daten abgerufen oder übermittelt (Stapelverarbeitung), so bezieht sich die

Gewährleistung der Feststellung und Überprüfung nur auf die Zulässigkeit des Abrufes oder der Übermittlung des Gesamtbestandes.

(5) Die Absätze 1 bis 4 gelten nicht für den Abruf aus Datenbeständen, die jedermann, sei es ohne oder nach besonderer Zulassung, zur Benutzung offenstehen.

§11 Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag durch andere Stellen verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§6 bis 8 genannten Rechte sind ihm gegenüber geltend zu machen.

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei die Datenverarbeitung oder –nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden.

(3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten oder nutzen. Ist er der Ansicht, daß eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(4) Für den Auftragnehmer gelten neben den §§5, 9, 43 Abs. 1, Abs. 3 und 4 sowie §44 Abs. 1 Nr. 2, 5, 6 und 7 und Abs. 2 nur die Vorschriften über die Datenschutzkontrolle oder die Aufsicht, und zwar für

1. a) öffentliche Stellen,

b) nicht-öffentliche Stellen, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht und der Auftraggeber eine öffentliche Stelle ist, die §§18, 24 bis 26 oder die entsprechenden Vorschriften der Datenschutzgesetze der Länder,

2. die übrigen nicht-öffentlichen Stellen, soweit sie personen-bezogene Daten im Auftrag als Dienstleistungsunternehmen geschäftsmäßig verarbeiten oder nutzen, die §§ 32, 36 bis 38.

7.1.1.2 Zweiter Abschnitt

Datenverarbeitung der öffentlichen Stellen

7.1.1.2.1 Erster Unterabschnitt

Rechtsgrundlagen der Datenverarbeitung

§12 Anwendungsbereich

(1) Die Vorschriften dieses Abschnittes gelten für öffentliche Stellen des Bundes, soweit sie nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen.

(2) Soweit der Datenschutz nicht durch Landesgesetz geregelt ist, gelten die §§12 bis 17, 19 und 20 auch für die öffentlichen Stellen der Länder, soweit sie

1. Bundesrecht ausführen und nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen oder

2. als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt.

(3) Für Landesbeauftragte für den Datenschutz gilt §23 Abs. 4 entsprechend.

(4) Werden personenbezogene Daten für frühere, bestehende oder zukünftige dienst- oder arbeitsrechtliche Rechtsverhältnisse verarbeitet oder genutzt, gelten anstelle der §§ 14 bis 17, 19 und 20 der§28Abs.1 und2 Nr.1 sowiedie§§33 bis35.

§13 Datenerhebung

(1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllungder Aufgaben der erhebenden Stellen erforderlich ist.

(2) Personenbezogene Daten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder

2. a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder

b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde

und keine Anhaltspunkte dafür bestehen, daß überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

(3) Werden personenbezogene Daten beim Betroffenen mit seiner Kenntnis erhoben, so ist der Erhebungszweck ihm gegenüber anzugeben. Werden sie beim Betroffenen auf Grund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Auf Verlangen ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

(4) Werden personenbezogene Daten statt beim Betroffenen bei einer nicht-öffentlichen Stelle erhoben, so ist die Stelle auf die Rechtsvorschrift, die zur Auskunft verpflichtet, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

§14 Datenspeicherung, -veränderung und -nutzung

(1) Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind.

(2) Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,

2. der Betroffene eingewilligt hat,

3. offensichtlich ist, daß es im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, daß er in Kenntnis des anderen Zwecks seine Einwilligung verweigern würde,

4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,

5. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Zweckänderung offensichtlich überwiegt,

6. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit erforderlich ist,

7. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des §11 Abs. 1 Nr. 8 des Strafgesetzbuches oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist,

8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder

9. es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluß der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(3) Eine Verarbeitung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für die speichernde Stelle dient. Das gilt auch für die Verarbeitung oder Nutzung zu Ausbildungs- und Prüfungszwecken durch die speichernde Stelle, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

(4) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet´werden.

§15 Datenübermittlung an öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist und

2. die Voraussetzungen vorliegen, die eine Nutzung nach §14 zulassen würden.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Empfängers, trägt dieser die Verantwortung. In diesem Falle prüft die übermittelnde Stelle nur, ob das

Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt, es sei denn, daß besonderer Anlaß zur Prüfung der Zulässigkeit der Übermittlung besteht. §10 Abs. 4 bleibt unberührt.

(3) Der Empfänger darf die übermittelten Daten für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen des §14 Abs. 2 zulässig.

(4) Für die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften gelten die Absätze 1 bis 3 entsprechend, sofern sichergestellt ist, daß bei dem Empfänger ausreichende Datenschutzmaßnahmen getroffen werden.

(5) Sind mit personenbezogenen Daten, die nach Absatz 1 übermittelt werden dürfen, weitere personenbezogene Daten des Betroffenen oder eines Dritten in Akten so verbunden, daß eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechtigte Interessen des Betroffenen oder eines Dritten an deren Geheimhaltung offensichtlich überwiegen; eine Nutzung dieser Daten ist unzulässig.

(6) Absatz 5 gilt entsprechend, wenn personenbezogene Daten innerhalb einer öffentlichen Stelle weitergegeben werden.

§16 Datenübermittlung an nicht-öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach §14 zulassen würden, oder

2. der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(3) In den Fällen der Übermittlung nach Absatz 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten. Dies gilt nicht, wenn damit zu rechnen ist, daß er davon auf andere Weise Kenntnis erlangt, oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde.

(4) Der Empfänger darf die übermittelten Daten nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Die übermittelnde Stelle hat den Empfänger darauf hinzuweisen. Eine Verarbeitung oder Nutzung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Absatz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.

§17 Datenübermittlung an Stellen außerhalb des Geltungsbereiches dieses Gesetzes

(1) Für die Übermittlung personenbezogener Daten an Stellen außerhalb des Geltungsbereichs dieses Gesetzes sowie an über- und zwischenstaatliche Stellen gilt §16 Abs. 1 nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen, sowie §16 Abs. 3.

(2) Eine Übermittlung unterbleibt, soweit Grund zu der Annahme besteht, daß durch sie gegen den Zweck eines deutschen Gesetzes verstoßen würde.

(3) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(4) Der Empfänger ist darauf hinzuweisen, daß die übermittelten Daten nur zu dem Zweck verarbeitet oder genutzt werden dürfen, zu dessen Erfüllung sie ihm übermittelt werden.

§18 Durchführung des Datenschutzes in der Bundesverwaltung

(1) Die obersten Bundesbehörden, der Präsident des Bundeseisenbahnvermögens sowie die bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, über die von der Bundesregierung oder einer obersten Bundesbehörde lediglich die Rechtsaufsicht ausgeübt wird, haben für ihren Geschäftsbereich die Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen. Das gleiche gilt für die Vorstände der aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen

Unternehmen, solange diesen ein ausschließliches Recht nach dem Postgesetz oder dem Gesetz über Fernmeldeanlagen zusteht.

(2) Die öffentlichen Stellen führen ein Verzeichnis der eingesetzten Datenverarbeitungsanlagen. Für ihre Dateien haben sie schriftlich festzulegen:

1. Bezeichnung und Art der Dateien,

2. Zweckbestimmung,

3. Art der gespeicherten Daten,

4. betroffenen Personenkreis,

5. Art der regelmäßig zu übermittelnden Daten und deren

Empfänger,

6. Regelfristen für die Löschung der Daten,

7. zugriffsberechtigte Personengruppen oder Personen, die allein zugriffsberechtigt sind.

Sie haben ferner dafür zu sorgen, daß die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, überwacht wird.

(3) Absatz 2 Satz 2 gilt nicht für Dateien, die nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Erstellung gelöscht werden.

7.1.1.2.2 Zweiter Unterabschnitt

Rechte des Betroffenen

§19 Auskunft an den Betroffenen

(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über 1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf Herkunft oder Empfänger dieser Daten beziehen, und

2. den Zweck der Speicherung.

In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Sind die personenbezogenen Daten in Akten gespeichert, wird die Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft

erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. Die speichernde Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

(2) Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb gespeichert sind, weil sie auf Grund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen.

(3) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministers der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(4) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben gefährden würde,

2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder

3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheimgehalten werden müssen und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muß.

(5) Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Falle ist der Betroffene darauf hinzuweisen, daß er sich an den Bundesbeauftragten für den Datenschutz wenden kann.

(6) Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Bundesbeauftragten für den Datenschutz zu erteilen, soweit nicht die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, daß dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung des Bundesbeauftragten an den Betroffenen darf keine Rückschlüsse auf den

Erkenntnisstand der speichernden Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

(7) Die Auskunft ist unentgeltlich.

§20 Berichtigung, Löschung und Sperrung von Daten

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Wird festgestellt, daß personenbezogene Daten in Akten unrichtig sind, oder wird ihre Richtigkeit von dem Betroffenen bestritten, so ist dies in der Akte zu vermerken oder auf

sonstige Weise festzuhalten.

(2) Personenbezogene Daten in Dateien sind zu löschen, wenn

1. ihre Speicherung unzulässig ist oder

2. ihre Kenntnis für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit

1. einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,

2. Grund zu der Annahme besteht, daß durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder

3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) Personenbezogene Daten in Dateien sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt.

(5) Personenbezogene Daten in Akten sind zu sperren, wenn die Behörde im Einzelfall feststellt, daß ohne die Sperrung schutzwürdige Interessen des Betroffenen beeinträchtigt würden und die Daten für die Aufgabenerfüllung der Behörde nicht mehr erforderlich sind.

(6) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerläßlich ist und

2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

(7) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer regelmäßigen Datenübermittlung diese

Daten zur Speicherung weitergegeben werden, wenn dies zur

Wahrung schutzwürdiger Interessen des Betroffenen erforderlich

ist.

(8) §2 Abs. 1 bis 6, 8 und 9 des Bundesarchivgesetzes ist anzuwenden.

§21 Anrufung des Bundesbeauftragten für den Datenschutz

Jedermann kann sich an denBundesbeauftragten für den Datenschutz wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen des Bundes in seinen Rechten verletzt worden zu sein. Für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch Gerichte des Bundes gilt dies nur, soweit diese in Verwaltungsangelegenheiten tätig werden.

7.1.1.2.3 Dritter Unterabschnitt

Bundesbeauftragter für den Datenschutz

§22 Wahl des Bundesbeauftragten für den Datenschutz

(1) Der Deutsche Bundestag wählt auf Vorschlag der Bundesregierung den Bundesbeauftragten für den Datenschutz mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder. Der Bundesbeauftragte muß bei seiner Wahl das 35. Lebensjahr vollendet haben. Der Gewählte ist vom Bundespräsidenten zu ernennen.

(2) Der Beauftragte leistet vor dem Bundesminister des Innern folgenden Eid:

> „Ich schwöre, daß ich meine Kraft dem Wohle des deutschen Volkes widmen, seinen Nutzen mehren, Schaden von ihm wenden, das Grundgesetz und die Gesetze des Bundes

wahren und verteidigen, meine Pflichten gewissenhaft erfüllen und Gerechtigkeit gegen jedermann üben werde. So wahr mir Gott helfe.„

Der Eid kann auch ohne religiöse Beteuerung geleistet werden.

(3) Die Amtszeit des Bundesbeauftragten beträgt fünf Jahre. Einmalige Wiederwahl ist zulässig.

(4) Der Bundesbeauftragte steht nach Maßgabe dieses Gesetzes zum Bund in einem öffentlich-rechtlichen Amtsverhältnis. Er ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Er untersteht der Rechtsaufsicht der Bundesregierung.

(5) Der Bundesbeauftragte wird beim Bundesminister des Innern eingerichtet. Er untersteht der Dienstaufsicht des Bundesministers des Innern. Dem Bundesbeauftragten ist die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen; sie ist im Einzelplan des Bundesministers des Innern in einem eigenen Kapitel auszuweisen. Die Stellen sind im Einvernehmen mit dem Bundesbeauftragten zu besetzen. Die Mitarbeiter können, falls sie mit der beabsichtigten Maßnahme nicht einverstanden sind, nur im Einvernehmen mit ihm versetzt, abgeordnet oder umgesetzt werden.

(6) Ist der Bundesbeauftragte vorübergehend an der Ausübung seines Amtes verhindert, kann der Bundesminister des Innern einen Vertreter mit der Wahrnehmung der Geschäfte beauftragen. Der Bundesbeauftragte soll dazu gehört werden.

§23 Rechtsstellung des Bundesbeauftragten für den Datenschutz

(1) Das Amtsverhältnis des Bundesbeauftragten für den Datenschutz beginnt mit der Aushändigung der Ernennungsurkunde. Es endet

1. mit Ablauf der Amtszeit,

2. mit der Entlassung.

Der Bundespräsident entläßt den Bundesbeauftragten, wenn dieser es verlangt oder auf Vorschlag der Bundesregierung, wenn Gründe vorliegen, die bei einem Richter auf Lebenszeit die Entlassung aus dem Dienst rechtfertigen. Im Falle der Beendigung des Amtsverhältnisses erhält der Bundesbeauftragte eine vom

Bundespräsidenten vollzogene Urkunde. Eine Entlassung wird mit der Aushändigung der Urkunde wirksam. Auf Ersuchen des Bundesministers des Innern ist der Bundesbeauftragte verpflichtet, die Geschäfte bis zur Ernennung seines Nachfolgers weiterzuführen.

(2) Der Bundesbeauftragte darf neben seinem Amt kein anderes besoldetes Amt, kein Gewerbe und keinen Beruf ausüben und weder der Leitung oder dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Landes angehören. Er darf nicht gegen Entgelt außergerichtliche Gutachten abgeben.

(3) Der Bundesbeauftragte hat dem Bundesminister des Innern Mitteilung über Geschenke zu machen, die er in bezug auf sein Amt erhält. Der Bundesminister des Innern entscheidet über die Verwendung der Geschenke.

(4) Der Bundesbeauftragte ist berechtigt, über Personen, die ihm in seiner Eigenschaft als Bundesbeauftragter Tatsachen anvertraut haben, sowie über diese Tatsachen selbst das Zeugnis zu verweigern. Dies gilt auch für die Mitarbeiter des Bundesbeauftragten mit der Maßgabe, daß über die Ausübung dieses Rechts der Bundesbeauftragte entscheidet. Soweit das Zeugnisverweigerungsrecht des Bundesbeauftragten reicht, darf die Vorlegung oder Auslieferung von Akten oder anderen Schriftstücken von ihm nicht gefordert werden.

(5) Der Bundesbeauftragte ist, auch nach Beendigung seines Amtsverhältnisses, verpflichtet, über die ihm amtlich bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Der Bundesbeauftragte darf, auch wenn er nicht mehr im Amt ist, über solche Angelegenheiten ohne Genehmigung des Bundesministers des Innern weder vor Gericht noch außergerichtlich aussagen oder Erklärungen abgeben. Unberührt bleibt die gesetzlich begründete Pflicht, Straftaten anzuzeigen und bei Gefährdung der freiheitlichen demokratischen Grundordnung für deren Erhaltung einzutreten.

(6) Die Genehmigung, als Zeuge auszusagen, soll nur versagt werden, wenn die Aussage dem Wohle des Bundes oder eines deutschen Landes Nachteile bereiten oder die Erfüllung öffentlicher Aufgaben ernstlich gefährden oder erheblich

erschweren würde. Die Genehmigung, ein Gutachten zu erstatten, kann versagt werden, wenn die Erstattung den dienstlichen Interessen Nachteile bereiten würde. §28 des Gesetzes über das Bundesverfassungsgericht in der Fassung der Bekanntmachung vom 12. Dezember 1985 (BGBl. I S. 2229) bleibt unberührt.

(7) Der Bundesbeauftragte erhält vom Beginn des Kalendermonats an, in dem das Amtsverhältnis beginnt, bis zum Schluß des Kalendermonats, in dem das Amtsverhältnis endet, im Falle des Absatzes 1 Satz 6 bis zum Ende des Monats, in dem die Geschäftsführung endet, Amtsbezüge in Höhe der einem Bundesbeamten der Besoldungsgruppe B 9 zustehenden Besoldung. Das Bundesreisekostengesetz und das Bundesumzugskostengesetz sind entsprechend anzuwenden. Im übrigen sind die §§13 bis 20 des Bundesministergesetzes in der Fassung der Bekanntmachung vom 27. Juli 1971 (BGBl. I S. 1166), zuletzt geändert durch das Gesetz zur Kürzung des Amtsgehalts der Mitglieder der Bundesregierung und der Parlamentarischen Staatssekretäre vom 22. Dezember 1982 (BGBl. I S. 2007), mit der Maßgabe anzuwenden, daß an die Stelle der zweijährigen Amtszeit in §15 Abs. 1 des Bundesministergesetzes eine Amtszeit von fünf Jahren tritt. Abweichend von Satz 3 in Verbindung mit den §§15 bis 17 des Bundesministergesetzes berechnet sich das Ruhegehalt des Bundesbeauftragten unter Hinzurechnung der Amtszeit als ruhegehaltsfähige Dienstzeit in entsprechender Anwendung des Beamtenversorgungsgesetzes, wenn dies günstiger ist und der Bundesbeauftragte sich unmittelbar vor seiner Wahl zum Bundesbeauftragten als Beamter oder Richter mindestens in dem letzten gewöhnlich vor Erreichen der Besoldungsgruppe B 9 zu durchlaufenden Amt befunden hat.

§24 Kontrolle durch den Bundesbeauftragten für den Datenschutz

(1) Der Bundesbeauftragte für den Datenschutz kontrolliert bei den öffentlichen Stellen des Bundes die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den´Datenschutz. Werden personenbezogene Daten in Akten verarbeitet oder genutzt, kontrolliert der Bundesbeauftragte die Erhebung, Verarbeitung oder Nutzung, wenn der Betroffene ihm hinreichende Anhaltspunkte dafür darlegt, daß er dabei in seinen Rechten verletzt worden ist, oder dem Bundesbeauftragten hinreichende Anhaltspunkte für eine derartige Verletzung vorliegen.

(2) Die Kontrolle des Bundesbeauftragten erstreckt sich auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach §30 der Abgabenordnung, unterliegen. Bei den Stellen des Bundes im Sinne des §2 Abs. 1 Satz 2 wird das Post- und Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) eingeschränkt, soweit dies zur Ausübung der Kontrolle bei den speichernden Stellen erforderlich ist. Das Kontrollrecht erstreckt sich mit Ausnahme von Nummer 1 nicht auf den Inhalt des Post- und Fernmeldeverkehrs. Der Kontrolle durch den Bundesbeauftragten unterliegen nicht:

1. personenbezogene Daten, die der Kontrolle durch die Kommission nach §9 des Gesetzes zu Artikel 10 Grundgesetz unterliegen, es sei denn, die Kommission ersucht den Bundesbeauftragten, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten, und

2. a) personenbezogene Daten, die dem Post- und Fernmeldegeheimnis nach Artikel 10 des Grundgesetzes unterliegen,

b) personenbezogene Daten, die dem Arztgeheimnis unterliegen und

c) personenbezogene Daten in Personalakten oder in den Akten über die Sicherheitsüberprüfung, wenn der Betroffene der Kontrolle der auf ihn bezogenen Daten im Einzelfall gegenüber dem Bundesbeauftragten für den Datenschutz widerspricht. Unbeschadet des Kontrollrechts des Bundesbeauftragten unterrichtet die öffentliche Stelle die Betroffenen in allgemeiner Form über das ihnen zustehende Widerspruchsrecht.

(3) Die Bundesgerichte unterliegen der Kontrolle des Bundesbeauftragten nur, soweit sie in Verwaltungsangelegenheiten tätig werden.

(4) Die öffentlichen Stellen des Bundes sind verpflichtet, den Bundesbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist dabei insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen und Akten, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Kontrolle nach Absatz 1 stehen,

2. jederzeit Zutritt in alle Diensträume zu gewähren.

Die in §6 Abs. 2 und §19 Abs. 3 genannten Behörden gewähren die Unterstützung nur dem Bundesbeauftragten selbst und den von ihm schriftlich besonders Beauftragten. Satz 2 gilt für diese Behörden nicht, soweit die oberste Bundesbehörde im Einzelfall feststellt, daß die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde.

(5) Der Bundesbeauftragte teilt das Ergebnis seiner Kontrolle der öffentlichen Stelle mit. Damit kann er Vorschläge zur Verbesserung des Datenschutzes, insbesondere zur Beseitigung von festgestellten Mängeln bei der Verarbeitung oder Nutzung personenbezogener Daten, verbinden. §25 bleibt unberührt.

(6) Absatz 2 gilt entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.

§25 Beanstandungen durch den Bundesbeauftragten für den Datenschutz

(1) Stellt der Bundesbeauftragte für den Datenschutz Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten fest, so beanstandet er dies

1. bei der Bundesverwaltung gegenüber der zuständigen obersten Bundesbehörde,

2. beim Bundeseisenbahnvermögen,

3. bei den aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz oder dem Gesetz über Fernmeldeanlagen zusteht, gegenüber deren Vorständen,

4. bei den bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ

und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. In den Fällen von Satz 1 Nr. 4 unterrichtet der Bundesbeauftragte gleichzeitig die zuständige Aufsichtsbehörde.

(2) Der Bundesbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt.

(3) Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung des Bundesbeauftragten getroffen worden sind. Die in Absatz 1 Satz 1 Nr. 4 genannten Stellen leiten der zuständigen Aufsichtsbehörde gleichzeitig eine Abschrift ihrer Stellungnahme an den Bundesbeauftragten zu.

§26 Weitere Aufgaben des Bundesbeauftragten für den Datenschutz, Dateienregister

(1) Der Bundesbeauftragte für den Datenschutz erstattet dem Deutschen Bundestagalle zwei Jahre einen Tätigkeitsbericht. Der Tätigkeitsbericht soll auch eine Darstellung der wesentlichen Entwicklung des Datenschutzes im nicht-öffentlichen Bereich enthalten.

(2) Auf Anforderung des Deutschen Bundestages oder der Bundesregierung hat der Bundesbeauftragte Gutachten zu erstellen und Berichte zu erstatten. Auf Ersuchen des Deutschen Bundestages, des Petitionsausschusses, des Innenausschusses oder der Bundesregierung geht der Bundesbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen des Bundes nach. Der Bundesbeauftragte kann sich jederzeit an den Deutschen Bundestag wenden.

(3) Der Bundesbeauftragte kann der Bundesregierung und den in §12 Abs. 1 genannten Stellen des Bundes Empfehlungen zur Verbesserung des Datenschutzes geben und sie in Fragen des Datenschutzes beraten. Die in §25 Abs. 1 Nr. 1 bis 4 genannten Stellen sind durch den Bundesbeauftragten zu unterrichten, wenn die Empfehlung oder Beratung sie nicht unmittelbar betrifft.

(4) Der Bundesbeauftragte wirkt auf die Zusammenarbeit mit den öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach §38 hin.

(5) Der Bundesbeauftragte führt ein Register der automatisiert geführten Dateien, in denen personenbezogene Daten gespeichert werden. Das gilt nicht für die Dateien der in §19 Abs. 3 genannten Behörden sowie für Dateien nach §18 Abs. 3. Die öffentlichen Stellen, deren Dateien in das Register aufgenommen werden, sind verpflichtet, dem Bundesbeauftragten eine Übersicht gemäß § 18 Abs.2 Satz2 Nr.1 bis 6 zuzuleiten. Das Register kann von jedermann eingesehen werden. Die Angaben nach §18 Abs. 2Satz 2Nr. 3und 5über Dateien der in §6 Abs. 2 genannten

Behörden unterliegen nicht der Einsichtnahme. Der Bundesbeauftragte kann im Einzelfall für andere öffentliche Stellen mit deren Einverständnis festlegen, daß einzelne Angaben nicht der Einsichtnahme unterliegen.

7.1.1.3 Dritter Abschnitt

Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen

7.1.1.3.1 Erster Unterabschnitt

Rechtsgrundlagen der Datenverarbeitung

§27 Anwendungsbereich

(1) Die Vorschriften dieses Abschnittes finden Anwendung, soweit personenbezogene Daten in oder aus Dateien geschäftsmäßig oder für berufliche oder gewerbliche Zwecke verarbeitet oder genutzt werden durch

1. nicht-öffentliche Stellen,

2. a) öffentliche Stellen des Bundes, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen,

b) öffentliche Stellen der Länder, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, Bundesrecht ausführen und der Datenschutz nicht durch

Landesgesetz geregelt ist.

In den Fällen der Nummer 2 Buchstabe a gelten anstelle des §38 die §§ 18, 21 und 24 bis 26.

(2) Die Vorschriften dieses Abschnittes gelten nicht für die Verarbeitung und Nutzung personenbezogener Daten in Akten, soweit es sich nicht um personenbezogene Daten handelt, die offensichtlich aus einer Datei entnommen worden sind.

§28 Datenspeicherung, -übermittlung und –nutzung für eigene Zwecke

(1) Das Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

1. im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen,

2. soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zu der Annahme besteht, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Verarbeitung oder Nutzung überwiegt,

3. wenn die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Verarbeitung oder Nutzung offensichtlich überwiegt,

4. wenn es im Interesse der speichernden Stelle zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluß der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

Die Daten müssen nach Treu und Glauben und auf rechtmäßige Weise erhoben werden.

(2) Die Übermittlung oder Nutzung ist auch zulässig

1. a) soweit es zur Wahrung berechtigter Interessen eines Dritten oder öffentlicher Interessen erforderlich ist oder

b) wenn es sich um listenmäßig oder sonst zusammengefaßte Daten über Angehörige einer Personengruppe handelt, die sich auf

- eine Angabe über die Zugehörigkeit des Betroffenen zu dieser Personengruppe,
- Berufs-, Branchen- oder Geschäftsbezeichnung,
- Namen,
- Titel,
- akademische Grade,
- Anschrift,
- Geburtsjahr

beschränken und kein Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat. In den Fällen des Buchstabens b kann im allgemeinen davon ausgegangen werden, daß dieses

Interesse besteht, wenn im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses gespeicherte Daten übermittelt werden sollen, die sich

- auf gesundheitliche Verhältnisse,
- auf strafbare Handlungen,
- auf Ordnungswidrigkeiten,
- auf religiöse oder politische Anschauungen sowie
- bei Übermittlung durch den Arbeitgeber auf arbeitsrechtliche Rechtsverhältnisse

beziehen, oder

2. wenn es im Interesse einer Forschungseinrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluß der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(3) Widerspricht der Betroffene bei der speichernden Stelle der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung, ist eine Nutzung oder Übermittlung für diese Zwecke unzulässig. Widerspricht der Betroffene beim Empfänger der nach Absatz 2 übermittelten Daten der Verarbeitung oder Nutzung für Zwecke der Werbung oder der Markt- oder Meinungsforschung, hat dieser die Daten für diese Zwecke zu sperren.

(4) Der Empfänger darf die übermittelten Daten für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen der Absätze 1 und 2 zulässig. Die übermittelnde Stelle hat den Empfänger darauf hinzuweisen.

§29 Geschäftsmäßige Datenspeicherung zum Zwecke der Übermittlung

(1) Das geschäftsmäßige Speichern oder Verändern personenbezogener Daten zum Zwecke der Übermittlung ist zulässig, wenn

1. kein Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Speicherung oder Veränderung hat, oder

2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Speicherung oder Veränderung offensichtlich überwiegt.

§28 Abs.1 Satz 2 ist anzuwenden.

(2) Die Übermittlung ist zulässig, wenn

1. a) der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat oder

b) es sich um listenmäßig oder sonst zusammengefaßte Daten nach §28 Abs.2 Nr.1 Buchstabe b handelt, die für Zwecke der Werbung oder der Markt- oder Meinungsforschung übermittelt werden sollen, und

2. kein Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat.

§28 Abs. 2 Nr. 1 Satz 2 gilt entsprechend. Bei der Übermittlung nach Nummer 1 Buchstabe a sind die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung von der übermittelnden Stelle aufzuzeichnen. Bei der Übermittlung im automatisierten Abrufverfahren obliegt die Aufzeichnungspflicht dem Empfänger.

(3) Für die Verarbeitung oder Nutzung der übermittelten Daten gilt §28 Abs. 3 und 4.

§30 Geschäftsmäßige Datenspeicherung zum Zwecke der Übermittlung in anonymisierter Form

(1) Werden personenbezogene Daten geschäftsmäßig gespeichert, um sie in anonymisierter Form zu übermitteln, sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Diese Merkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit dies für die Erfüllung des Zweckes der Speicherung oder zu wissenschaftlichen Zwecken erforderlich ist.

(2) Die Veränderung personenbezogener Daten ist zulässig, wenn

1. kein Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Veränderung hat, oder

2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Veränderung offensichtlich überwiegt.

(3) Die personenbezogenen Daten sind zu löschen, wenn ihre Speicherung unzulässig ist.

(4) Die §§ 29, 33 bis 35 gelten nicht.

§31 Besondere Zweckbindung

Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

§32 Meldepflichten

(1) Die Stellen, die personenbezogene Daten geschäftsmäßig

1. zum Zwecke der Übermittlung speichern,

2. zum Zwecke der anonymisierten Übermittlung speichern oder

3. im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen,

sowie ihre Zweigniederlassungen und unselbständigen Zweigstellen haben die Aufnahme und Beendigung ihrer Tätigkeit der zuständigen Aufsichtsbehörde innerhalb eines Monats mitzuteilen.

(2) Bei der Anmeldung sind folgende Angaben für das bei der Aufsichtsbehörde geführt Register mitzuteilen:

1. Name oder Firma der Stelle,

2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzlich oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,

3. Anschrift,

4. Geschäftszwecke der Stelle und der Datenverarbeitung,

5. Name des Beauftragten für den Datenschutz,

6. allgemeine Beschreibung der Art der gespeicherten perso-nenbezogenen Daten. Im Falle des Absatzes 1 Nr. 3 ist diese Angabe nicht erforderlich.

(3) Bei der Anmeldung sind außerdem folgende Angaben mit-zuteilen, die nicht in das Register aufgenommen werden:

1. Art der eingesetzten Datenverarbeitungsanlagen,

2. bei regelmäßiger Übermittlung personenbezogener Daten Empfänger und Art der übermittelten Daten.

(4) Absatz 1 gilt für die Änderung der nach Absätzen 2 und 3 mitgeteilten Angaben entsprechend.

(5) Die Aufsichtsbehörde kann im Einzelfall festlegen, welche Angaben nach Absatz 2 Nr. 4 und 6, Absatz 3 und Absatz 4 mitgeteilt werden müssen. Der mit den Mitteilungen verbundene Aufwand muß in einem angemessenen Verhältnis zu ihrer Bedeutung für die Überwachung durch die Aufsichtsbehörde stehen.

7.1.1.3.2 Zweiter Unterabschnitt

Rechte des Betroffenen

§33 Benachrichtigung des Betroffenen

(1) Werden erstmals personenbezogene Daten für eigene Zwecke gespeichert, ist der Betroffene von der Speicherung und der Art der Daten zu benachrichtigen. Werden personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert, ist der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen.

(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,

2. die Daten nur deshalb gespeichert sind, weil sie auf Grund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich der Datensicherung oder der Datenschutzkontrolle dienen,

3. die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheimgehalten werden müssen,

4. die zuständige öffentliche Stelle gegenüber der speichernden Stelle festgestellt hat, daß das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,

5. die Daten in einer Datei gespeichert werden, die nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Erstellung gelöscht wird,

6. die Daten für eigene Zwecke gespeichert sind und

a) aus allgemein zugänglichen Quellen entnommen sind oder

b) die Benachrichtigung die Geschäftszwecke der speichernden Stelle erheblich gefährden würde, es sei denn, daß das Interesse an der Benachrichtigung die Gefährdung überwiegt, oder

7. die Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert sind und

a) aus allgemein zugänglichen Quellen entnommen sind, soweit sie sich auf diejenigen Personen beziehen, die diese Daten veröffentlicht haben, oder

b) es sich um listenmäßig oder sonst zusammengefaßte Daten handelt (§29 Abs. 2 Nr. 1 Buchstabe b).

§34 Auskunft an den Betroffenen

(1) Der Betroffene kann Auskunft verlangen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf Herkunft und Empfänger beziehen,

2. den Zweck der Speicherung und

3. Personen und Stellen, an die seine Daten regelmäßig übermittelt werden, wenn seine Daten automatisiert verarbeitet werden.

Er soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen. Werden die personenbezogenen Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert, kann der Betroffene über Herkunft und Empfänger nur Auskunft verlangen, wenn er begründete Zweifel an der Richtigkeit

der Daten geltend macht. In diesem Falle ist Auskunft über Herkunft und Empfänger auch dann zu erteilen, wenn diese Angaben nicht gespeichert sind.

(2) Der Betroffene kann von Stellen, die geschäftsmäßig personenbezogene Daten zum Zwecke der Auskunftserteilung speichern, Auskunft über seine personenbezogenen Daten verlangen, auch wenn sie nicht in einer Datei gespeichert sind. Auskunft über Herkunft und Empfänger kann der Betroffene nur verlangen, wenn er begründete Zweifel an der Richtigkeit der Daten geltend macht. §38 Abs. 1 ist mit der Maßgabe anzuwenden, daß die Aufsichtsbehörde im Einzelfall die Einhaltung von Satz 1 überprüft, wenn der Betroffene begründet darlegt, daß die Auskunft nicht oder nicht richtig erteilt worden ist.

(3) Die Auskunft wird schriftlich erteilt, soweit nicht wegen der besonderen Umstände eine andere Form der Auskunftserteilung angemessen ist.

(4) Eine Pflicht zur Auskunftserteilung besteht nicht, wenn der Betroffene nach §33 Abs. 2 Nr. 2 bis 6 nicht zu benachrichtigen ist.

(5) Die Auskunft ist unentgeltlich. Werden die personenbezogenen Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert, kann jedoch ein Entgelt verlangt werden, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann. Das Entgelt darf über die durch die Auskunftserteilung entstandenen direkt zurechenbaren Kosten nicht hinausgehen. Ein Entgelt kann in den Fällen nicht verlangt werden, in denen besondere Umstände die Annahme rechtfertigen, daß Daten unrichtig oder unzulässig gespeichert werden, oder in denen die Auskunft ergibt, daß die Daten zu berichtigen oder unter der Voraussetzung des §35 Abs. 2 Satz 2 Nr. 1 zu löschen sind.

(6) Ist die Auskunftserteilung nicht unentgeltlich, ist dem Betroffenen die Möglichkeit zu geben, sich im Rahmen seines Auskunftsanspruchs persönlich Kenntnis über die ihn betreffenden Daten und Angaben zu verschaffen. Er ist hierauf in geeigneter Weise hinzuweisen.

§35 Berichtigung, Löschung und Sperrung von Daten

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.

(2) Personenbezogene Daten können außer in den Fällen des Absatzes 3 Nr. 1 und 2 jederzeit gelöscht werden. Personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig ist,

2. es sich um Daten über gesundheitliche Verhältnisse, strafbare Handlungen, Ordnungswidrigkeiten sowie religiöse oder politische Anschauungen handelt und ihre Richtigkeit von der speichernden Stelle nicht bewiesen werden kann,

3. sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist, oder

4. sie geschäftsmäßig zum Zwecke der Übermittlung verarbeitet werden und eine Prüfung am Ende des fünften Kalenderjahres nach ihrer erstmaligen Speicherung ergibt, daß eine längerwährende Speicherung nicht erforderlich ist.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit

1. im Falle des Absatzes 2 Nr. 3 oder 4 einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,

2. Grund zu der Annahme besteht, daß durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder

3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) Personenbezogene Daten sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt.

(5) Personenbezogene Daten, die unrichtig sind oder deren Richtigkeit bestritten wird, müssen bei der geschäftsmäßigen Datenspeicherung zum Zwecke der Übermittlung außer in den Fällen des Absatzes 2 Nr. 2 nicht berichtigt, gesperrt oder gelöscht werden, wenn sie aus allgemein zugänglichen Quellen entnommen und zu Dokumentationszwecken gespeichert sind. Auf Verlangen des Betroffenen ist diesen Daten für die Dauer der Speicherung seine Gegendarstellung beizufügen. Die Daten dürfen nicht ohne diese Gegendarstellung übermittelt werden.

(6) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer regelmäßigen Datenübermittlung diese Daten zur Speicherung weitergegeben werden, wenn dies zur Wahrung der schutzwürdigen Interessen des Betroffenen erforderlich ist.

(7) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerläßlich ist und

2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

7.1.1.3.3 Dritter Unterabschnitt

Beauftragter für den Datenschutz, Aufsichtsbehörde

§36 Bestellung eines Beauftragten für den Datenschutz

(1) Die nicht-öffentlichen Stellen, die personenbezogene Daten automatisiert verarbeiten und damit in der Regel mindestens fünf Arbeitnehmer ständig beschäftigen, haben spätestens innerhalb eines Monats nach Aufnahme ihrer Tätigkeit einen Beauftragten für den Datenschutz schriftlich zu bestellen. Das gleiche gilt, wenn personenbezogene Daten auf andere Weise verarbeitet werden und damit in der Regel mindestens zwanzig Arbeitnehmer ständig beschäftigt sind.

(2) Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt.

(3) Der Beauftragte für den Datenschutz ist dem Inhaber, dem Vorstand, dem Geschäftsführer oder dem sonstigen gesetzlich oder nach der Verfassung des Unternehmens berufenen Leiter unmittelbar zu unterstellen. Er ist bei Anwendung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Die Bestellung zum Beauftragten für den Datenschutz kann nur auf Verlangen der Aufsichtsbehörde oder in entsprechender Anwendung von §626 des Bürgerlichen Gesetzbuchs widerrufen werden.

(4) Der Beauftragte für den Datenschutz ist zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen befreit wird.

(5) Die nicht-öffentliche Stelle hat den Beauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen und ihm insbesondere, soweit dies zur

Erfüllungseiner Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen.

§37 Aufgaben des Beauftragten für den Datenschutz

(1) Der Beauftragte für den Datenschutz hat die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz sicherzustellen. Zu diesem Zweck kann er sich in Zweifelsfällen an die Aufsichtsbehörde wenden. Er hat insbesondere

1. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten,

2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz, bezogen auf die besonderen Verhältnisse in diesem Geschäftsbereich und die sich daraus ergebenden besonderen Erfordernisse für den Datenschutz, vertraut zu machen,

3. bei der Auswahl der bei der Verarbeitung personenbezogener Daten tätigen Personen beratend mitzuwirken.

(2) Dem Beauftragten ist von der nicht-öffentlichen Stelle eine Übersicht zur Verfügung zu stellen über

1. eingesetzte Datenverarbeitungsanlagen,

2. Bezeichnung und Art der Dateien,

3. Art der gespeicherten Daten,

4. Geschäftszwecke, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist,

5. deren regelmäßige Empfänger,

6. zugriffsberechtigte Personengruppen oder Personen, die allein zugriffsberechtigt sind.

(3) Absatz 2 Nr. 2 bis 6 gilt nicht für Dateien, die nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Erstellung gelöscht werden.

§38 Aufsichtsbehörde

(1) Die Aufsichtsbehörde überprüft im Einzelfall die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die Verarbeitung oder Nutzung personenbezogener Daten in oder aus Dateien regeln, wenn ihr hinreichende Anhaltspunkte dafür vorliegen, daß eine dieser Vorschriften durch nicht-öffentliche Stellen verletzt ist, insbesondere wenn es der Betroffene selbst begründet darlegt.

(2) Werden personenbezogene Daten geschäftsmäßig

1. zum Zwecke der Übermittlung gespeichert,

2. zum Zwecke der anonymisierten Übermittlung gespeichert oder

3. im Auftrag durch Dienstleistungsunternehmen verarbeitet,

überwacht die Aufsichtsbehörde die Ausführung dieses Gesetzes oder anderer Vorschriften über den Datenschutz, soweit diese die Verarbeitung oder Nutzung personenbezogener Daten in oder aus Dateien regeln. Die Aufsichtsbehörde führt das Register nach §32 Abs. 2. Das Register kann von jedem eingesehen werden.

(3) Die der Prüfung unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen haben der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in §383 Abs. 1 Nr. 1 bis 3 der Zivilprozeßordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Der Auskunftspflichtige ist darauf hinzuweisen.

(4) Die von der Aufsichtsbehörde mit der Überprüfung oder Überwachung beauftragten Personen sind befugt, soweit es zur Erfüllung der der Aufsichtsbehörde übertragenen Aufgaben erforderlich ist, während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume der Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen. Sie können geschäftliche Unterlagen, insbesondere die Übersicht nach §37 Abs. 2 sowie die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme, einsehen. §24 Abs. 6 gilt entsprechend. Der Auskunftspflichtige hat diese Maßnahmen zu dulden.

(5) Zur Gewährleistung des Datenschutzes nach diesem Gesetz und anderen Vorschriften über den Datenschutz, soweit diese die Verarbeitung oder Nutzung

personenbezogener Daten in oder aus Dateien regeln, kann die Aufsichtsbehörde anordnen, daß im Rahmen der Anforderungen nach §9 Maßnahmen zur Beseitigung festgestellter technischer oder organisatorischer Mängel getroffen werden. Bei schwerwiegenden Mängeln dieser Art, insbesondere, wenn sie mit besonderer Gefährdung des Persönlichkeitsrechts verbunden sind, kann sie den Einsatz einzelner Verfahren untersagen, wenn die Mängel entgegen der Anordnung nach Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden. Sie kann die Abberufung des Beauftragten für den Datenschutz verlangen, wenn er die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt.

(6) Die Landesregierungen oder die von ihnen ermächtigten Stellen bestimmen die für die Überwachung der Durchführung des Datenschutzes im Anwendungsbereich dieses Abschnittes zuständigen Aufsichtsbehörden.

(7) Die Anwendung der Gewerbeordnung auf die den Vorschriften dieses Abschnitts unterliegenden Gewerbebetriebe bleibt unberührt.

7.1.1.4 Vierter Abschnitt

Sondervorschriften

§39 Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen

(1) Personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und die von der zur Verschwiegenheit verpflichteten Stelle in Ausübung ihrer Berufs- oder Amtspflicht zur Verfügung gestellt worden sind, dürfen von der speichernden Stelle nur für den Zweck verarbeitet oder genutzt werden, für den sie sie erhalten hat. In die Übermittlung an eine nicht-öffentliche Stelle muß die zur Verschwiegenheit verpflichtete Stelle einwilligen.

(2) Für einen anderen Zweck dürfen die Daten nur verarbeitet oder genutzt werden, wenn die Änderung des Zwecks durch besonderes Gesetz zugelassen ist.

§40 Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen

(1) Für Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für Zwecke der wissenschaftlichen Forschung verarbeitet oder genutzt werden.

(2) Die Übermittlung personenbezogener Daten an andere als öffentliche Stellen für Zwecke der wissenschaftlichen Forschung ist nur zulässig, wenn diese sich verpflichten, die übermittelten Daten nicht für andere Zwecke zu verarbeiten oder zu nutzen und die Vorschrift des Absatzes 3 einzuhalten.

(3) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.

(4) Die wissenschaftliche Forschung betreibenden Stellen dürfen personenbezogene Daten nur veröffentlichen, wenn

1. der Betroffene eingewilligt hat oder

2. dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerläßlich ist.

§41 Verarbeitung und Nutzung personenbezogener Daten durch die Medien

(1) Soweit personenbezogene Daten von Unternehmen oder Hilfsunternehmen der Presse oder des Films oder von Hilfsunternehmen des Rundfunks ausschließlich zu eigenen journalistisch-redaktionellen Zwecken verarbeitet oder genutzt werden, gelten

von den Vorschriften dieses Gesetzes nur die §§5 und 9. Soweit Verlage personenbezogene Daten zur Herausgabe von Adressen-, Telefon-, Branchen- oder vergleichbaren Verzeichnissen verarbeiten oder nutzen, gilt Satz 1 nur, wenn mit der Herausgabe zugleich eine journalistisch-redaktionelle Tätigkeit verbunden ist.

(2) Führt die journalistisch-redaktionelle Verarbeitung oder Nutzungpersonenbezogener Daten durch die Rundfunkanstalten des Bundesrechts zur Veröffentlichung von Gegendarstellungen des Betroffenen, so sind diese

Gegendarstellungen zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst .

(3) Wird jemand durch eine Berichterstattung der Rundfunkanstalten des Bundesrechts in seinem Persönlichkeitsrecht beeinträchtigt, so kann er Auskunft über die der Berichterstattung zugrundeliegenden, zu seiner Person gespeicherten Daten verlangen. Die Auskunft kann verweigert werden, soweit aus den Daten auf die Person des Verfassers, Einsenders oder Gewährsmannes von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann. Der Betroffene kann die Berichtigung unrichtiger Daten verlangen.

(4) Im übrigen gelten für die Rundfunkanstalten des Bundesrechts von den Vorschriften dieses Gesetzes die §§5 und 9. Anstelle der §§24 bis 26 gilt §42, auch soweit es sich um Verwaltungsangelegenheiten handelt.

§42 Datenschutzbeauftragte der Rundfunkanstalten des Bundesrechts

(1) Die Rundfunkanstalten des Bundesrechts bestellen jeweils einen Beauftragten für den Datenschutz, der an die Stelle des Bundesbeauftragten für den Datenschutz tritt. Die Bestellung erfolgt auf Vorschlag des Intendanten durch den Verwaltungsrat für die Dauer von vier Jahren, wobei Wiederbestellungen zulässig sind. Das Amt eines Beauftragten für den Datenschutz kann neben anderen Aufgaben innerhalb der Rundfunkanstalt wahrgenommen werden.

(2) Der Beauftragte für den Datenschutz kontrolliert die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz. Er ist in Ausübung dieses Amtes unabhängig und nur dem Gesetz unterworfen. Im übrigen untersteht er der Dienst- und Rechtsaufsicht des Verwaltungsrates.

(3) Jedermann kann sich entsprechend §21 Satz 1 an den Beauftragten für den Datenschutz wenden.

(4) Der Beauftragte für den Datenschutz erstattet den Organen der jeweiligen Rundfunkanstalt des Bundesrechts alle zwei Jahre, erstmals zum 1. Januar 1994 einen Tätigkeitsbericht. Er erstattet darüber hinaus besondere Berichte auf Beschluß eines Organes der jeweiligen Rundfunkanstalt. Die Tätigkeitsberichte übermittelt der Beauftragte auch an den Bundesbeauftragten für den Datenschutz.

(5) Weitere Regelungen entsprechend den §§23 bis 26 treffen die Rundfunkanstalten des Bundesrechts jeweils für ihren Bereich. §18 bleibt unberührt.

7.1.1.5 Fünfter Abschnitt

Schlußvorschriften

§43 Strafvorschriften

(1) Wer unbefugt von diesem Gesetz geschützte personenbezogene Daten, die nicht offenkundig sind,

1. speichert, verändert oder übermittelt,

2. zum Abruf mittels automatisierten Verfahrens bereithält oder

3. abruft oder sich oder einem anderen aus Dateien verschafft,

wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer

1. die Übermittlung von durch dieses Gesetz geschützten personenbezogenen Daten, die nicht offenkundig sind, durch unrichtige Angaben erschleicht,

2. entgegen §16 Abs. 4 Satz 1, §28 Abs. 4 Satz 1, auch in Verbindung mit §29 Abs. 3, §39 Abs. 1 Satz 1 oder §40 Abs. 1 die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt, oder

3. entgegen §30 Abs. 1 Satz 2 die in §30 Abs. 1 Satz 1 bezeichneten Merkmale oder entgegen § 40 Abs. 3 Satz 3 die in § 40 Abs. 3 Satz 2 bezeichneten Merkmale mit den Einzelangaben zusammenführt.

(3) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geld-strafe.

(4) Die Tat wird nur auf Antrag verfolgt.

§44 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig 1. entgegen §29 Abs. 2 Satz 3 oder 4 die dort bezeichneten Gründe oder die Art und Weise ihrer glaubhaften Darlegung nicht aufzeichnet,

2. entgegen §32 Abs. 1, auch in Verbindung mit Absatz 4, eine Meldung nicht oder nicht rechtzeitig erstattet oder entgegen §32 Abs. 2, auch in Verbindung mit Absatz

4, bei einer solchen Meldung die erforderlichen Angaben nicht, nicht richtig oder nicht vollständig mitteilt,

3. entgegen §33 Abs. 1 den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt,

4. entgegen §35 Abs. 5 Satz 3 Daten ohne Gegendarstellung übermittelt,

5. entgegen §36 Abs. 1 einen Beauftragten für den Datenschutz nicht oder nicht rechtzeitig bestellt,

6. entgegen §38Abs. 3Satz 1eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder entgegen §38 Abs. 4 Satz 4 den Zutritt zu den Grundstücken oder Geschäftsräumen oder die Vornahme von Prüfungen oder Besichtigungen oder die Einsicht in geschäftliche Unterlagen nicht duldet, oder

7. einer vollziehbaren Anordnung nach §38 Abs. 5 Satz 1 zuwiderhandelt.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Deutsche Mark geahndet werden.

7.1.2 Gesetz zur digitalen Signatur (Signaturgesetz - SigG)

Vom 22. Juli 1997 (BGBl I Nr. 52, 1870), Artikel 3 des Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz – IuKDG)

§ 1 Zweck und Anwendungsbereich

(1) Zweck des Gesetzes ist es, Rahmenbedingungen für digitale Signaturen zu schaffen, unter denen diese als sicher gelten und Fälschungen digitaler Signaturen oder Verfälschungen von signierten Daten zuverlässig festgestellt werden können.

(2) Die Anwendung anderer Verfahren für digitale Signaturen ist freigestellt, soweit nicht digitale Signaturen nach diesem Gesetz durch Rechtsvorschrift vorgeschrieben sind.

§ 2 Begriffsbestimmungen

(1) Eine digitale Signatur im Sinne dieses Gesetzes ist ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüssel-Zertifikat einer Zertifizierungsstelle oder der Behörde nach § 3 versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen läßt.

(2) Eine Zertifizierungsstelle im Sinne dieses Gesetzes ist eine natürliche oder juristische Person, die die Zuordnung von öffentlichen Signaturschlüsseln zu natürlichen Personen bescheinigt und dafür eine Genehmigung gemäß § 4 besitzt.
(3) Ein Zertifikat im Sinne dieses Gesetzes ist eine mit einer digitalen Signatur versehene digitale Bescheinigung über die Zuordnung eines öffentlichen Signaturschlüssels zu einer natürlichen Person (Signaturschlüssel-Zertifikat) oder eine gesonderte digitale Bescheinigung, die unter eindeutiger Bezugnahme auf ein Signaturschlüssel-Zertifikat weitere Angaben enthält (Attribut-Zertifikat).
(4) Ein Zeitstempel im Sinne dieses Gesetzes ist eine mit einer digitalen Signatur versehene digitale Bescheinigung einer Zertifizierungsstelle, daß ihr bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorgelegen haben.

§ 3 Zuständige Behörde

Die Erteilung von Genehmigungen und die Ausstellung von Zertifikaten, die zum Signieren von Zertifikaten eingesetzt werden, sowie die Überwachung der Einhaltung dieses Gesetzes und der Rechtsverordnung nach § 16 obliegen der Behörde nach § 66 des Telekommunikationsgesetzes.

§ 4 Genehmigung von Zertifizierungsstellen

(1) Der Betrieb einer Zertifizierungsstelle bedarf einer Genehmigung der zuständigen Behörde. Diese ist auf Antrag zu erteilen.
(2) Die Genehmigung ist zu versagen, wenn Tatsachen die Annahme rechtfertigen, daß der Antragsteller nicht die für den Betrieb einer Zertifizierungsstelle erforderliche Zuverlässigkeit besitzt, wenn der Antragsteller nicht nachweist, daß die für den Betrieb einer Zertifizierungsstelle erforderliche Fachkunde vorliegt, oder wenn zu erwarten ist, daß bei Aufnahme des Betriebes die übrigen Voraussetzungen für den Betrieb der Zertifizierungsstelle nach diesem Gesetz und der Rechtsverordnung nach § 16 nicht vorliegen werden.
(3) Die erforderliche Zuverlässigkeit besitzt, wer die Gewähr dafür bietet, als Inhaber der Zertifizierungsstelle die für deren Betrieb maßgeblichen Rechtsvorschriften einzuhalten. Die erforderliche Fachkunde liegt vor, wenn die im Betrieb der Zertifizierungsstelle tätigen Personen über die dafür erforderlichen Kenntnisse, Erfahrungen und Fertigkeiten verfügen. Die übrigen Voraussetzungen für den Betrieb der Zertifizierungsstelle liegen vor, wenn die Maßnahmen zur Erfüllung der Sicherheitsanforderungen dieses Gesetzes und der Rechtsverordnung nach § 16 der zuständigen Behörde rechtzeitig in einem Sicherheitskonzept aufgezeigt und die

Umsetzung durch eine von der zuständigen Behörde anerkannten Stelle geprüft und bestätigt worden ist.

(4) Die Genehmigung kann mit Nebenbestimmungen versehen werden, soweit dies erforderlich ist um sicherzustellen, daß die Zertifizierungsstelle bei Aufnahme des Betriebes und im Betrieb die Voraussetzungen dieses Gesetzes und der Rechtsverordnung nach § 16 erfüllt.

(5) Die zuständige Behörde stellt für Signaturschlüssel, die zum Signieren von Zertifikaten eingesetzt werden, die Zertifikate aus. Die Vorschriften für die Vergabe von Zertifikaten durch Zertifizierungsstellen gelten für die zuständige Behörde entsprechend. Diese hat die von ihr ausgestellten Zertifikate jederzeit für jeden über öffentlich erreichbare Telekommunikationsverbindungen nachprüfbar und abrufbar zu halten. Dies gilt auch für Informationen über Anschriften und Rufnummern der Zertifizierungsstellen, die Sperrung von von ihr ausgestellten Zertifikaten, die Einstellung und die Untersagung des Betriebs einer Zertifizierungsstelle sowie die Rücknahme oder den Widerruf von Genehmigungen.

(6) Für öffentliche Leistungen nach diesem Gesetz und der Rechtsverordnung nach § 16 werden Kosten (Gebühren und Auslagen) erhoben.

§ 5 Vergabe von Zertifikaten

(1) Die Zertifizierungsstelle hat Personen, die ein Zertifikat beantragen, zuverlässig zu identifizieren. Sie hat die Zuordnung eines öffentlichen Signaturschlüssels zu einer identifizierten Person durch ein Signaturschlüssel-Zertifikat zu bestätigen und dieses sowie Attribut-Zertifikate jederzeit für jeden über öffentlich erreichbare Telekommunikationsverbindungen nachprüfbar und mit Zustimmung des Signaturschlüssel-Inhabers abrufbar zu halten.

(2) Die Zertifizierungsstelle hat auf Verlangen eines Antragstellers Angaben über seine Vertretungsmacht für eine dritte Person sowie zur berufsrechtlichen oder sonstigen Zulassung in das Signaturschlüssel-Zertifikat oder ein Attribut-Zertifikat aufzunehmen, soweit ihr die Einwilligung des Dritten zur Aufnahme dieser Vertretungsmacht oder die Zulassung zuverlässig nachgewiesen wird.

(3) Die Zertifizierungsstelle hat auf Verlangen eines Antragstellers im Zertifikat anstelle seines Namens ein Pseudonym aufzuführen.

(4) Die Zertifizierungsstelle hat Vorkehrungen zu treffen, damit Daten für Zertifikate nicht unbemerkt gefälscht oder verfälscht werden können. Sie hat weiter Vorkehrungen zu treffen, um die Geheimhaltung der privaten Signaturschlüssel zu

gewährleisten. Eine Speicherung privater Signaturschlüssel bei der Zertifizierungsstelle ist unzulässig.

(5) Die Zertifizierungsstelle hat für die Ausübung der Zertifizierungstätigkeit zuverlässiges Personal einzusetzen. Für das Bereitstellen von Signaturschlüsseln sowie das Erstellen von Zertifikaten hat sie technische Komponenten gemäß § 14 einzusetzen. Dies gilt auch für technische Komponenten, die ein Nachprüfen von Zertifikaten nach Absatz 1 Satz 2 ermöglichen.

§ 6 Unterrichtungspflicht

Die Zertifizierungsstelle hat die Antragsteller nach § 5 Abs. 1 über die Maßnahmen zu unterrichten, die erforderlich sind, um zu sicheren digitalen Signaturen und deren zuverlässiger Prüfung beizutragen. Sie hat die Antragsteller darüber zu unterrichten, welche technischen Komponenten die Anforderungen nach § 14 Abs. 1 und 2 erfüllen, sowie über die Zuordnung der mit einem privaten Signaturschlüssel erzeugten digitalen Signaturen. Sie hat die Antragsteller darauf hinzuweisen, daß Daten mit digitaler Signatur bei Bedarf neu zu signieren sind, bevor der Sicherheitswert der vorhandenen Signatur durch Zeitablauf geringer wird.

§ 7 Inhalt von Zertifikaten

(1) Das Signaturschlüssel-Zertifikat muß folgende Angaben enthalten:

1. den Namen des Signaturschlüssel-Inhabers, der im Falle einer Verwechslungsmöglichkeit mit einem Zusatz zu versehen ist, oder ein dem Signaturschlüssel-Inhaber zugeordnetes unverwechselbares Pseudonym, das als solches kenntlich sein muß,
2. den zugeordneten öffentlichen Signaturschlüssel,
3. die Bezeichnung der Algorithmen, mit denen der öffentliche Schlüssel des Signaturschlüssel-Inhabers sowie der öffentliche Schlüssel der Zertifizierungsstelle benutzt werden kann,
4. die laufende Nummer des Zertifikates,
5. Beginn und Ende der Gültigkeit des Zertifikates,
6. den Namen der Zertifizierungsstelle und
7. Angaben, ob die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art und Umfang beschränkt ist.

(2) Angaben zur Vertretungsmacht für eine dritte Person sowie zur berufsrechtlichen oder sonstigen Zulassung können sowohl in das Signaturschlüssel-Zertifikat als auch in ein Attribut-Zertifikat aufgenommen werden.

(3) Weitere Angaben darf das Signaturschlüssel-Zertifikat nur mit Einwilligung der Betroffenen enthalten.

§ 8 Sperrung von Zertifikaten

(1) Die Zertifizierungsstelle hat ein Zertifikat zu sperren, wenn ein Signaturschlüssel-Inhaber oder sein Vertreter es verlangen, das Zertifikat auf Grund falscher Angaben zu § 7 erwirkt wurde, sie ihre Tätigkeit beendet haben und diese nicht von einer anderen Zertifizierungsstelle fortgeführt wird oder die zuständige Behörde gemäß § 13 Abs. 5 Satz 2 eine Sperrung anordnet. Die Sperrung muß den Zeitpunkt enthalten, von dem an sie gilt. Eine rückwirkende Sperrung ist unzulässig.
(2) Enthält ein Zertifikat Angaben einer dritten Person, so kann auch diese eine Sperrung dieses Zertifikates verlangen.
(3) Die zuständige Behörde sperrt von ihr nach § 4 Abs. 5 ausgestellte Zertifikate, wenn eine Zertifizierungsstelle ihre Tätigkeit einstellt oder wenn die Genehmigung zurückgenommen oder widerrufen wird.

§ 9 Zeitstempel

Die Zertifizierungsstelle hat digitale Daten auf Verlangen mit einem Zeitstempel zu versehen. § 5 Abs. 5 Satz 1 und 2 gilt entsprechend.

§ 10 Dokumentation

Die Zertifizierungsstelle hat die Sicherheitsmaßnahmen zur Einhaltung dieses Gesetzes und der Rechtsverordnung nach § 16 sowie die ausgestellten Zertifikate so zu dokumentieren, daß die Daten und ihre Unverfälschtheit jederzeit nachprüfbar sind.

§ 11 Einstellung der Tätigkeit

(1) Die Zertifizierungsstelle hat, wenn sie ihre Tätigkeit einstellt, dies zum frühestmöglichen Zeitpunkt der zuständigen Behörde anzuzeigen und dafür zu sorgen, daß die bei Einstellung der Tätigkeit gültigen Zertifikate von einer anderen Zertifizierungsstelle übernommen werden, oder diese zu sperren.
(2) Sie hat die Dokumentation nach § 10 an die Zertifizierungsstelle, welche die Zertifikate übernimmt, oder andernfalls an die zuständige Behörde zu übergeben.
(3) Sie hat einen Antrag auf Eröffnung eines Konkurs- oder Vergleichsverfahrens der zuständigen Behörde unverzüglich anzuzeigen.

§ 12 Datenschutz

(1) Die Zertifizierungsstelle darf personenbezogene Daten nur unmittelbar beim Betroffenen selbst und nur insoweit erheben, als dies für Zwecke eines Zertifikates erforderlich ist. Eine Datenerhebung bei Dritten ist nur mit Einwilligung des Betroffenen zulässig. Für andere als die in Satz 1 genannten Zwecke dürfen die Daten nur verwendet werden, wenn dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Betroffene eingewilligt hat.

(2) Bei einem Signaturschlüssel-Inhaber mit Pseudonym hat die Zertifizierungsstelle die Daten über dessen Identität auf Ersuchen an die zuständigen Stellen zu übermitteln, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes oder des Zollkriminalamtes erforderlich ist. Die Auskünfte sind zu dokumentieren. Die ersuchende Behörde hat den Signaturschlüssel-Inhaber über die Aufdeckung des Pseudonyms zu unterrichten, sobald dadurch die Wahrnehmung der gesetzlichen Aufgaben nicht mehr beeinträchtigt wird oder wenn das Interesse des Signaturschlüssel-Inhabers an der Unterrichtung überwiegt.

(3) § 38 des Bundesdatenschutzgesetzes findet mit der Maßgabe Anwendung, daß die Überprüfung auch vorgenommen werden darf, wenn Anhaltspunkte für eine Verletzung von Datenschutzvorschriften nicht vorliegen.

§ 13 Kontrolle und Durchsetzung von Verpflichtungen

(1) Die zuständige Behörde kann gegenüber Zertifizierungsstellen Maßnahmen zur Sicherstellung der Einhaltung dieses Gesetzes und der Rechtsverordnung treffen. Dazu kann sie insbesondere die Benutzung ungeeigneter technischer Komponenten untersagen und den Betrieb der Zertifizierungsstelle vorübergehend ganz oder teilweise untersagen. Personen, die den Anschein erwecken, über eine Genehmigung nach § 4 zu verfügen, ohne daß dies der Fall ist, kann die Tätigkeit der Zertifizierung untersagt werden.

(2) Zum Zwecke der Überwachung nach Absatz 1 Satz 1 haben Zertifizierungsstellen der zuständigen Behörde das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten, auf Verlangen die in Betracht kommenden Bücher, Aufzeichnungen, Belege, Schriftstücke und sonstigen Unterlagen zur Einsicht vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren. Der zur Erteilung einer Auskunft Verpflichtete kann die Auskunft auf

solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Absatz 1 Nr. 1 bis 3 der Zivilprozeßordnung bezeichneten Angehörigen der Gefahr der Verfolgung wegen einer Straftat oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Der zur Auskunft Verpflichtete ist auf dieses Recht hinzuweisen.

(3) Bei Nichterfüllung der Pflichten aus diesem Gesetz oder der Rechtsverordnung oder bei Entstehen eines Versagungsgrundes für eine Genehmigung hat die zuständige Behörde die erteilte Genehmigung zu widerrufen, wenn Maßnahmen nach Absatz 1 Satz 2 keinen Erfolg versprechen.

(4) Im Falle der Rücknahme oder des Widerrufs einer Genehmigung oder der Einstellung der Tätigkeit einer Zertifizierungsstelle hat die zuständige Behörde eine Übernahme der Tätigkeit durch eine andere Zertifizierungsstelle oder die Abwicklung der Verträge mit den Signaturschlüssel-Inhabern sicherzustellen. Dies gilt auch bei Antrag auf Eröffnung eines Konkurs- oder Vergleichsverfahrens, wenn die genehmigte Tätigkeit nicht fortgesetzt wird.

(5) Die Gültigkeit der von einer Zertifizierungsstelle ausgestellten Zertifikate bleibt von der Rücknahme oder vom Widerruf einer Genehmigung unberührt. Die zuständige Behörde kann eine Sperrung von Zertifikaten anordnen, wenn Tatsachen die Annahme rechtfertigen, daß Zertifikate gefälscht oder nicht hinreichend fälschungssicher sind oder daß zur Anwendung der Signaturschlüssel eingesetzte technische Komponenten Sicherheitsmängel aufweisen, die eine unbemerkte Fälschung digitaler Signaturen oder eine unbemerkte Verfälschung signierter Daten zulassen.

§ 14 Technische Komponenten

(1) Für die Erzeugung und Speicherung von Signaturschlüsseln sowie die Erzeugung und Prüfung digitaler Signaturen sind technische Komponenten mit Sicherheitsvorkehrungen erforderlich, die Fälschungen digitaler Signaturen und Verfälschungen signierter Daten zuverlässig erkennbar machen und gegen unberechtigte Nutzung privater Signaturschlüssel schützen.

(2) Für die Darstellung zu signierender Daten sind technische Komponenten mit Sicherheitsvorkehrungen erforderlich, die die Erzeugung einer digitalen Signatur vorher eindeutig anzeigen und feststellen lassen, auf welche Daten sich die digitale Signatur bezieht. Für die Überprüfung signierter Daten sind technische Komponenten mit Sicherheitsvorkehrungen erforderlich, die feststellen lassen, ob die signierten

Daten unverändert sind, auf welche Daten sich die digitale Signatur bezieht und welchem Signaturschlüssel-Inhaber die digitale Signatur zuzuordnen ist.

(3) Bei technischen Komponenten, mit denen Signaturschlüssel-Zertifikate gemäß § 5 Abs. 1 Satz 2 nachprüfbar oder abrufbar gehalten werden, sind Vorkehrungen erforderlich, um die Zertifikatverzeichnisse vor unbefugter Veränderung und unbefugtem Abruf zu schützen.

(4) Bei technischen Komponenten nach den Absätzen 1 bis 3 ist es erforderlich, daß sie nach dem Stand der Technik hinreichend geprüft sind und die Erfüllung der Anforderungen durch eine von der zuständigen Behörde anerkannten Stelle bestätigt ist.

(5) Bei technischen Komponenten, die nach den in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum geltenden Regelungen oder Anforderungen rechtmäßig hergestellt oder in den Verkehr gebracht werden und die gleiche Sicherheit gewährleisten, ist davon auszugehen, daß die die sicherheitstechnische Beschaffenheit betreffenden Anforderungen nach den Absätzen 1 bis 3 erfüllt sind. In begründeten Einzelfällen ist auf Verlangen der zuständigen Behörde nachzuweisen, daß die Anforderungen nach Satz 1 erfüllt sind. Soweit zum Nachweis der die sicherheitstechnische Beschaffenheit betreffenden Anforderungen im Sinne der Absätze 1 bis 3 die Vorlage einer Bestätigung einer von der zuständigen Behörde anerkannten Stelle vorgesehen ist, werden auch Bestätigungen von in anderen Mitgliedstaaten der Europäischen Union oder in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum zugelassenen Stellen berücksichtigt, wenn die den Prüfberichten dieser Stellen zugrundeliegenden technischen Anforderungen, Prüfungen und Prüfverfahren denen der durch die zuständige Behörde anerkannten Stellen gleichwertig sind.

§ 15 Ausländische Zertifikate

(1) Digitale Signaturen, die mit einem öffentlichen Signaturschlüssel überprüft werden können, für den ein ausländisches Zertifikat aus einem anderen Mitgliedstaat der Europäischen Union oder aus einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum vorliegt, sind, soweit sie gleichwertige Sicherheit aufweisen, digitalen Signaturen nach diesem Gesetz gleichgestellt.

(2) Absatz 1 gilt auch für andere Staaten, soweit entsprechende überstaatliche oder zwischenstaatliche Vereinbarungen getroffen sind.

§ 16 Rechtsverordnung

Die Bundesregierung wird ermächtigt, durch Rechtsverordnung die zur Durchführung der §§ 3 bis 15 erforderlichen Rechtsvorschriften zu erlassen über

1. die näheren Einzelheiten des Verfahrens der Erteilung, Rücknahme und des Widerrufs einer Genehmigung sowie des Verfahrens bei Einstellung des Betriebs einer Zertifizierungsstelle,
2. die gebührenpflichtigen Tatbestände nach § 4 Abs. 6 und die Höhe der Gebühr,
3. die nähere Ausgestaltung der Pflichten der Zertifizierungsstellen,
4. die Gültigkeitsdauer von Signaturschlüssel-Zertifikaten,
5. die nähere Ausgestaltung der Kontrolle der Zertifizierungsstellen,
6. die näheren Anforderungen an die technischen Komponenten sowie die Prüfung technischer Komponenten und die Bestätigung, daß die Anforderungen erfüllt sind,
7. den Zeitraum sowie das Verfahren, nach dem eine neue digitale Signatur angebracht werden sollte.

7.2 Anschriften der Datenschutzbeauftragten des Bundes und der Länder und der Aufsichtsbehörden der Länder

7.2.1 Anschriften der Aufsichtsbehörden für den öffentlichen Bereich

Land	Postanschrift	Tel., Fax, E-Mail, WWW
Bund	Der Bundesbeauftragte für den Datenschutz Postfach 20 01 12 53131 Bonn	Tel.: 0228/81995-0 Fax: 0228/81995-50 E-Mail:poststelle@bfd.bund400.de X.400: C=de;A=bund400;P=bfd;S=poststelle Internet: http://www.bfd.bund.de
Baden-Württemberg	Der Landesbeauftragte für den Datenschutz Postfach 10 29 32 70025 Stuttgart	Tel.: 0711/615541-0 Fax: 0711/615541-15 E-Mail: LfD-BaWue@T-Online.de X.400: C=de; A=dbp; P=bwl; O=lfd; S=poststelle Internet: http://www.baden-wuerttemberg.datenschutz.de
Bayern	Der Bayerische Landesbeauftragte für den	Tel.: 089/212672-0 Fax: 089/212672-50

	Datenschutz Postfach 22 12 19 80502 München	E-Mail: poststelle@datenschutz-bayern.de X.400: C=de; A=d400-gw; DDA.Type=RFC-822; DDA.VALUE=poststelle(a)datenschutz-bayern.de Internet: http://www.datenschutz-bayern.de
Berlin	Berliner Datenschutzbeauftragter Pallasstr. 25/26 10781 Berlin	Tel.: 030/78768844 Fax: 030/216 99 27 E-Mail: mailbox@datenschutz-berlin.de X.400: C=de; A=d400-gw; DDA.Type=RFC-822; DDA.VALUE=dsb(a)datenschutz-berlin.de Internet: http://www.datenschutz-berlin.de
Brandenburg	Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Stahnsdorfer Damm 77 14532 Kleinmachnow	Tel.: 033203/356-0 Fax: 033203/356-49 E-Mail: Poststelle@LDA.Brandenburg.de X.400: C=de; A=d400-gw; P=brandenburg; O=LDA; S=Poststelle Internet: http://www.lda.brandenburg.de
Bremen	Landesbeauftragter für den Datenschutz der Freien Hansestadt Bremen Postfach 10 03 80 27503 Bremerhaven	Tel.: 0471/924610 Fax: 0471/92 46 12 8 E-Mail: office@datenschutz.bremen.de X.400: C=de; A=d400-gw; P=bremen; O=datenschutz; S=office
Hamburg	Der Hamburgische Datenschutzbeauftragte Baumwall 7 20459 Hamburg	Tel.: 040/3504-2044 (ab Juli 1999: 040/42841-2044) Fax: 040/3504-2372 E-Mail: Mailbox@datenschutz.hamburg.de X.400: C=de; A=d400-gw; P=hamburg; O=datenschutz; S=Mailbox Internet: http://www.hamburg.de/Behoerden/HmbDSB
Hessen	Der Hessische Datenschutzbeauftragte Postfach 31 63 65021 Wiesbaden	Tel.: 0611/1408-0 Fax: 0611/378579 E-Mail: DSB-Hessen@t-online.de X.400: C=de; A= d400-gw; P=t-online; S=dsb-hessen Internet: http://www.hessen.de/hdsb
Mecklenburg- Vorpommern	Landesbeauftragter für den Datenschutz Schloß Schwerin Lennéstr. 1 19053 Schwerin	Tel.: 0385/59494-0 Fax: 0385/59494-58 E-Mail: Datenschutz@mvnet.de X.400: C=de; A=d400-gw; P=mvnet; S=Datenschutz Internet: http://www.lfd.m-v.de
Niedersachsen	Der Landesbeauftragte für den	Tel.: 0511/120 4552

	Datenschutz Niedersachsen Postfach 2 21 30002 Hannover	Fax: -4591 E-Mai: poststelle@lfd.niedersachsen.de X.400: C=de; A=d400-gw; P=niedersachsen; O=lfd; S=poststelle Internet: http://www.lfd.niedersachsen.de
Nordrhein-Westfalen	Die Landesbeauftragte für den Datenschutz Postfach 20 04 44 40102 Düsseldorf	Tel.: 0211/38424-0 Fax: 0211/38424-10 E-Mail: datenschutz@mail.lfd.nrw.de X.400: C=de; A=d400-gw; P=nrw; O=lfd; OU=mail; S=datenschutz Internet: http://www.nordrhein-westfalen.datenschutz.de www.lfd.nrw.de
Rheinland-Pfalz	Der Landesbeauftragte für den Datenschutz Deutschhausplatz 12 55116 Mainz	Tel.: 06131/208-2449 Fax: 06131/208-2497 E-Mail: poststelle@datenschutz.rlp.de X.400: C=de; A=d400-gw; P=rlp; O=datenschutz; S=poststelle Internet: http://www.datenschutz.rlp.de
Saarland	Der Landesbeauftragte für den Datenschutz Postfach 10 26 31 66026 Saarbrücken	Tel.: 0681/503-415 Fax: 0681/49 86 29 E-Mail: lfd-saar@t-online.de X.400: C=de; A= d400-gw; P=t-online; S=lfd-saar Internet: http://www.lfd.saarland.de
Sachsen	Der Sächsische Datenschutzbeauftragte Postfach 12 09 05 01008 Dresden	
Sachsen-Anhalt	Der Landesbeauftragte für den Datenschutz Postfach 19 47 39009 Magdeburg	Tel.: 0391/81803-0 Fax: 0391/8180333 E-Mail: poststelle@lfd.lsa-net.de X.400: C=de; A= dbp; P= lsa-net; O=lfd; S=poststelle
Schleswig-Holstein	Landesbeauftragter für den Datenschutz bei der Präsidentin des Schleswig-Holsteinischen Landtages Postfach 36 07	Tel.: 0431/9881200 Fax: 0431/9881223 E-Mail: ldsh@netzservice.de X.400: C=de; A= d400-gw; P=netzservice; S=ldsh Internet: http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH

	24100 Kiel	
Thüringen	Der Thüringer Landesbeauftragte für den Datenschutz Am Hügel 10 a 99084 Erfurt	Tel.: 0361/59026-0 Fax: 0361/59026-20 E-Mail: poststelle@datenschutz.thueringen.de X.400: C=DE; A=DBP; P=THL;O=TLFD; S=poststelle Internet: http://www.thueringen.de/datenschutz

7.2.2 Anschriften der Aufsichtsbehörden für den nicht-öffentlichen Bereich

Land	oberste Aufsichtsbehörde	regional zuständige Aufsichtsbehörden
Baden-Würtemberg	Innenministerium Baden-Württemberg Dorotheenstraße 6 70173 Stuttgart Postfach 10 24 43 70020 Stuttgart Tel.: 0711/23132-50	Innenministerium Baden-Württemberg Dorotheenstraße 6 70173 Stuttgart Postfach 10 24 43 70020 Stuttgart Tel.: 0711/23123-50
Bayern	Bayerisches Staatsministerium des Innern Odeonsplatz 3 80524 München Tel.: 089/21922585	Regierung von Oberbayern Maximilianstraße 39 80534 München Tel.: 089/21760
		Regierung von Niederbayern Regierungsplatz 540 84023 Landshut Tel.: 0871/80801
		Regierung der Oberpfalz Emmeramsplatz 8 93047 Regensburg Tel.: 0941-56800
		Regierung von Oberfranken Ludwigstraße 20 59444 Bayreuth Tel.: 0921/6040
		Regierung von Mittelfranken Postfach 6 06 91511 Ansbach Tel.: 0981/530
		Regierung von Unterfranken

		Peterplatz 9 97070 Würzburg Tel.: 0931/3800
		Regierung von Schwaben Fronhof 10 86145 Augsburg Tel.: 0821/32701
Berlin	Berliner Datenschutzbeauftragter Pallasstraße 25/26 10781 Berlin Tel.: 030/78768844	Berliner Datenschutzbeauftragter Pallasstraße 25/26 10781 Berlin Tel.: 030/78768844
Brandenburg	Innenministerium des Landes Brandenburg Henning-von-Treskow-Str. 9-13 14467 Potsdam Tel.: 0331/866-0	Innenministerium des Landes Brandenburg Henning-von-Treskow-Str. 9-13 14467 Potsdam Tel.: 0331/866-0
Bremen	Landesbeauftragter für den Datenschutz Arndtstraße 1 27570 Bremerhaven Postfach 10 03 80 27503 Bremen Tel.: 0471/924610	Landesbeauftragter für den Datenschutz Arndtstraße 1 27570 Bremerhaven Postfach 10 03 80 27503 Bremen Tel.: 0471/924610
Hamburg	Der Hamburgische Datenschutzbeauftragte Baumwall 7 20459 Hamburg Tel.: 040/3504-2044	Der Hamburgische Datenschutzbeauftragte Baumwall 7 20459 Hamburg Tel.: 040/3504-2044
Hessen	Hessisches Ministerium des Innern und für Europaangelegenheiten Friedrich-Ebert-Allee 12 65185 Wiesbaden Tel.: 0611-3530	Regierungspräsidium Darmstadt Luisenplatz 2 64283 Darmstadt Tel.: 06151/120
		Regierungspräsidium Kassel Steinweg 6 34117 Kassel Tel.: 0561/1060
		Regierungspräsident Gießen Landgraf-Philipp-Platz 3

		35390 Gießen Tel.: 0641-3030
Mecklenburg-Vorpommern	Innenministerium des Landes Mecklenburg-Vorpommern 19048 Schwerin Tel.: 0385/588-0	Innenministerium des Landes Mecklenburg-Vorpommern 19048 Schwerin Tel.: 0385/588-0
Niedersachsen	Niedersächsisches Ministerium des Innern Lavesallee 6 30169 Hannover Tel.: 0511/120-1	Der Landesbeauftragte für den Datenschutz Niedersachsen Brühlstraße 9 30169 Hannover Tel.: 0511/120-4552
Nordrhein-Westfalen	Innenministerium des Landes Nordrhein-Westfalen Haroldstraße 5 40213 Düsseldorf Tel.: 0221/87101	Bezirksregierung Arnsberg Seibertzstraße 1 59821 Arnsberg Tel.: 02931/820
		Bezirksregierung Köln Zeughausstraße 2-10 50667 Köln Tel.: 0221/1470
Rheinland-Pfalz	Ministerium des Innern und für Sport Schillerplatz 3 - 5 55116 Mainz Tel.: 06131/160	Bezirksregierung Koblenz Stresemannstraße 3 - 5 56068 Koblenz Tel.: 0261/1200
		Bezirksregierung Rheinhessen-Pfalz Friedrich-Ebert-Straße 14 67433 Neustadt/Weinstraße Tel.: 06321/990
		Bezirksregierung Trier Willy-Brandt-Platz 3 54290 Trier Tel.: 0651/94940
Saarland	Ministerium des Innern Franz-Josef-Röder-Straße 21 66119 Saarbrücken Postfach 10 26 31 66026 Saarbrücken Tel.: 0681/501-00	Ministerium des Innern Franz-Josef-Röder-Straße 21 66119 Saarbrücken Postfach 10 26 31 66026 Saarbrücken Tel.: 0681/501-00
Sachsen	Sächsisches Staatsministerium	Regierungspräsidium Chemnitz

	des Innern 01095 Dresden Archivstraße 1 01097 Dresden Tel.: 0351/564-0 Fax: 0351-564-3209	09105 Chemnitz Altchemnitzer Straße 41 09120 Chemnitz Tel.: 0371/532-0
		Regierungspräsidium Dresden Postfach 10 06 53 01076 Dresden Stauffenbergallee 2 01099 Dresden Tel.: 0351/825-0
		Regierungspräsidium Leipzig Postfach 1529 04257 Leipzig Brausstraße 2 04107 Leipzig Tel.: 0341/3990
Sachsen-Anhalt	Innenministerium des Innern des Landes Sachsen-Anhalt Halberstädter Straße 2 39114 Magdeburg Tel.: 0391/567-01	Regierungspräsidium Dessau Wolfgangstraße 25 06844 Dessau Tel.: 0340/65060
		Regierungspräsidium Halle Willy-Lohmann-Straße 7 06114 Halle Tel.: 0345/5140
		Regierungspräsidium Magdeburg Olvenstedter Straße 1 - 2 39108 Magdeburg Tel.: 0391/56702
Schleswig-Holstein	Innenministerium des Landes Schleswig-Holstein Düsternbrooker Weg 92 Landeshaus 24105 Kiel Tel.: 0431/988-0	Innenministerium des Landes Schleswig-Holstein Düsternbrooker Weg 92 Landeshaus 24105 Kiel Tel.: 0431/988-0
Thüringen	Innenministerium des Landes Thüringen Steigerstr. 24	Thüringer Landesverwaltungsamt Carl-August-Allee 2a 99423 Weimar

	99096 Erfurt Tel.: 0361/37900	Postfach 2 49 99403 Weimar Tel.: 03643/585

7.3 Zugriff auf Patientendaten im Krankenhaus

(Erarbeitet von der GMDS-Arbeitsgruppe, *Datenschutz in Gesundheitsinformationssystemen*, Stand 21.4.1999)

Ziel dieser Empfehlung ist eine Hilfestellung bei der Organisation der datenschutzkonformen Handhabung von elektronisch gespeicherten Patientendaten im Krankenhaus und bei der Erstellung eines Datenschutzkonzeptes. Insbesondere sollen Hinweise für die Umsetzung des Grundprinzips der sparsamen Datenerhebung und -verarbeitung gegeben und die Definition eines Regelwerks für Zugriffsrechte und Datenfreigabe erleichtert werden. Abweichungen von diesen Empfehlungen können aufgrund unterschiedlicher gesetzlicher Regelungen in den einzelnen Bundesländern notwendig sein. Abweichungen können auch je nach den lokalen Organisationsstrukturen sinnvoll sein. Sie erfordern dann aber eine Begründung, in der dem Patienten sonst drohender Schaden sowie durch die Abweichung entstehender Nutzen für den Patienten dargelegt sind, und müssen die konstituierenden Elemente des Datenschutzes im Krankenhaus, die ärztliche Schweigepflicht und das informationelle Selbstbestimmungsrecht des Patienten, wahren. Soweit einige der folgenden Empfehlungen in einem bestehenden System nicht unmittelbar umgesetzt werden können, sollte die entsprechende Anforderung an den Hersteller weitergegeben werden.

Papierakten und Registraturen müssen ebenfalls datenschutzkonform gehandhabt werden; die folgenden Empfehlungen beziehen sich jedoch nur auf elektronisch gespeicherte Patientendaten, weil hier, vor allem durch die rasante technische Entwicklung, ein erheblicher Regelungsbedarf besteht.

7.3.1 Grundsätze

Durch die Einführung von Informationstechnik im Krankenhaus mit dem dadurch ermöglichten einfachen, schnellen und multiplen Zugriff auf Patientendaten ergeben sich Datenschutzprobleme, die durch organisatorische Regelungen und Sicherheitstechnik gelöst werden müssen. Bisher beim Umgang mit der papierenen Patientenakte übliche Einsichtnahme- und Weitergabeverfahren können nicht ohne

weiteres auf das rechnergestützte Krankenhausinformationssystem und die elektronische Patientenakte übertragen werden.

Aus dem Datenschutzrecht (siehe die Grundsatzerklärung der AG sowie die Stellungnahme für das Krankenhaus-Management) ergeben sich für die Zugriffsrechte auf Patientendaten im Krankenhaus die folgenden Grundsätze: Patientendaten dürfen nur im Rahmen der Zweckbestimmung des Behandlungsvertrages und den damit verbundenen gesetzlichen Regelungen erhoben und verarbeitet, nicht aber uneingeschränkt - d. h. über die unmittelbare Zweckbindung hinaus - ausgetauscht und verwendet werden, auch nicht innerhalb des Krankenhauses; das Krankenhaus ist in diesem Sinne keine informationelle Einheit. Das Prinzip der Erforderlichkeit ist hier streng zu beachten, das auch als Prinzip der minimalen Rechte oder »need-to-know«-Prinzip bezeichnet wird. Insbesondere ist hier zwischen dem Arzt und seinen berufsmäßig tätigen Gehilfen einerseits sowie den sonstigen Gehilfen andererseits zu unterscheiden. Das medizinische Fachpersonal als Produzent der Information trägt die Verantwortung für die korrekte Verwendung der Daten unter Berücksichtigung der Persönlichkeitsrechte der Beteiligten, insbesondere des Patienten, der Quelle (oder »Urheber«) der Information ist. Folglich kann nur der die Daten produzierende, das heißt, sie erhebende, Arzt bzw. der ärztliche Leiter der Fachabteilung die Rechte für den Zugriff auf die medizinischen Daten des Patienten und deren definierte Verwendung erteilen. Der Patient hat, sofern das zuständige Krankenhausgesetz wie etwa in Rheinland-Pfalz nichts anderes bestimmt, das Recht, Daten für bestimmte Zugriffe sperren zu lassen, wobei er auf eventuell für ihn entstehende Nachteile hinzuweisen ist; er hat andererseits auch ein Anrecht darauf, daß seine Daten zur rechten Zeit am rechten Ort verfügbar sind, insbesondere nicht gegen seinen Willen oder seine Interessen zurückgehalten oder außerhalb der gesetzlichen Pflichten vernichtet werden.

7.3.2 Daten und Patientenakten

Unter einer **Patientenakte** wird im folgenden die Gesamtheit der über diesen Patienten gespeicherten Informationen verstanden, die in Form einer abgeschlossenen Dokumentation, z. B. von einem Arzt, verantwortet sind. Diese können in einer einheitlichen zentralen Datenbank oder in einem verteilten Krankenhausinformationssystem gespeichert sein. Die Patientenakte erstreckt sich

über alle Behandlungszusammenhänge in diesem Krankenhaus. Wird der Patient (im Sinne des shared care) in mehreren Organisationseinheiten des Gesundheitswesens behandelt, führt jede solche Einheit eine eigene Patientenakte. Im Interesse des Patienten und unter Berücksichtigung seiner Einwilligung sind in diesem Fall analoge Datenweitergabe- und -zugriffsregelungen zu treffen, wie im folgenden für das Krankenhaus beschrieben.

Ein **Behandlungszusammenhang** beginnt mit der Aufnahme des Patienten und umfaßt Verlegungen, Mitbehandlung durch andere Fachabteilungen, Konsile und Leistungsanforderungen; er erstreckt sich auch über eventuellen Heimurlaub sowie über zusammengehörige ambulante Besuche. Er kann sich auch über Entlassung und Wiederaufnahme erstrecken, wenn diese der Fortsetzung einer bei einem früheren Aufenthalt begonnenen Behandlung dient.

Nicht zur Patientenakte gehören **abteilungsinterne Daten**, also in der behandelnden Fachabteilung über den Patienten angefallene nicht autorisierte Daten wie nicht befundete Röntgenbilder oder ähnliches; solche Daten sind aber selbstverständlich auch Patientendaten im Sinne der Datenschutzgesetzgebung und daher entsprechend zu schützen. Nicht zur Krankenakte gehören auch persönliche Arztnotizen. Es ist aber das Prinzip der ordnungsgemäßen Aktenführung zu beachten, d. h., es ist eine bearbeitungsgerechte, nachvollziehbare, auf sachlichen Prinzipien beruhende Struktur der abgespeicherten Daten anzustreben, um Behandlungsprozesse im Detail und im Kontext nachvollziehen zu können. Alles, was im Verlaufe der Behandlung an Daten erzeugt wird und derzeit relevant ist oder als künftig relevant erachtet wird, gehört in die Patientenakte.

Um die unterschiedlichen Zugriffsanforderungen und -befugnisse sowie Sensibilitätsstufen angemessen berücksichtigen zu können, sind folgende Arten von Daten zu unterscheiden, die alle dem Datenschutz und dem Arztgeheimnis unterliegen:

- **Identifikationsdaten** (Name, Geburtsdatum, Adresse, evtl. Krankenkassennummer, sowie krankenhausinterne Identifikatoren),
- **administrative Daten**:
- Versicherungsdaten,
- Bewegungsdaten,
- weitere fallbezogene Daten, z. B. Wahlleistungen,
- **medizinische Daten**:

- Notfalldaten,
- allgemeine anamnestischen Daten,
- abrechnungsrelevante Diagnosen und Therapien,
- Befunde, Laborwerte und andere diagnostische und therapeutische Daten,
- besonders sensible Daten (z. B. psychiatrische Daten, bestimmte Befunde),
- genetische Daten.

Die Identifikationsdaten und administrativen Personendaten einschließlich Versicherungsdaten werden oft auch als Stammdaten bezeichnet. Die medizinische Daten sind gemäß der EU-Richtlinie zum Datenschutz weiter zu untergliedern. Zu den Patientendaten gehören auch Daten, die sich auf Angehörige, Bezugspersonen oder Dritte beziehen; dies können sowohl administrative als auch medizinische Daten sein.

Notfalldaten werden in der Patientenakte so gespeichert, daß der Zugriff auf sie unabhängig vom restlichen Teil der Patientenakte möglich ist. Zu den Notfalldaten gehören Daten, die zur Abwehr einer Gefahr für Leben, körperliche Unversehrtheit oder persönliche Freiheit des Patienten für die mit der Untersuchung und Behandlung des Patienten befaßten Personen erforderlich sind (z. B. schwere Allergien). Sie sollen vollständig und unverzüglich in die Patientenakte eingetragen werden. Welche Daten als Notfalldaten gekennzeichnet werden, entscheidet der Arzt, bei dem sie produziert werden; Vorgaben dazu erläßt der Leiter der Fachabteilung (unter Berücksichtigung internationaler Festlegungen), ebenso wie Richtlinien, welche Daten als besonders sensibel einzustufen sind. Das Widerspruchsrecht des Patienten, sofern gegeben, bleibt unberührt.

Die Patientenakten prominenter Personen können auf deren Wunsch mit einer VIP-Kennzeichnung versehen werden und werden nur unter besonderen Einschränkungen freigegeben. Alternativ ist eine Speicherung unter einem Pseudonym möglich. Eine analoge Regelung ist für Kliniksmitarbeiter und deren Angehörige vorzusehen, wobei die Schutzmaßnahmen nach dem Prinzip der Verhältnismäßigkeit weniger streng sein können.

7.3.3 Zugriffsrechte

Daten werden in der Verantwortung der erhebenden Fachabteilung des Krankenhauses gespeichert und verarbeitet und sind vor dem Zugriff durch nicht autorisierte Mitarbeiter zu schützen. Die erhebende Stelle verantwortet die

Zugriffsrechte auf diese Daten; somit können Rechte an Dritte stets nur gegeben (logische Überweisung) und, außer in Notfallsituationen, nie selbständig durch sie genommen werden. Die Datenhoheit einer Fachabteilung über die bei ihr erhobenen Daten gilt unabhängig vom Ort der Speicherung, auch, wenn diese in einer zentralen Datenbank erfolgt. Das Recht zur Einsicht und Verarbeitung der Patientendaten ist grundsätzlich an den Behandlungszusammenhang gebunden. Das Erscheinen des Patienten in einer anderen Fachabteilung ist, sofern ein Behandlungszusammenhang besteht, in der Regel als Zustimmung zum Zugriff auf die nötigen Daten der überweisenden Abteilung zu werten; aufgrund der informationellen Selbstbestimmung des Patienten kann höchstens dieser, nicht die überweisende Stelle die Freigabe verweigern. Pauschalisierte Sonderregelungen aufgrund struktureller Einheiten, funktioneller Gemeinsamkeiten und besonderer Kooperationsbedingungen zwischen Fachabteilungen bedürfen einer sorgfältigen Begründung; Beispiele dafür folgen.

Der zugriffsberechtigte Personenkreis sowie dessen Rechte sind stets nach dem Grundsatz der Erforderlichkeit zu minimieren. Auch die Krankenhausverwaltung darf nur zu den Daten Zugang haben, die für ihre Zwecke erforderlich sind. Eine zentrale Referenzdatenbank, sofern ihr Umfang über eine reine Verweisdatei hinausgeht, ist, ebenso wie ein Archiv, kein Selbstbedienungsladen; auch hier gilt die Datenhoheit der Fachabteilungen.

Zugriffsrechte werden in Form eines kliniksweiten sowie eines abteilungsspezifischen Regelwerkes festgelegt, das mit dem Datenschutzbeauftragten abzustimmen ist. Bei Bedarf wird für den einzelnen Patienten eine Rechteliste in der Patientenakte mitgeführt, z. B. wenn er von seinem Widerspruchsrecht Gebrauch gemacht hat. Die Rechte werden je nach Anwendungsfall vergeben an

- Fachabteilungen,
- Rolleninhaber,
- Einzelpersonen,

wobei hierarchisch geordnete rollenbasierte Zugriffsrechte im Krankenhausbetrieb meistens angemessen sind. Den unterschiedlichen Aufgaben und Zielen entsprechend ist der Zugriff selektiv nach der Art der Daten und der Art des Zugriffs zu gewährleisten. Die Definition der Rollen und der ihnen zugeordneten Zugriffsrechte soll durch durch den Kliniksvorstand vorgenommen und durch eine zentrale verfahrensbetreuende Stelle umgesetzt werden; die Zuweisung von Rollen

zu bestimmten Personen erfolgt durch die Fachabteilung. Soweit lediglich abteilungsinterne Zugriffsmöglichkeiten betroffen sind, können eigene Rollen auch durch die Fachabteilung definiert werden.

Innerhalb des Behandlungszeitraums haben behandelnde Ärzte Zugriff auf den ganzen zum Behandlungszusammenhang gehörigen Teil der Patientenakte, soweit nicht besonders sensible Daten von anderen Fachabteilungen gesperrt sind, sowie auf die zu früheren Behandlungszusammenhängen in der gleichen Fachabteilung angefallenen Daten des Patienten. Dies gilt auch für Ärzte im Praktikum und Studenten im praktischen Jahr sowie für Ärzte, die der Fachabteilung zeitweise, z. B. im Rahmen von Nachtdienst, zugeordnet sind; deren Berechtigung ist auf die Zeit dieses Dienstes zu beschränken. Nach der Entlassung ist der Zugriff noch für einen angemessenen Zeitraum zulässig (z. B. für Arztbriefschreibung) - diese zeitliche Befristung ist allerdings nicht in allen einschlägigen Landesgesetzen vorgesehen.

Außerhalb des Behandlungszusammenhangs dürfen die Daten eines Patienten auch dem medizinischen Personal innerhalb der Abteilung nicht zur Verfügung stehen (nicht in allen Bundesländern zwingend), außer für definierte Forschungsprojekte oder Auswertungen im Rahmen der Qualitätssicherung; hierfür sind die Datenschutzregelungen für Forschungsvorhaben zu beachten, die insbesondere im Regelfall Anonymisierung oder Pseudonymisierung verlangen. Einem behandelnden Arzt sollen auch Rückgriffe auf Musterfälle seiner eigenen Behandlungstätigkeit möglich sein.

In der Fachabteilung tätige Pflegekräfte haben während des Aufenthalts des Patienten auf ihrer Station Zugriff auf die Krankenakte in einem Umfang, den der Leiter der Abteilung nach den Anforderungen der Arbeitsorganisation festlegt; auch hierbei ist der Grundsatz der Erforderlichkeit zu befolgen. Das gleiche gilt auch für sonstige Mitarbeiter der Fachabteilung. Für Famulanten, Studenten und Auszubildende legt der verantwortliche Lehrende im Rahmen seiner eigenen Befugnisse die Zugriffsberechtigung fest.

Der Nachweis eines Behandlungszusammenhangs wird in der Regel durch den Bewegungseintrag im Krankenhausinformationssystem erbracht. Oft erscheint der Patient aber schon in der neuen Abteilung, bevor wegen der Heterogenität des Krankenhausinformationssystems der Bewegungseintrag zur Verfügung steht. Für diesen Fall soll ein vorgezogener Zugriff möglich sein; unverzichtbare Grundlagen dafür sind

- die Zustimmung durch den Patienten (konkludent durch sein Erscheinen angenommen),
- die Freischaltung des Datenzugriffs durch die überweisende Abteilung (die in deren Abteilungssystem eventuell schon in Kraft ist oder in bestimmten Situationen, z. B. Röntgen, generell gewährt wird),
- die Nachvollziehbarkeit durch die Protokollierung.

Der Zugriff sollte sich auf administrative Daten und Überweisungsdiagnose beschränken. Wenn die Berechtigung nicht innerhalb einer angemessenen Frist nachgereicht wird, ist eine automatische Warnung an den für die Daten Verantwortlichen zu versenden. (*Anmerkung*: Dieser Fall ist in der gegenwärtigen Situation, wo die Krankenhauskommunikation an vielen Stellen noch unzulänglich funktioniert, häufig. Mit verbessertem Ausbau der Krankenhausinformationssysteme sollte er selten oder gar nicht mehr vorkommen.)

Zugriffe auf die Patientenakte sollten protokolliert werden mit Angabe von Person, Rolle, Fachabteilung, sowie Art, Zeitpunkt und Umfang des Zugriffs. Die Granularität dieser Protokollierung ist nach dem Grundsatz der Verhältnismäßigkeit unter dem Gesichtspunkt der Praktikabilität auszubalancieren; ordnungsgemäße, den Richtlinien entsprechende Zugriffe durch das behandelnde Personal der Fachabteilung brauchen nicht im Protokoll zu erscheinen; eine stichprobenartige Protokollierung hiervon erscheint aber sinnvoll. Das Zugriffsprotokoll wird als Teil der Patientenakte behandelt, egal wo es physisch gespeichert ist, und ist nur für den verantwortlichen Arzt, den Patienten selbst und für den Datenschutzbeauftragten jederzeit einsehbar; diese haben auch das Recht, eine nachträgliche Rechtfertigung für den Zugriff zu verlangen. Die Folgen bei entdecktem Mißbrauch sind durch eine Dienstvereinbarung unter Berücksichtigung des Datenschutzrechts und des Strafgesetzbuchs zu regeln. Protokolleinträge sollen für eine angemessene Zeit aufbewahrt werden; mit Rücksicht auf das Auskunftsrecht des Patienten erscheinen 2 Jahre angemessen.

In Notfällen (z. B. Nacht- oder Wochenendaufnahme) ist im Interesse des Patienten - auch gemäß der EU-Richtlinie - ein schneller, unkomplizierter Zugriff auf die Daten zu gewährleisten. Hier ist in der Regel der Zugriff auf die Notfalldaten sowie der Hinweis auf frühere Aufenthalte ausreichend. Dabei ist über die gewöhnliche Protokollierung hinaus eine sofortige gesonderte Benachrichtigung des für die Daten

Verantwortlichen und ein regelmäßiges Sonderaudit vorzusehen - in diesem Fall gehen die Datenschutzrechte des Patienten denen des Personals vor.
Die Notfalldaten eines Patienten sind ohne weitere explizite Freigabe von allen bei der Behandlung dieses Patienten beteiligten Fachabteilungen einsehbar. Die Existenz von Notfalldaten ist unübersehbar zu kennzeichnen, sie müssen besonders schnell abrufbar sein und übersichtlich zusammengefaßt präsentiert werden (»Cave-Fenster«). Auch hier ist die Protokollierung zur Entdeckung eines Mißbrauchs unverzichtbar.
Über Zugriffe auf die als besonders sensibel gekennzeichneten Daten entscheidet der Leiter der Fachabteilung, in der sie produziert wurden. Bei Zielkonflikten zwischen Notfalldaten und besonders sensiblen Daten - z. B. Diagnose AIDS - hat die Sensibilität der Daten Vorrang. Eine Einwilligung des Patienten reicht hier aber auch zur Freigabe.

7.3.4 Technische Absicherung der Zugriffsrechte und -einschränkungen

Patientendaten sind nach dem Stand der Technik zu schützen, wobei das Prinzip der Verhältnismäßigkeit zu beachten ist. Für medizinische Daten ist wegen ihrer Sensibilität ein entsprechend hoher Aufwand zur Realisierung der Sicherheit geboten. Durch technische und organisatorische Maßnahmen muß gewährleistet sein, daß genau die in der entsprechenden Rechteliste definierten Zugriffe auf eine Patientenakte stattfinden können. Die vom Sicherheitskonzept geforderten Beschränkungen müssen durch geeignete Implementation und durch Sicherheitstechnik garantiert werden. Natürlich dürfen auch die Möglichkeiten zum Datenzugriff unter Umgehung der Anwendungsprogramme nicht vergessen werden, z. B. mit Hilfe von direktem Plattenzugriff oder Netzmonitorprogrammen. Die Sicherheitsanforderungen sind daher nur durch kryptographische Techniken - verschlüsselte Speicherung und Übertragung, starke Authentisierung - zu erfüllen.
Verschlüsselte Übertragung soll die Daten zwischen Ursprungs- und Zielsystem vor der Einsicht durch Unberechtigte, auch durch IT-Personal, schützen. Verschlüsselt werden sollten die Nutzdaten der Übertragung, nicht die Verbindungsdaten, wie etwa Protokoll-Header. Der geeignetste Ansatz scheint die Verschlüsselung auf der Protokoll-Ebene zu sein, etwa die Verwendung von SSL beim Einsatz von Intranet-Techniken. Eine Minimalforderung, solange im Einzelfall geeignete kryptographische Techniken noch nicht zur Verfügung stehen, ist das Unterdrücken von

Identifizierungsdaten bei der Übermittlung; werden bei der Übertragung nur Patientennummern mitgeschickt, ist bereits eine wenigstens schwache Pseudonymisierung erreicht.

Um IT-Personal bei Systempflege und -wartung an sachlich nicht notwendigen Einblicken in Patientendaten zu hindern, wird eine Speicherung der identifizierenden Daten in einer getrennten Tabelle und die Verwendung von Pseudonymen für den Fall, daß die Zusammenführung unvermeidbar ist, empfohlen.

Server und Kommunikationsknoten sind als besondere Sicherheitsbereiche zu definieren und physisch zu schützen, in der Regel in verschlossenen Räumen.

Zum Nachweis der Benutzerberechtigung sollte entsprechend deutscher, europäischer und internationaler Rechtsgrundlagen eine Sicherheitsinfrastruktur nach dem Stand der Technik aufgebaut werden, die insbesondere starke Authentisierung und Rechteprüfung aufgrund von Zertifikaten beinhaltet. Hier sind zukünftig die Möglichkeiten der Health Professional Card (HPC) zu nutzen. Es soll ein fliegender Rollen- oder Benutzerwechsel möglich sein; dazu ist eine Speicherung der aktuellen Benutzungsoberfläche in einem sicheren Systembereich geeignet, so daß sie nur durch erneute Authentisierung wieder aktiviert werden kann. Auf analoge Weise ist ein Time-Out zu realisieren.

Die Benutzungsoberfläche ist so zu gestalten, daß die Sicht, die dem Benutzer gewährt wird, genau seinen Rechten entspricht; d. h., es sind nur die Daten sichtbar, für die Leserecht besteht, und nur die Datenfelder editierbar, für die Schreibrecht besteht. Die Existenz von Notfalldaten ist deutlich anzuzeigen. Die Bedienungselemente für Notfallzugriffe außerhalb bereits gewährter Rechte sind mit deutlichen Warnhinweisen auf die Konsequenzen zu versehen. Die Berechtigung dazu ist lokal unter dem Gesichtspunkt der Praktikabilität eindeutig zu regeln.

Noch nicht Stand der Technik, aber spätestens nach Einführung der Health Professional Card anzustreben, ist die konsequente Anwendung der digitalen Signatur, um die Verbindlichkeit (Zurechenbakeit, Unleugbarkeit) von Dokumentation und Maßnahmen zu sichern. Dazu gehört auch ein, vom Trustcenter anzubietender, sicherer Zeitstempeldienst.

7.3.5 Typische Beispielsituationen

Hier werden Empfehlungen für die Ausgestaltung der Zugriffsrechte in typischen Situationen des Krankenhausalltags gegeben.

Aufnahme

Die reguläre Aufnahme eines Patienten erfolgt durch einen dazu berechtigten Verwaltungsmitarbeiter. Bei der Aufnahme wird der Patient, in der Regel durch einen separaten Vordruck, auf seine Rechte bezüglich des Datenschutzes hingewiesen und darüber informiert, welche Daten von wem verarbeitet werden, und stimmt mit seiner Unterschrift der Speicherung und Verarbeitung seiner Daten zu. Er wird durch den aufnehmenden Verwaltungsmitarbeiter einer Fachabteilung zugewiesen. Dadurch werden die Zugriffsrechte für diese Fachabteilung freigegeben.

Handelt es sich um eine Wiederaufnahme, d. h. wurde der Patient schon einmal in diesem Krankenhaus behandelt, darf bei der Aufnahme auf bereits vorhandene Stammdaten zugegriffen werden. Bei Identifizierungsproblemen ist eine minimierte Auswahl an Fällen und identifizierenden Daten anzubieten, auf keinen Fall aber eine vollständige Patientenliste zur Auswahl. Die Anzeige eines anderen Patienten in einer solchen minimalen Auswahlliste braucht nicht als Zugriff auf dessen Daten protokolliert zu werden. Bei einer Wiederaufnahme ist, sofern das Landesrecht nichts anderes vorsieht, der Patient zu fragen, ob medizinische Daten aus früheren Aufenthalten in anderen Fachabteilungen herangezogen werden dürfen. Widerspricht der Patient, so ist für den behandelnden Arzt ein entsprechender Vermerk zu machen, ohne jedoch die betroffenen anderen Abteilungen zu nennen. Der Arzt hat so die Möglichkeit, später doch noch die Zustimmung des Patienten zu erhalten. Der aufnehmende Verwaltungsmitarbeiter darf in diese Daten keinen Einblick erhalten.

Die Häufigkeit des Zugriffs auf Auswahllisten durch bestimmte Benutzer ist zu protokollieren, ebenso wie unnötige Zugriffe, um Mißbrauch zu entdecken. Ein Mißbrauch liegt z. B. vor, wenn eine Aufnahme vorgetäuscht wird, um in frühere Patientendaten einer Person Einblick zu erhalten.

Kurzaufnahme

Eine Kurzaufnahme erfolgt außerhalb der normalen Dienststunden direkt in der Fachabteilung. Welche Personen, z. B. auch Pflegepersonal, zu einer Kurzaufnahme berechtigt sind, legt der Abteilungsleiter in Absprache mit der ansonsten für die Aufnahme zuständigen Verwaltungsstelle fest. Die Prüfung, ob der Patient bereits im Krankenhausinformationssystem vorhanden ist, erfolgt entsprechend zur regulären Aufnahme. Die Kurzaufnahme ist baldmöglichst vom dazu berechtigten Verwaltungspersonal in eine reguläre Aufnahme zu überführen. Nach Abschluß der Kurzaufnahme erhält die aufnehmende Abteilung den Zugriff auf die Notfalldaten des

Patienten sowie, wenn dies nicht ohnehin unbeschränkt möglich ist, auf eventuell schon vorhandene Daten in der eigenen Abteilung mit Fallbezug.

Notaufnahme

Eine Notaufnahme erfolgt, wenn aufgrund des Gesundheitszustandes des Patienten eine reguläre Aufnahme oder eine Kurzaufnahme nicht möglich ist. Ist der Patient nicht bei Bewußtsein, ist in seinem Interesse von der Einwilligung zum Datenzugriff im benötigten Umfang auszugehen; ist seine Identität nicht ermittelbar, wird er zunächst unter einem Pseudonym eingetragen.

Wiederaufnahme im gleichen Behandlungszusammenhang

Hier wird die unmittelbar vor der Entlassung gültige Datensicht wiederhergestellt.

Ambulante Aufnahme

Die ambulante Patientenaufnahme erfolgt in der Regel dezentral in den Polikliniken und in Leistungsbereichen wie der technischen Orthopädie oder der physikalischen Therapie. Es gelten analoge Empfehlungen wie für die Kurzaufnahme.

Erstkontakt mit dem Arzt

Im Interesse des Patienten ist es, schon aus haftungsrechtlichen Gründen, unerläßlich, daß eine neu aufnehmende Fachabteilung Lesezugriff auf die in der Patientenakte enthaltenen Informationen über frühere Kliniksaufenthalte auch in anderen Fachabteilungen hat; letztlich kann nur die neu behandelnde Fachabteilung beurteilen, welche medizinischen Daten sie für die Behandlung dieses Patienten braucht. Der verantwortliche Arzt muß daher vom Krankenhausinformationssystem über die Existenz früherer oder paralleler Behandlungszusammenhänge informiert werden, aber nicht über Art und Abteilung - dieses nur nach Zustimmung des Patienten. Notfalldaten müssen in jedem Fall sichtbar sein, auch wenn dadurch Rückschlüsse auf frühere Aufenthalte möglich sind.

Verlegung

Mit einer angeordneten Verlegung eines Patienten in eine andere Fachabteilung werden die im Behandlungszusammenhang benötigten Daten für die neue Abteilung freigegeben und sind dann dort unter Berücksichtigung der Rolle des Zugreifenden verfügbar, in der Regel nur mit Leseberechtigung. Der Patient ist bei der Besprechung seiner Weiterbehandlung auch über die vorgesehene Datenfreigabe und sein eventuelles Widerspruchsrecht zu informieren.

Hier sollte die im Routinefall übliche Freigabe im benötigten Datenumfang in den Verlegungsvorgang des Krankenhausinformationssystems eingebaut werden; in der Regel handelt es sich um die administrativen Daten sowie den in der Verantwortung der überweisenden Abteilung gespeicherten Teil der Patientenakte ohne die besonders sensiblen Daten. Das Speichern der Daten der alten Abteilung im System der neuen Abteilung würde sie der Datenhoheit der alten Abteilung entziehen und ist daher nicht zulässig, wenn auch technisch kaum zu verhindern.

Mitbehandlung und Konsil

Für die Mitbehandlung in einer anderen Fachabteilung ist die Datenfreigabe analog zur Verlegung zu regeln, zusätzlich ist umgekehrt die Freigabe der hier anfallenden Informationen für die hauptsächlich behandelnde Fachabteilung ohne weitere Umstände als Rückmeldung vorzusehen. Gleiches gilt für Konsiliardienste. Wie weit rückgemeldete Daten in die Hoheit der anfordernden Abteilung übergehen, ist im Einzelfall verbindlich zu regeln.

Ausnahmeregelungen, wo die Notwendigkeit zur expliziten Freigabe im Einzelfall als zu einschränkend erachtet wird, sind bei routinemäßiger abteilungsübergreifender Zusammenarbeit möglich, wenn sie im Einvernehmen mit dem Datenschutzbeauftragten vom Kliniksvorstand schriftlich genehmigt wurden. Beispiele hierfür können sein die Zusammenarbeit zwischen operativen Abteilungen und der Anästhesie oder zwischen der Geburtshilfe und der Kinderklinik. Auch hier ist aber das Widerspruchsrecht des Patienten, soweit vorhanden, in der Form zu berücksichtigen, daß gegebenenfalls die Daten gesperrt werden können.

Leistungsanforderung

Mit der Leistungsanforderung, z. B. von Laborleistungen oder bildgebenden Verfahren oder bei anderen Funktionsbereichen, werden die benötigten Daten freigegeben, sofern der Patient nicht widerspricht. Auch hier sollte der typische Datenumfang im Krankenhausinformationssystem implementiert sein; in der Regel ist das nur ein Teil der Patientenakte. Werden darüber hinaus weitere Daten benötigt, ist das Recht dazu von der datenspeichernden Abteilung explizit einzuholen. Werden als Rückmeldung Daten nicht nur freigegeben, sondern übermittelt, liegt die Datenhoheit für die übermittelten Daten dann beim Empfänger.

Abteilungssysteme mit Stammdaten

Fachabteilungen oder Funktionsbereiche, die mitbehandeln oder Leistungen erbringen, können die Stammdaten des betroffenen Patienten in ihrem eigenen Abteilungssystem speichern; dies erhöht die Ausfallsicherheit des Krankenhausinformationssystems und hilft, wenn die Krankenhauskommunikation zu langsam oder unzuverlässig funktioniert, wie es in der gegenwärtigen Praxis oft noch der Fall ist. Eine völlige Freigabe der Stammdaten aller Patienten, möglichst sogar Mitteilung der Neuaufnahmen per Broadcast, wird insbesondere vom Zentrallabor und der Radiologie oft gewünscht; da in diesen beiden Fällen fast alle Patienten im Laufe ihrer Behandlung dort sowieso erfaßt werden, ist eine Ausnahmeregelung wie unter »Mitbehandlung« sinnvoll. Diese sollte aber vorübergehenden Charakter haben, bis die Krankenhauskommunikation zuverlässig funktioniert, und verbietet sich bei Leistungsstellen, die nicht zum Krankenhaus gehören, z. B. bei Outsourcing.

Zentralküche

Es ist sinnvoll und unbedenklich, wenn jeder neu aufgenommene stationäre Patient mit Namen, Geburtsdatum, Station und gegebenenfalls Diätverordnung automatisch an die Zentralküche gemeldet wird. Auf Wunsch des Patienten sind hier auch Ernährungsbesonderheiten mitzuteilen - auf keinen Fall aber die Religionszugehörigkeit. Wird die Essensversorgung außer Haus gegeben, sind die Vorschriften für Datenverarbeitung im Auftrag zu beachten.

Pförtner- und Telefonliste

Mit Einverständnis des Patienten können Name und Station in die Pförtnerliste aufgenommen werden. Ebenfalls mit Einverständnis des Patienten kann die Telefonzentrale die Nummer seines Anschlusses bei Anfragen nennen.

Umherirrender Patient

Für den Fall, daß ein verwirrter Patient auf dem Flur angetroffen wird, wird gelegentlich gewünscht, daß von jeder Station aus auf Identifizierungs- und Bewegungsdaten aller momentan stationär aufgenommenen Patienten lesend zugegriffen werden kann. Dies erscheint aber nicht notwendig. Eine Klärung am Telefon ist hier sinnvoller.

Entlassung und Abrechnung

Die Ärzte der jeweiligen Abteilung sind für die Mitteilung der ausgeführten Leistungen (Diagnosen, Therapien, und, soweit schon ermittelt, Fallpauschalen und

Sonderentgelte) an die Kliniksverwaltung verantwortlich. Diese abrechnungsrelevanten Daten werden von der Fachabteilung bzw. dem Funktionsbereich an die Kliniksverwaltung übermittelt und für den verantwortlichen Sachbearbeiter der Verwaltung mit Leserecht versehen. Da Prüfung des Abrechnungsvorschlags und eventuell Nacherfassung durch die Verwaltung nötig ist, ist dieser mit Schreibrecht zu versehen. Der Sachbearbeiter der Verwaltung erhält auf diese Weise unvermeidlich auch Einblick in besonders sensible Daten, z. B. Diagnosen und Therapien einer psychiatrischen Behandlung. Ferner hat der Sachbearbeiter Zugriffsrechte auf die administrativen Daten und verwaltungsinterne Sonderdaten wie Buchhaltungsdaten bei Selbst- und Zuzahlern.

Archivierung

Zugriffe auf archivierte Daten, egal wo diese physisch lagern, sind wie für aktuell gehaltene Daten zu regeln. Insbesondere unterliegen sie weiterhin der Datenhoheit der Fachabteilung. Die Vorschriften über Aufbewahrungsfristen und Löschpflichten sind zu beachten. Eine Archivierung der Daten und damit Herausnahme aus dem Direktzugriff ist nach etwa 5 Jahren sinnvoll; für die Aufbewahrungsfrist im Archiv erscheinen in der Regel 30 Jahre angemessen, sofern nicht andere Gesichtspunkte oder gesetzliche Vorschriften dem entgegenstehen (z. B. medizinische Gesichtspunkte, Archivgesetzgebeung). In jedem Fall sind die Vorschriften des Sperrens bzw. Löschens von Daten angepaßt an das jeweilige Speichermedium wirksam umzusetzen.

7.4 Well Known Ports

Reserved	0	
TCP Port Service Multiplexer	1	tcpmux
Management Utility	2	compressnet
Compression Process	3	compressnet
Unassigned	4	
Remote Job Entry	5	rje
Unassigned	6	
Echo	7	echo

Unassigned	8	
Discard	9	discard
Unassigned	10	
Active Users	11	systat
Unassigned	12	
Daytime (RFC 867)	13	daytime
Unassigned	14	
Unassigned [was netstat]	15	

Unassigned	16	
Quote of the Day	17	qotd
Message Send Protocol	18	msp
Character Generator	19	chargen
File Transfer [Default Data]	20	ftp-data
File Transfer [Control]	21	ftp
SSH Remote Login Protocol	22	ssh
Telnet	23	telnet
any private mail system	24	
Simple Mail Transfer	25	smtp
Unassigned	26	
NSW User System FE	27	nsw-fe
Unassigned	28	
MSG ICP	29	msg-icp
Unassigned	30	
MSG Authentication	31	msg-auth
Unassigned	32	
Display Support Protocol	33	dsp
Unassigned	34	
any private printer server	35	
Unassigned	36	
Time	37	time
Route Access Protocol	38	rap
Resource Location Protocol	39	rlp

Unassigned	40	
Graphics	41	graphics
Host Name Server	42	name
Host Name Server	42	nameserver
Who Is	43	nicname
MPM FLAGS Protocol	44	mpm-flags
Message Processing Module [recv]	45	mpm
MPM [default send]	46	mpm-snd
NI FTP	47	ni-ftp
Digital Audit Daemon	48	auditd
Login Host Protocol (TACACS)	49	tacacs
Remote Mail Checking Protocol	50	re-mail-ck
IMP Logical Address Maintenance	51	la-maint
XNS Time Protocol	52	xns-time
Domain Name Server	53	domain
XNS Clearinghouse	54	xns-ch
ISI Graphics Language	55	isi-gl
XNS Authentication	56	xns-auth
any private terminal access	57	
XNS Mail	58	xns-mail
any private file service	59	
Unassigned	60	
NI MAIL	61	ni-mail
ACA Services	62	acas
whois++	63	whois++
Communications	64	covia

Integrator (CI)		
TACACS-Database Service	65	tacacs-ds
Oracle SQL*NET	66	sql*net
Bootstrap Protocol Server	67	bootps
Bootstrap Protocol Client	68	bootpc
Trivial File Transfer	69	tftp
Gopher	70	gopher
Remote Job Service	71	netrjs-1
Remote Job Service	72	netrjs-2
Remote Job Service	73	netrjs-3
Remote Job Service	74	netrjs-4
any private dial out service	75	
Distributed External Object Store	76	deos
any private RJE service	77	
vettcp	78	vettcp
Finger	79	finger
World Wide Web HTTP	80	http
World Wide Web HTTP	80	www
World Wide Web HTTP	80	www-http
HOSTS2 Name Server	81	hosts2-ns
XFER Utility	82	xfer
MIT ML Device	83	mit-ml-dev
Common Trace Facility	84	ctf
MIT ML Device	85	mit-ml-dev
Micro Focus Cobol	86	mfcobol
any private terminal link	87	
Kerberos	88	kerberos
SU/MIT Telnet Gateway	89	su-mit-tg
DNSIX Securit Attribute Token Map	90	dnsix
MIT Dover Spooler	91	mit-dov
Network Printing Protocol	92	npp
Device Control Protocol	93	dcp
Tivoli Object Dispatcher	94	objcall
SUPDUP	95	supdup
DIXIE Protocol Specification	96	dixie
Swift Remote Virtural File Protocol	97	swift-rvf
TAC News	98	tacnews
Metagram Relay	99	metagram
[unauthorized use]	100	newacct
NIC Host Name Server	101	hostname
ISO-TSAP Class 0	102	iso-tsap
Genesis Point-to-Point Trans Net	103	gppitnp
ACR-NEMA Digital Imag. & Comm. 300	104	acr-nema
CCSO name server protocol	105	cso

Mailbox Name Nameserver	105	csnet-ns
3COM-TSMUX	106	3com-tsmux
Remote Telnet Service	107	rtelnet
SNA Gateway Access Server	108	snagas
Post Office Protocol - Version 2	109	pop2
Post Office Protocol - Version 3	110	pop3
SUN Remote Procedure Call	111	sunrpc
	113	ident
Authentication Service	113	auth
Audio News Multicast	114	audionews
Simple File Transfer Protocol	115	sftp
ANSA REX Notify	116	ansanotify
UUCP Path Service	117	uucp-path
SQL Services	118	sqlserv
Network News Transfer Protocol	119	nntp
CFDPTKT	120	cfdptkt
Encore Expedited Remote Pro.Call	121	erpc
SMAKYNET	122	smakynet
Network Time Protocol	123	ntp
ANSA REX Trader	124	ansatrader
Locus PC-Interface Net Map Ser	125	locus-map
NXEdit	126	nxedit
Unisys Unitary Login	126	unitary

Locus PC-Interface Conn Server	127	locus-con
GSS X License Verification	128	gss-xlicen
Password Generator Protocol	129	pwdgen
cisco FNATIVE	130	cisco-fna
cisco TNATIVE	131	cisco-tna
cisco SYSMAINT	132	cisco-sys
Statistics Service	133	statsrv
INGRES-NET Service	134	ingres-net
DCE endpoint resolution	135	epmap
PROFILE Naming System	136	profile
NETBIOS Name Service	137	netbios-ns
NETBIOS Datagram Service	138	netbios-dgm
NETBIOS Session Service	139	netbios-ssn
EMFIS Data Service	140	emfis-data
EMFIS Control Service	141	emfis-cntl
Britton-Lee IDM	142	bl-idm
Internet Message Access Protocol	143	imap
Universal Management Architecture	144	uma
UAAC Protocol	145	uaac
ISO-IP0	146	iso-tp0
ISO-IP	147	iso-ip
Jargon	148	jargon

AED 512 Emulation Service	149	aed-512
SQL-NET	150	sql-net
HEMS	151	hems
Background File Transfer Program	152	bftp
SGMP	153	sgmp
NETSC	154	netsc-prod
NETSC	155	netsc-dev
SQL Service	156	sqlsrv
KNET/VM Command/Message Protocol	157	knet-cmp
PCMail Server	158	pcmail-srv
NSS-Routing	159	nss-routing
SGMP-TRAPS	160	sgmp-traps
SNMP	161	snmp
SNMPTRAP	162	snmptrap
CMIP/TCP Manager	163	cmip-man
CMIP/TCP Agent	164	cmip-agent
Xerox	165	xns-courier
Sirius Systems	166	s-net
NAMP	167	namp
RSVD	168	rsvd
SEND	169	send
Network PostScript	170	print-srv
Network Innovations Multiplex	171	multiplex
Network Innovations CL/1	172	cl/1
Xyplex	173	xyplex-mux

MAILQ	174	mailq
VMNET	175	vmnet
GENRAD-MUX	176	genrad-mux
X Display Manager Control Protocol	177	xdmcp
NextStep Window Server	178	nextstep
Border Gateway Protocol	179	bgp
Intergraph	180	ris
Unify	181	unify
Unisys Audit SITP	182	audit
OCBinder	183	ocbinder
OCServer	184	ocserver
Remote-KIS	185	remote-kis
KIS Protocol	186	kis
Application Communication Interface	187	aci
Plus Five's MUMPS	188	mumps
Queued File Transport	189	qft
Gateway Access Control Protocol	190	gacp
Prospero Directory Service	191	prospero
OSU Network Monitoring System	192	osu-nms
Spider Remote Monitoring Protocol	193	srmp
Internet Relay Chat Protocol	194	irc
DNSIX Network Level	195	dn6-nlm-aud

Module Audit		
DNSIX Session Mgt Module Audit Redir	196	dn6-smm-red
Directory Location Service	197	dls
Directory Location Service Monitor	198	dls-mon
SMUX	199	smux
IBM System Resource Controller	200	src
AppleTalk Routing Maintenance	201	at-rtmp
AppleTalk Name Binding	202	at-nbp
AppleTalk Unused	203	at-3
AppleTalk Echo	204	at-echo
AppleTalk Unused	205	at-5
AppleTalk Zone Information	206	at-zis
AppleTalk Unused	207	at-7
AppleTalk Unused	208	at-8
The Quick Mail Transfer Protocol	209	qmtp
ANSI Z39.50	210	z39.50
Texas Instruments 914C/G Terminal	211	914c/g
ATEXSSTR	212	anet
IPX	213	ipx
VM PWSCS	214	vmpwscs
Insignia Solutions	215	softpc
Computer Associates Int'l License Server	216	CAIlic
dBASE Unix	217	dbase
Netix Message Posting Protocol	218	mpp
Unisys ARPs	219	uarps
Interactive Mail Access Protocol v3	220	imap3
Berkeley rlogind with SPX auth	221	fln-spx
Berkeley rshd with SPX auth	222	rsh-spx
Certificate Distribution Center	223	cdc
masqdialer	224	masqdialer
Direct	242	direct
Survey Measurement	243	sur-meas
Dayna	244	dayna
LINK	245	link
Display Systems Protocol	246	dsp3270
SUBNTBCST_TFTP	247	subntbcst_tftp
bhfhs	248	bhfhs
RAP	256	rap
Secure Electronic Transaction	257	set
Yak Winsock Personal Chat	258	yak-chat
Efficient Short Remote Operations	259	esro-gen
Openport	260	openport
IIOP Name Service over TLS/SSL	261	nsiiops
Arcisdms	262	arcisdms

HDAP	263	hdap
BGMP	264	bgmp
http-mgmt	280	http-mgmt
Personal Link	281	personal-link
Cable Port A/X	282	cableport-ax
Unassigned	283-307	
Novastor Backup	308	novastorbakcup
EntrustTime	309	entrusttime
bhmds	310	bhmds
AppleShare IP WebAdmin	311	asip-webadmin
VSLMP	312	vslmp
Magenta Logic	313	magenta-logic
Opalis Robot	314	opalis-robot
DPSI	315	dpsi
decAuth	316	decauth
Zannet	317	zannet
PIP	321	pip
Prospero Data Access Protocol	344	pdap
Perf Analysis Workbench	345	pawserv
Zebra server	346	zserv
Fatmen Server	347	fatserv
Cabletron Management Protocol	348	csi-sgwp
mftp	349	mftp
MATIP Type A	350	matip-type-a
MATIP Type B	351	matip-type-b
bhoetty (added 5/21/97)	351	bhoetty
DTAG (assigned long ago)	352	dtag-ste-sb
bhoedap4 (added 5/21/97)	352	bhoedap4
NDSAUTH	353	ndsauth
bh611	354	bh611
DATEX-ASN	355	datex-asn
Cloanto Net 1	356	cloanto-net-1
bhevent	357	bhevent
Shrinkwrap	358	shrinkwrap
nebris Network Trace Service	359	tenebris_nts
scoi2odialog	360	scoi2odialog
Semantix	361	semantix
SRS Send	362	srssend
RSVP Tunnel	363	rsvp_tunnel
Aurora CMGR	364	aurora-cmgr
DTK	365	dtk
ODMR	366	odmr
MortgageWare	367	mortgageware
QbikGDP	368	qbikgdp
rpc2portmap	369	rpc2portmap
codaauth2	370	codaauth2
Clearcase	371	clearcase
ListProcessor	372	ulistproc
Legent Corporation	373	legent-1
Legent Corporation	374	legent-2
Hassle	375	hassle
Amiga Envoy Network Inquiry Proto	376	nip

NEC Corporation	377	tnETOS
NEC Corporation	378	dsETOS
TIA/EIA/IS-99 modem client	379	is99c
TIA/EIA/IS-99 modem server	380	is99s
hp performance data collector	381	hp-collector
hp performance data managed node	382	hp-managed-node
hp performance data alarm manager	383	hp-alarm-mgr
A Remote Network Server System	384	arns
IBM Application	385	ibm-app
ASA Message Router Object Def.	386	asa
Appletalk Update-Based Routing Pro.	387	aurp
Unidata LDM Version 4	388	unidata-ldm
Lightweight Directory Access Protocol	389	ldap
UIS	390	uis
SynOptics SNMP Relay Port	391	synotics-relay
SynOptics Port Broker Port	392	synotics-broker
Data Interpretation System	393	dis
EMBL Nucleic Data Transfer	394	embl-ndt
NETscout Control Protocol	395	netcp
Novell Netware over IP	396	netware-ip
Multi Protocol Trans. Net.	397	mptn
Kryptolan	398	kryptolan
ISO Transport Class 2 Non-Control over TCP	399	iso-tsap-c2
Workstation Solutions	400	work-sol
Uninterruptible Power Supply	401	ups
Genie Protocol	402	genie
decap	403	decap
nced	404	nced
ncld	405	ncld
Interactive Mail Support Protocol	406	imsp
Timbuktu	407	timbuktu
Prospero Resource Manager Sys. Man.	408	prm-sm
Prospero Resource Manager Node Man.	409	prm-nm
DECLadebug Remote Debug Protocol	410	decladebug
Remote MT Protocol	411	rmt
Trap Convention Port	412	synoptics-trap
SMSP	413	smsp
InfoSeek	414	infoseek
BNet	415	bnet
Silverplatter	416	silverplatter
Onmux	417	onmux
Hyper-G	418	hyper-g

Ariel	419	ariel1
SMPTE	420	smpte
Ariel	421	ariel2
Ariel	422	ariel3
IBM Operations Planning and Control Start	423	opc-job-start
IBM Operations Planning and Control Track	424	opc-job-track
ICAD	425	icad-el
smartsdp	426	smartsdp
Server Location	427	svrloc
OCS_CMU	428	ocs_cmu
OCS_AMU	429	ocs_amu
UTMPSD	430	utmpsd
UTMPCD	431	utmpcd
IASD	432	iasd
NNSP	433	nnsp
MobileIP-Agent	434	mobileip-agent
MobilIP-MN	435	mobilip-mn
DNA-CML	436	dna-cml
comscm	437	comscm
dsfgw	438	dsfgw
dasp	439	dasp
sgcp	440	sgcp
decvms-sysmgt	441	decvms-sysmgt
cvc_hostd	442	cvc_hostd
http protocol over TLS/SSL	443	https
Simple Network Paging Protocol	444	snpp
Microsoft-DS	445	microsoft-ds
DDM-RDB	446	ddm-rdb
DDM-RFM	447	ddm-dfm
DDM-SSL	448	ddm-ssl
AS Server Mapper	449	as-servermap
TServer	450	tserver
Cray Network Semaphore server	451	sfs-smp-net
Cray SFS config server	452	sfs-config
CreativeServer	453	creativeserver
ContentServer	454	contentserver
CreativePartnr	455	creativepartnr
macon-tcp	456	macon-tcp
scohelp	457	scohelp
apple quick time	458	appleqtc
ampr-rcmd	459	ampr-rcmd
skronk	460	skronk
DataRampSrv	461	datasurfsrv
DataRampSrvSec	462	datasurfsrvsec
alpes	463	alpes
kpasswd	464	kpasswd
SMTP Protocol over TLS/SSL	465	smtps
digital-vrc	466	digital-vrc
mylex-mapd	467	mylex-mapd
proturis	468	photuris
Radio Control Protocol	469	rcp
scx-proxy	470	scx-proxy

Mondex	471	mondex
ljk-login	472	ljk-login
hybrid-pop	473	hybrid-pop
tn-tl-w1	474	tn-tl-w1
tcpnethaspsrv	475	tcpnethaspsrv
tn-tl-fd1	476	tn-tl-fd1
ss7ns	477	ss7ns
spsc	478	spsc
iafserver	479	iafserver
iafdbase	480	iafdbase
Ph service	481	ph
bgs-nsi	482	bgs-nsi
ulpnet	483	ulpnet
Integra Software Management Environment	484	integra-sme
Air Soft Power Burst	485	powerburst
avian	486	avian
saft Simple Asynchronous File Transfer	487	saft
gss-http	488	gss-http
nest-protocol	489	nest-protocol
micom-pfs	490	micom-pfs
go-login	491	go-login
Transport Independent Convergence for FNA	492	ticf-1
Transport Independent Convergence for FNA	493	ticf-2
POV-Ray	494	pov-ray
intecourier	495	intecourier

PIM-RP-DISC	496	pim-rp-disc
dantz	497	dantz
siam	498	siam
ISO ILL Protocol	499	iso-ill
isakmp	500	isakmp
STMF	501	stmf
asa-appl-proto	502	asa-appl-proto
Intrinsa	503	intrinsa
citadel	504	citadel
mailbox-lm	505	mailbox-lm
ohimsrv	506	ohimsrv
crs	507	crs
xvttp	508	xvttp
snare	509	snare
FirstClass Protocol	510	fcp
PassGo	511	passgo
remote process execution; authentication performed using passwords and UNIX loppgin names	512	exec
remote login a la telnet; automatic authentication performed based on priviledged port numbers and distributed data bases which identify "authentication domains"	513	login
cmd like exec, but automatic	514	shell

authentication is performed as for login server		
spooler	515	printer
videotex	516	videotex
like tenex link, but across machine - unfortunately, doesn't use link protocol (this is actually just a rendezvous port from which a tcp connection is established)	517	talk
	518	ntalk
unixtime	519	utime
extended file name server	520	efs
ripng	521	ripng
ULP	522	ulp
IBM-DB2	523	ibm-db2
NCP	524	ncp
timeserver	525	timed
newdate	526	tempo
Stock IXChange	527	stx
Customer IXChange	528	custix
IRC-SERV	529	irc-serv
rpc	530	courier
chat	531	conference
readnews	532	netnews
for emergency broadcasts	533	netwall
MegaMedia Admin	534	mm-admin
iiop	535	iiop
opalis-rdv	536	opalis-rdv
Networked Media Streaming Protocol	537	nmsp
gdomap	538	gdomap
Apertus Technologies Load Determination	539	apertus-ldp
uucpd	540	uucp
uucp-rlogin	541	uucp-rlogin
commerce	542	commerce
	543	klogin
krcmd	544	kshell
appleqtcsrvr	545	appleqtcsrvr
DHCPv6 Client	546	dhcpv6-client
DHCPv6 Server	547	dhcpv6-server
AFP over TCP	548	afpovertcp
IDFP	549	idfp
new-who	550	new-rwho
cybercash	551	cybercash
deviceshare	552	deviceshare
pirp	553	pirp
Real Time Stream Control Protocol	554	rtsp
	555	dsf
rfs server	556	remotefs
openvms-sysipc	557	openvms-sysipc
SDNSKMP	558	sdnskmp
TEEDTAP	559	teedtap
rmonitord	560	rmonitor

	561	monitor
chcmd	562	chshell
nntp protocol over TLS/SSL (was snntp)	563	nntps
plan 9 file service	564	9pfs
whoami	565	whoami
streettalk	566	streettalk
banyan-rpc	567	banyan-rpc
microsoft shuttle	568	ms-shuttle
microsoft rome	569	ms-rome
demon	570	meter
udemon	571	meter
sonar	572	sonar
banyan-vip	573	banyan-vip
FTP Software Agent System	574	ftp-agent
VEMMI	575	vemmi
ipcd	576	ipcd
vnas	577	vnas
ipdd	578	ipdd
decbsrv	579	decbsrv
SNTP HEARTBEAT	580	sntp-heartbeat
Bundle Discovery Protocol	581	bdp
SCC Security	582	scc-security
Philips Video-Conferencing	583	philips-vc
Key Server	584	keyserver
IMAP4+SSL (Use of 585 is not recommended, use 993 instead)	585	imap4-ssl
Password Change	586	password-chg
Submission	587	submission
CAL	588	cal
EyeLink	589	eyelink
TNS CML	590	tns-cml
FileMaker, Inc. - HTTP Alternate (see Port 80)	591	http-alt
Eudora Set	592	eudora-set
HTTP RPC Ep Map	593	http-rpc-epmap
TPIP	594	tpip
CAB Protocol	595	cab-protocol
SMSD	596	smsd
PTC Name Service	597	ptcnameservice
SCO Web Server Manager 3	598	sco-websrvrmg3
Aeolon Core Protocol	599	acp
Sun IPC server	600	ipcserver
Cray Unified Resource Manager	606	urm
nqs	607	nqs
Sender-Initiated/Unsolicited File Transfer	608	sift-uft
npmp-trap	609	npmp-trap
npmp-local	610	npmp-local
npmp-gui	611	npmp-gui
HMMP Indication	612	hmmp-ind
HMMP Operation	613	hmmp-op
SSLshell	614	sshell
Internet Configuration	615	sco-inetmgr

Manager		
SCO System Administration Server	616	sco-sysmgr
SCO Desktop Administration Server	617	sco-dtmgr
DEI-ICDA	618	dei-icda
Digital EVM	619	digital-evm
SCO WebServer Manager	620	sco-websrvrmgr
ESCP	621	escp-ip
Collaborator	622	collaborator
Aux Bus Shunt	623	aux_bus_shunt
Crypto Admin	624	cryptoadmin
DEC DLM	625	dec_dlm
ASIA	626	asia
PassGo Tivoli	627	passgo-tivoli
QMQP	628	qmqp
3Com AMP3	629	3com-amp3
RDA	630	rda
IPP (Internet Printing Protocol)	631	ipp
bmpp	632	bmpp
Service Status update (Sterling Software)	633	servstat
ginad	634	ginad
RLZ DBase	635	rlzdbase
ldap protocol over TLS/SSL (was sldap)	636	ldaps
lanserver	637	lanserver
mcns-sec	638	mcns-sec
MSDP	639	msdp
entrust-sps	640	entrust-sps
repcmd	641	repcmd
ESRO-EMSDP V1.3	642	esro-emsdp
SANity	643	sanity
dwr	644	dwr
PSSC	645	pssc
LDP	646	ldp
DHCP Failover	647	dhcp-failover
Registry Registrar Protocol (RRP)	648	rrp
Aminet	649	aminet
OBEX	650	obex
IEEE MMS	651	ieee-mms
UDLR_DTCP	652	udlr-dtcp
	666	mdqs
doom	666	doom
campaign contribution disclosures - SDR Technologies	667	disclose
MeComm	668	mecomm
MeRegister	669	meregister
VACDSM-SWS	670	vacdsm-sws
VACDSM-APP	671	vacdsm-app
VPPS-QUA	672	vpps-qua
CIMPLEX	673	cimplex
ACAP	674	acap
DCTP	675	dctp
VPPS Via	676	vpps-via
Virtual Presence Protocol	677	vpp

GNU Generation Foundation NCP	678	ggf-ncp
MRM	679	mrm
entrust-aaas	680	entrust-aaas
entrust-aams	681	entrust-aams
XFR	682	xfr
CORBA IIOP	683	corba-iiop
CORBA IIOP SSL	684	corba-iiop-ssl
MDC Port Mapper	685	mdc-portmapper
Hardware Control Protocol Wismar	686	hcp-wismar
asipregistry	687	asipregistry
errlog copy/server daemon	704	elcsd
AgentX	705	agentx
Borland DSJ	707	borland-dsj
Entrust Key Management Service Handler	709	entrust-kmsh
Entrust Administration Service Handler	710	entrust-ash
Cisco TDP	711	cisco-tdp
IBM NetView DM/6000 Server/Client	729	netviewdm1
IBM NetView DM/6000 send/tcp	730	netviewdm2
IBM NetView DM/6000 receive/tcp	731	netviewdm3
netGW	741	netgw
Network based Rev. Cont. Sys.	742	netrcs
Flexible License Manager	744	flexlm
Fujitsu Device Control	747	fujitsu-dev
Russell Info Sci Calendar Manager	748	ris-cm
kerberos administration	749	kerberos-adm
	750	rfile
	751	pump
	752	qrh
	753	rrh
send	754	tell
	758	nlogin
	759	con
	760	ns
	761	rxe
	762	quotad
	763	cycleserv
	764	omserv
	765	webster
phone	767	phonebook
	769	vid
	770	cadlock
	771	rtip
	772	cycleserv2
	773	submit
	774	rpasswd
	775	entomb
	776	wpages
Multiling HTTP	777	multiling-http

	780	wpgs
Concert	786	concert
QSC	787	qsc
	800	mdbs_daemon
	801	device
FCP	810	fcp-udp
itm-mcell-s	828	itm-mcell-s
PKIX-3 CA/RA	829	pkix-3-ca-ra
rsync	873	rsync
ICL coNETion locate server	886	iclcnet-locate
ICL coNETion server info	887	iclcnet_svinfo
AccessBuilder	888	accessbuilder
CD Database Protocol	888	cddbp
OMG Initial Refs	900	omginitialrefs
xact-backup	911	xact-backup
ftp protocol, data, over TLS/SSL	989	ftps-data

ftp protocol, control, over TLS/SSL	990	ftps
Netnews Administration System	991	nas
telnet protocol over TLS/SSL	992	telnets
imap4 protocol over TLS/SSL	993	imaps
irc protocol over TLS/SSL	994	ircs
pop3 protocol over TLS/SSL (was spop3)	995	pop3s
vsinet	996	vsinet
	997	maitrd
	998	busboy
	999	garcon
	999	puprouter
	1000	cadlock
surf	1010	surf
Reserved	1023	

7.5 Netzwerkgeräte

7.5.1 Typische Paßwörter

Gerät/Hersteller	Lese-Paßwort	Schreib-/Lese-Paßwort
Ascend	public	write
Bay	public	private
Cisco	public	private
3Com	public, monitor	manager, security

7.5.1.1 Gängige SNMP-Community-Paßwörter

- public
- community
- password

- private
- secret
- worldread
- network
- manager
- writeciscoall
- private
- admin
- default
- security
- tivoli
- openview
- monitor
- monitor

Das Paßwort „all private“ gilt größtenteils für Solaris.

7.5.1.2 Switches / Router

Gerät	Benutzername	Paßwort	Ebene
Bay-Router	User Manager	<null> <null>	Benutzer Administrator
Bay 350T-Switch	NetICs	NA	Administrator
Bay SuperStackII	security	security	Administrator
3Com	admin read write debug tech monitor manager security	synnet synnet synnet synnet tech monitor manager security	Administrator Benutzer Administrator Administrator enutzer Administrator Administrator
Cisco	(telnet) (telnet) enable (telnet)	c(Cisco 2600s) cisco cisco cisco routers	Benutzer Benutzer Administrator
Shiva	root Guest	<null> <null>	Administrator Benutzer
Webramp	wradmin	trancell	Administrator
Notorola-CableRouter	cablecom	router	Administrator

7.5.2 Port-Analyse

7.5.2.1 Standardmäßig geöffnete Ports

Hardware	TCP	UDP
Cisco Routers	21 (FTP) 23 (Telnet) 79 (Finger) 80 (HTTP) 512 (exec) 513 (Login) 514 (Shell) 1993 (Cisco SNMP) 1999 (Cisco ident) 2001 4001 6001 9001 (XRemote service)	0 (tcpmux) 49 (domain) 67 (bootps 123 (NTP) 161 (SNMP)
Cisco Switches	23 (Telnet) 7161	0 (tcpmux) 123 (NTP) 161 (SNMP)
Bay Routers	21 (FTP) 23 (Telnet)	7 (Echo) 9 (Discard) 67 (Bootps) 68 (bootpc) 69 (TFTP) 161 (SNMP) 520 (Route)
Ascend Routers	23 (Telnet)	7 (Echo) 9 (Discard) 161 (SNMP) 162 (SNMP-Trap) 514 (Shell) 520 (Route)

8 Inhaltsverzeichnis

A

Applets 14
Application Level Gateway ii, 18, 24, 25
ARP i, 8
Authentifizierung 9, 13, 25, 26, 41, 42, 43, 112, 113

B

Bastion-Host 18
Blowfish iii, 6, 40, 46, 49
BSI 1, 3

C

Challenge Handshake Authentication Protocol ii, 26
CHAP ii, 26
Client 20

D

Daten
Patientendateniv, 105, 106, 107, 108, 109, 112, 113, 114
Datenschutzbeauftragteiv, 88, 98, 99, 100, 102, 109, 111, 116
Diffie-Hellman iii, 40
Digital Signature Standard iii, 40
Digitale Sinatur iii, 6, 34, 97
DSS iii, 40
Dual-Homed-Host 18, 19

E

ECP ii, 27
Einwegfunktionen 34
Elliptische Kurven iii, 6, 40
Email iii, 12, 17, 43

F

Firewall 20, 24
Paketfilter 18
Firewall-Authentifizierungsmechanismen ii, 24
FTP i, 10, 13, 14, 18, 20, 45, 46, 119, 129, 134

G

Grundschutzansatz i

H

Hash-Funktionen 34
Host 19
Bastion-Host 18
Dual-Homed-Host 18, 19
Hostabsicherung ii, 15
HTTP i, iii, 10, 13, 14, 20, 43, 120, 129, 131, 134

I

ICMP i, 9
IDEA iii, 6, 33, 37, 38, 40, 46, 50
International Protocol Security iii, 22, 23, 45
Internet Protokoll 17
Internet Protokollei, 8, 9, 10, 11, 15, 17, 22, 23, 45, 124, 125
IP i, 8, 9, 10, 11, 15, 17, 22, 23, 45, 124, 125
IPSec iii, 22, 23, 45

K

Kryptographie ii, iii, 9, 33, 42, 45, 46, 47, 48, 50
asymmetrische iii, 33
Blowfish iii, 6, 40, 46, 49
DES iii, 35, 36, 37, 38, 41, 44, 46
Diffie-Hellman iii, 40
Digital Signature Standard iii, 40
Digitale Signatur iii, 6, 34, 97
Effizienz iii, 45, 46
Einwegfuntionen 34
Elliptische Kurven iii, 6, 40
Hash-Funktionen 34
International Protocol Security iii, 45
Pretty Good Privacy iii, 44, 50
Public-Key-Verfahren 26, 33, 34, 35, 42, 44
RC 5 iii, 41

RSA iii, 6, 38, 39, 40, 41, 42, 44
Secure Hypertext Transfer Protocol iii, 43
Secure Multi Purpose Mail Extension iii, 44
Secure Shell iii, 13, 41
Secure Socket Layer iii, 41
Simple Key Management for Internet Protocoliii, 43, 49, 50
symmetrische ii, 33
Twofish iii, 40
Kryptographie IDEA iii, 6, 33, 37, 38, 40, 46, 50

N

Netzabsicherung ii, 16
Application Level Gateway ii, 18, 24, 25
Firewall-Authentifizierungsmechanismen ii, 24
Paketfilter ii, 16, 18
Proxy Gateway ii, 18
Netzwerkgeräte iv, 132
Port-Analyse iv, 134
SNMP-Community-Paßwörter iv, 132
Switches / Router iv, 133
Typische Paßwörter iv, 132

P

Paket 17, 18
Paketfilter 18
Paketfilterung ii, 16, 17, 18, 19, 21
PAP ii, 26
Password Authentication Protocol ii, 26
Paßwörter
SNMP-Community-Paßwörter iv, 132
Paßwörter, Typische iv, 132
Patientendaten iv, 105, 106, 107, 108, 109, 112, 113, 114
PGP iii, 44, 45, 50
Port-Analyse iv, 134
PPP Encryption Control Protocol ii, 27
Pretty Good Privacy iii, 44, 45, 50
Protokolle, Internet
ARP i, 8
Email iii, 12, 17, 43
FTP i, 10, 13, 14, 18, 20, 45, 46, 119, 129, 134
HTTP i, iii, 10, 13, 14, 20, 43, 120, 129, 131, 134
ICMP i, 9
IP i, 8, 9, 10, 11, 15, 17, 22, 23, 45, 124, 125
SMTP i, 12, 21, 43, 126
TCPi, 7, 9, 10, 11, 12, 13, 14, 15, 17, 31, 41, 42, 47, 50, 118, 122, 125, 128, 134
Telnet i, 13, 18, 19, 20, 21, 41, 119, 120, 121, 134
UDP i, 9, 10, 11, 17, 134
Well Known Ports iv, 118
Proxy Gateway ii, 18
Proxy-Server 19, 20
Public-Key-Verfahren 26, 33, 34, 35, 42, 44

R

Radius ii, 27, 28
RAS ii, 26, 27, 28
Challenge Handshake Authentication Protocol ii, 26
CHAP ii, 26
ECP ii, 27
Internet iii, 49
ISDN iii, 49
PAP ii, 26
Password Authentication Protocol ii, 26
PPP Encryption Control Protocol ii, 27
Radius ii, 27, 28
Tacacs+ ii, 28
Wardialer ii, 28, 29
RC 5 iii, 41
Remote Access Lösungen iii, 49
Remote Access Service ii, 26, 27, 28
Risikoanalye i, 2, 4
Risikoanalyse
Grundschutzansatz i
Sicherheitskonzept i, iii, 4, 5, 30, 49, 91, 112
Router 17
RPC 17
RSA iii, 6, 38, 39, 40, 41, 42, 44

S

S/MIME iii, 44
SafeGuard 46, 49
Schlüsselmanagement 43
Schutzmechanismen ii, 15, 17
Hostabsicherung ii, 15
Netzabsicherung ii, 16
Verbindungsabsicherung ii, 15
Secure Hypertext Transfer Protocol iii, 14, 43

Secure Multi Purpose Mail Extension iii, 44
Secure Shell iii, 13, 41, 42, 43, 45, 46, 119
SSH Connection Protocol iii, 42
SSH Transport Layer Protocol iii, 42
SSH User Authentication Protocol iii, 42
Secure Socket Layeriii, 41, 112, 123, 126, 129, 130, 131, 132
S-HTTP iii, 14, 43
Sicherheitsanforderungen i, 4, 5, 6, 43, 91, 112
Sicherheitskonzept i, iii, 4, 5, 30, 49, 91, 112
Signatur, Digitale iii, 6, 34, 97
Signaturgesetz iv, 90
Simple Key Management for Internet Protocoliii, 43, 49, 50
SKIP iii, 43, 49, 50
SMTP i, 12, 21, 43, 126
SSH iii, 13, 41, 42, 43, 45, 46, 119
SSL iii, 41

T

Tacacs+ ii, 28
TCPi, 7, 9, 10, 11, 12, 13, 14, 15, 17, 31, 41, 42, 47, 50, 118, 122, 125, 128, 134
Telnet i, 13, 18, 19, 20, 21, 41, 119, 120, 121, 134
Transmission Control Protocol 17
Twofish iii, 40

U

UDP i, 9, 10, 11, 17, 134

V

Viren ii, 30
Virtuelle Private Netzwerke ii, 21, 22, 32, 45, 46, 47, 49
VPN ii, 21, 22, 32, 45, 46, 47, 49

W

Wardialer ii, 28, 29
Well Known Ports iv, 118