Computer-spionage

Risiken und Prävention

Karl-Friedrich Fecht / Walter Opfermann / Wolfgang Scheiterle

Die vorliegende Studie wird mit freundlicher Genehmigung der Autoren

Karl-Friedrich Fecht,

Walter Opfermann,

Wolfgang Scheiterle,

die Mitarbeiter des Landesamtes für Verfassungsschutz Baden Württemberg sind, herausgegeben. Der Inhalt gibt nicht notwendigerweise die Meinung des Bundesministeriums für Wirtschaft wieder. Bitte beachten Sie, daß einzelne Angaben bzw. Zahlen ggf. nicht dem aktuellen Stand entsprechen können.

"Bei der Frage der Bekämpfung dieses Phänomens *(der nachrichtendienstlichen Ausforschung)* müssen wir uns darüber im klaren sein, daß die klassische Spionage an Bedeutung verliert und zukünftig vermehrt durch den lautlosen elektronischen Angriff ersetzt wird."

RA Wolfgang Hoffmann,
Vorsitzender der Arbeitsgemeinschaft für Sicherheit
in der Wirtschaft

Inhaltsverzeichnis

8. Anhang 3

1. Ausgangssituation

1.1 Allgemeines

Die moderne elektronische Datenverarbeitung (EDV) tangiert zunehmend sämtliche gesellschaftlichen Bereiche. Inzwischen hat sich auch in der öffentlichen Verwaltung ein ähnlich hoher DV-Standard eingestellt, wie er in der Privatwirtschaft bereits seit längerer Zeit besteht. Das staatliche Gemeinwesen gerät immer mehr in Abhängigkeit vom zuverlässigen Funktionieren informations- und kommunikationstechnischer Systeme. Die immense Datenflut, mit der wir tagtäglich konfrontiert werden, bildet bisher schon ein ganz markantes Charakteristikum unserer sog. Informationsgesellschaft. Das unlängst angebrochene "Internet-Zeitalter" - verbunden mit den Schlagworten "Multimedia" und "Information Highway" - ist dabei, dieser Entwicklung gänzlich neue Dimensionen zu verleihen.

Die gesamte Vielfalt der Daten, ob wichtig oder weniger bedeutend, ob für die breite Öffentlichkeit oder - etwa als Betriebsgeheimnis - nur für einen auserwählten Zirkel bestimmt, wird in unendlicher Dichte auf Speichermedien abgelegt. Computergespeicherte Daten und Informationen sind zwischen-zeitlich zu einem der wichtigsten Faktoren betrieblichen Know-hows geworden. Maschinenlesbare Datenträger gewährleisten in aller Regel jederzeit den raschen Zugriff auf die elektronischen bzw. magnetischen Informationen. Da Wirtschaftsdaten und Nachrichten heutzutage weltweit überall und gleichzeitig verfügbar sind, spielen Standortfragen mittlerweile kaum noch eine Rolle. Dieser Wandel von der Industrie- zur Informationsgesellschaft, der historisch allenfalls mit der industriellen Revolution im letzten Jahrhundert vergleichbar ist, eröffnet vielfältige Chancen, birgt allerdings auch enorme Risiken.

Die rapide Ausbreitung der computerunterstützten Informations- und Kommunikationssysteme hat nämlich gleichzeitig ein erhebliches Anwachsen der damit verbundenen Mißbrauchsmöglichkeiten zur Folge. Mit ihren unterschiedlichsten Erscheinungsformen hat sich die Computerkriminalität zwischenzeitlich zu

einer herausragenden Deliktgruppe innerhalb der polizeilichen Kriminalstatistik entwickelt. In keinem anderen Straftatenbereich sind die jährlichen Steigerungsraten derart hoch. Nach einer Verlautbarung des Bundesministers des Innern vom Februar 1996 hat sich die Computerkriminalität innerhalb eines Jahres verdoppelt. Dabei ist davon auszugehen, daß lediglich ein geringer Teil der auf diesem Sektor verübten Straftaten überhaupt publik wird. Ein herausragendes Spezifikum der Computerkriminalität liegt nämlich nicht zuletzt in der extrem hohen Dunkelziffer von bis zu 85 %.

Strafrechtliche bzw. technische Gegenmaßnahmen vermögen mit dieser Entwicklung kaum Schritt zu halten. Mit Hilfe des "Zweiten Gesetzes zur Bekämpfung der Wirtschaftskriminalität" unternahm der deutsche Gesetzgeber im Jahr 1986 einen ersten Versuch, Computerkriminellen wirkungsvoller begegnen zu können. Neuartige Formen der Tatbegehung, die sich nicht mehr unter die althergebrachten Straftatbestände hatten einordnen lassen, konnten nunmehr ebenfalls strafrechtlich verfolgt werden. Quantensprünge auf dem Gebiet der technologischen Innovation einerseits und die nahezu atemberaubende Zunahme der praktischen Anwendungsmöglichkeiten andererseits verlangen inzwischen jedoch dringend nach einer erneuten Anpassung der Strafrechtsnormen. Besonders umstritten ist derzeit die strafrechtliche Verantwortlichkeit von Online-Dienste-Anbietern (Providern), die den Zugang zu Netzen wie etwa dem Internet ermöglichen.

Etwa Mitte der 80er Jahre entdeckte auch eine ganze Reihe größerer und kleinerer Computerfirmen die Marktnische "DV-Sicherheitssysteme". Die Palette der Erfindungen, die dem Datendieb das Leben schwer machen sollten, reichte von komplizierten Software-Verschlüsselungsalgorithmen bis hin zu simplen mechanischen Absicherungen wie verschließbaren Schubladen für die Tastatur. Von staatlicher Seite wurde 1991 das "Bundesamt für Sicherheit in der Informationstechnik" (BSI) eingerichtet, dessen zentrale Aufgabenstellung bereits aus der Behördenbezeichnung erkennbar wird. Selbstverständlich setzte diese Entwicklung auch bei den Computerstraftätern mannigfaltige kriminelle Energie zur Umgehung technischer Sicherheitseinrichtungen frei, so daß mitt-

lerweile ein regelrechter Wettlauf zwischen mißbräuchlicher Verwendung und Gegenmaßnahmen festzustellen ist.
Der Schwerpunkt der Computerkriminalität liegt seit eh und je im Bereich der verschiedenen Betrugsarten (§ 263 a Strafgesetzbuch/StGB); insbesondere der Mißbrauch gestohlener Eurocheque-Karten an Geldausgabe- und Kassenautomaten spielt hier eine wesentliche Rolle. Die stärkste Zuwachsrate war im Jahr 1994 allerdings beim "Ausspähen von Daten" (§ 202 a StGB) ohne nachrichtendienstlichen Auftrag zu verzeichnen. Auch wenn in der polizeilichen Kriminalstatistik von 1995 für dieses Antragsdelikt ein Rückgang um rund ein Drittel ausgewiesen ist, mehren sich die Anhaltspunkte, daß der staatlich gelenkten Computerspionage und -sabotage immer mehr Bedeutung zukommt.

Diese Entwicklung liegt offensichtlich im internationalen Trend. So sind nach einer aktuellen Studie aus den USA über 90 % aller amerikanischen Unternehmen bereits einmal Opfer von Computerstraftaten geworden. Nach der von der Michigan State University erstellten Expertise haben in den vergangenen fünf Jahren vor allem folgende Zwischenfälle dramatisch zugenommen:

* (Versuchter) Diebstahl von Kunden- oder Unternehmensinformationen
* (Versuchter) Diebstahl von Wirtschaftsgeheimnissen
* (Versuchter) Diebstahl von Informationen über neue Produkte
* (Versuchter) Diebstahl von Produktbeschreibungen
* Unerlaubter Computerzugriff auf vertrauliche Angestellteninformationen
* Unerlaubter Computerzugriff auf vertrauliche Geschäftsinformationen
* (Versuchter) Diebstahl von Geld
* (Versuchter) Diebstahl von Informationen über die Produktpreisgestaltung

Ausweislich einer anderen - vom amerikanischen Senat veröffentlichten - aktuellen Studie kosten allein die durch Hackerangriffe verursachten Schäden die betroffenen Firmen jährlich über 400 Millionen Dollar. Weltweit wird die Schadenshöhe auf mindestens 800 Millionen Dollar geschätzt.

Ein besonders gravierendes Beispiel für das Phänomen "Computermißbrauch" geht aus einer kürzlich veröffentlichten Untersuchung des amerikanischen Rechnungshofs hervor. Danach wurde das Pentagon[1], das in diesem Zusammenhang zweifellos ein besonders reizvolles Zielobjekt darstellt, im letzten Jahr mindestens 250.000mal von Hackern heimgesucht, in nicht weniger als 65 Prozent der Fälle sogar mit Erfolg. Aber nur einer von 150 Angriffen wurde den zuständigen Stellen gemeldet.

1.2 KGB-Hacker-Fall

Einer der spektakulärsten **nachrichtendienstlichen** Angriffe auf fremde DV-Systeme in Deutschland ist bereits im Jahr 1989 publik geworden. Dadurch wurde seinerzeit erstmals die Aufmerksamkeit der Öffentlichkeit auf die Informationstechnik als neuem Zielobjekt der Spionage gelenkt. Da der zugrundeliegende Sachverhalt - was die Tatmodalitäten anbelangt - als geradezu klassischer Computerspionagefall gelten kann, soll er nachfolgend näher dargestellt werden:

Drei Angehörige der Hackerszene in Hannover hatten im Herbst 1986 über einen Mittelsmann Verbindung zum ehemaligen sowjetischen Geheimdienst KGB[2] aufgenommen und diesem die Lieferung von Informationen zur Überwindung von Zugangssperren wissenschaftlich und militärisch genutzter Rechner in der Bundesrepublik Deutschland und im westlichen Ausland angeboten. Ursprünglich planten sie, ihr gesamtes Hackerwissen (Benutzernamen, Paßwörter, Rechnerrufnummern, Inhaltsbeschreibungen der geöffneten DV-Systeme etc.) zu einem Pauschalpreis von etwa 1 Mio. DM an das KGB zu verkaufen. Dieses lehnte das Angebot jedoch ab und übermittelte statt dessen eine "Wunschliste", die u. a. umfaßte:

- diverse Betriebssysteme im Quellcode

---

1 US-Verteidigungsministerium

2 KOMITET GOSUDARSTWENNOJ BESOPASTNOSTI
= Komitee für Staatssicherheit

- Compiler und Fertigungssteuerungen
- verschiedene CAD-Programme
- Informationen aus militärisch genutzten US-amerikanischen Informationstechnologie (IT)-Systemen und Datenbanken

Die drei Hacker gelangten mit ihren heimischen Rechnern über das normale Telefonnetz in das (früher von der Deutschen Bundespost betriebene) DATEX-P-Netz und "logten" sich in dort angeschlossene Rechner ein. Das Eindringen in fremde DV-Systeme wurde ihnen nicht zuletzt dadurch sehr erleichtert, daß in zahlreichen Fällen die vom Hersteller installierten Standard-Benutzerkennungen und -Paßwörter (trotz ausdrücklich anderslautender Empfehlung) nicht geändert worden waren. Dabei konzentrierten sie sich im wesentlichen auf Rechnersysteme eines bestimmten Herstellers. In anderen Fällen gelang das "Login" durch das "Spiel" mit häufig verwendeten Paßwort-Kombinationen (sog. Standard-Kombinationen). Im Erfolgsfalle wurden die Dateien im geöffneten Rechner gezielt nach weiteren "Login's" abgesucht. Die Suche erstreckte sich insbesondere auch auf (lokale und nicht-lokale) Netzverbindungen der Rechner.

Im einzelnen wurde u. a. folgendes Verratsmaterial an das KGB geliefert:

- eine Magnetbandkassette mit dem Entwicklungssystem für eine Computersprache
- eine Vielzahl von Programmen im Quellcode
- ein Softwarepaket zur Sicherung der in einem bestimmten Rechnersystem gespeicherten Daten gegen unberechtigte Zugriffe (reine Entwicklungskosten ca. 650.000,-- DM)
- Hinweise auf Datenbanken in den USA, die Angaben über toxikologische Verfahren, Dekontaminationszonen nach A-Waffen-Einsätzen, Nervengifte und C-Waffen enthielten
- eine Liste aller (ca. 4.000 bis 6.000) über die US- amerikanischen Datennetze ARPANET und MILNET verbundenen IT-Systeme

Als Gegenleistung erhielten die Hacker vom KGB insgesamt rund 90.000,-DM. Die Bezahlung erfolgte jeweils, nachdem Experten der Moskauer KGB-Zentrale die Lieferungen überprüft und ihren Wert eingeschätzt hatten.

Als Resümee aus diesem Fall bleibt festzuhalten, daß den Tätern der erfolgreiche Angriff auf IT-Systeme nicht zuletzt durch organisatorische Mängel und Nachlässigkeiten der Nutzer erleichtert worden war. Es kann wohl davon ausgegangen werden, daß sich das Sicherheitsbewußtsein der Computernutzer seither nicht unerheblich gesteigert hat. Andererseits sind es nach wie vor in erster Linie individuelle Bequemlichkeit oder grenzenloser Leichtsinn, die das kriminelle Wirken der Datenspione nachhaltig fördern bzw. überhaupt erst ermöglichen. Dabei sollte im übrigen nicht außer acht gelassen werden, daß sich - in Anbetracht der rapiden Weiterverbreitung von Informationstechniken und weltweiter Netzstrukturen - das Angriffsrisiko in letzter Zeit drastisch erhöht haben dürfte.

1.3 Andere Computerspionage-Fälle

Der "KGB-Hacker-Fall" war nicht zuletzt aufgrund der Selbstanbietung der Täter überhaupt "ins Rollen" gekommen. Das KGB war seinerzeit noch dringend auf die Unterstützung westlicher "Computer-Freaks" angewiesen, da sowohl der Ausbildungsstand als auch das informationstechnische Niveau des einstigen Ostblocks gravierende Defizite aufwiesen.

Es soll an dieser Stelle allerdings nicht unerwähnt bleiben, daß es der technischen Aufklärung des ehemaligen "Ministeriums für Staatssicherheit" (MfS) der früheren DDR im selben Zeitraum (1987 - 1989) gleichwohl gelungen war, in satellitengestützte Datenfernübertragungsverbindungen einzudringen und den dort aufgefangenen Datenverkehr bestimmten internationalen Wirtschaftsunternehmen zuzuordnen.

Vergleichbar spektakuläre Sachverhalte sind in der Folgezeit nicht mehr öffentlich bekanntgeworden. Dies mag gleichermaßen auf das geringe Entdeckungs-

risiko der Täter wie auf die ausgeprägte Neigung Betroffener zurückzuführen sein, Schadensfälle herunterzuspielen bzw. nicht publik zu machen. Es hat sich allerdings gezeigt, daß die EDV mittlerweile in "normalen" Spionagefällen immer häufiger entweder als unmittelbares Zielobjekt oder doch zumindest als (logistisches) Hilfsmittel eine Rolle spielt.

Um die Ausspähung moderner Informations- und Kommunikationstechnik bemühten sich fremde Nachrichtendienste schon in der Vergangenheit in besonderer Weise. Das Interesse der in diesem Bereich angesiedelten Agenten richtete sich auf nahezu sämtliche Details dieses Hochtechnologiebereichs und umfaßte komplette Hardware-Konfigurationen ebenso wie DV-Zubehör, Baupläne für Chips und Schaltkreise oder Unterlagen über neueste Software-Entwicklungen. Welche Dimensionen Spionageaktivitäten auf diesem Sektor einnehmen können, folgt z.B. daraus, daß der einstigen DDR-Computerindustrie durch die Verratstätigkeit von nur zwei Personen ein Kostenvorteil von mehreren hundert Millionen Mark erwachsen war. In ähnlichen Größenordnungen dürfte sich der Schaden bewegen, wenn angeworbene Agenten mehr oder weniger zufällig zu DV-Insidern werden. Der zum Systemverwalter und gleichzeitigen Sicherheitsadministrator in einem Bundeswehr-Rechenzentrum oder der zum leitenden Motorenbau-Entwicklungsingenieur mit unbeschränkter Zugriffsberechtigung auf alle firmeninternen Technik-Datenbanken aufgestiegene Spion brauchte im Rahmen seiner geheimdienstlichen Tätigkeit lediglich die ihm offiziell eingeräumten Befugnisse möglichst exzessiv wahr-zunehmen, um nahezu das gesamte Know-how seines Arbeitgebers "abzuräumen".

Heutzutage - nach dem Wegfall des "Eisernen Vorhangs" - werden Kommunikationsleitungen an der Ost-West-Grenze nicht mehr willkürlich abgeschnitten. Zudem bestehen nach der Aufhebung der Cocom-Bestimmungen so gut wie keine Beschränkungen mehr bezüglich des Exports neuester DV-Technologien nach Osteuropa. Auch wenn diese Entwicklung grundsätzlich als positiv zu begrüßen ist, sollte nicht außerachtgelassen werden, daß sie die Aktivitäten fremder - östlicher - Nachrichtendienste auf dem Gebiet der Computerspionage nachhaltig erleichtert. Aktuelle Anhaltspunkte deuten daraufhin, daß ins-

besondere die russischen Dienste für elektronische Aufklärung (FAPSI)[3] sowie für Militärspionage (GRU)[4] dabei sind, sich schwerpunktmäßig auf die Informationsbeschaffung aus Computernetzen einzurichten. So hat sich z.B. FAPSI in den letzten Jahren wiederholt - sowohl "unter offener Flagge" wie unter verschiedenen Abtarnungen - auf "Einkaufstour" ins westliche Ausland begeben, um ganz gezielt neueste Entwicklungen der Computer- und Telekommunikationsindustrie zu erwerben. Neben Produkten der EDV-Sicherheit (Verschlüsselungshard- und software, Zugriffskontrollsysteme, Virensuchprogramme etc.) ging es dabei vor allem auch um solche DV-Komponenten, die die Einsatzbereitschaft von Computeranlagen gewährleisten und störende Fremdeinflüsse eliminieren sollen. Hinsichtlich der GRU ist kürzlich bekanntgeworden, daß diese eine neue Organisationseinheit speziell für Zwecke der Computerspionage aufgebaut haben soll. Bemerkenswerterweise engagiert sich eine ganze Reihe im Bundesgebiet ansässiger sog. gemischter - deutsch/ russischer - Firmen auf dem Sektor der Kommunikations-/Computertechnik. Auffällig ist ferner, daß sich immer mehr an Legalresidenturen[5] im westlichen Ausland eingesetzte russische ND-Angehörige als Internet-Nutzer betätigen. Sogar in der Russischen Föderation selbst nimmt die Anzahl der mit einem offiziellen Internet-Anschluß versehenen Universitäten, Forschungsinstitute und anderen Einrichtungen ständig zu. Die Vorstellung, daß russische Agenten direkt aus ihrer Zentrale heraus über internationale Computernetz-werke in die Datenbanken ausländischer Zielobjekte einzudringen versuchen, muß in der Zwischenzeit als durchaus realistisches Szenario ins Kalkül gezogen werden.

Da mittlerweile auch die Möglichkeit der Spionage durch befreundete - gar militärisch verbündete - Staaten nicht mehr von vornherein ausgeschlossen werden kann, verdienen vor allem Berichte zum US-amerikanischen (Technik-)

---

3 FEDERALNOYE AGENTSTVO PRAVITELSTVENNOY SVYAZI INFORMATSII = Bundesagentur für staatliches Nachrichten- und Informationswesen

4 GLAVNOE RAZVEDIVATELNOE UPRAVLENIYE GENERALNOVO SHTABA = Hauptverwaltung Aufklärung des Generalstabs

5 Mit hauptamtlichen Mitarbeitern besetzter Stützpunkt eines fremden Aufklärungsdienstes innerhalb einer offiziellen Institution (z.B. Botschaft/Konsulat) im Operationsgebiet.

Abhördienst NSA[6] besondere Beachtung. Die NSA verfügt derzeit noch als Relikt des "Kalten Krieges" über verschiedene Überwachungsstationen auf dem Territorium der alten Bundesländer. Diesem Dienst wird nachgesagt, er habe sich mit Hilfe des Softwareprogramms "Promis" zum absoluten Supervisor des internationalen Datenverkehrs aufgeschwungen. Nach den ursprünglichen Intentionen der Herstellerfirma Inslaw war dieses Programm entwickelt worden, um eine schleppnetzartige Suche in Datenbanken, Netzwerken und sonstigen Datenbeständen zu ermöglichen, wobei der besondere Vorteil in speziellen Verknüpfungsoptionen der gefundenen Daten bestand. Durch geschickte Manipulationen des amerikanischen (und des israelischen) Geheimdienstes sei "Promis" dahingehend "optimiert" worden, daß es sich unsichtbar in andere Programme einniste und bei Computern, die es geladen hätten, ermögliche, sich unbemerkt von außen anzapfen zu lassen. Über unverdächtige Tarnfirmen sei "Promis" weltweit als vorgebliches Datenmanagementprogramm vertrieben und in einer Vielzahl von Fällen auch installiert worden.

1.4 Täterbild

Fremde Nachrichtendienste, die IT-Systeme angreifen, zielen in erster Linie darauf ab, möglichst unbemerkt die darin enthaltenen Informationen zu erlangen. Weiterhin kann es - unter den Stichworten Desinformation und Sabotage - aber auch um die Veränderung bzw. Vernichtung von Speicherinhalten gehen.

Als Täter kommen sowohl Innen- wie Außentäter in Betracht. Beim Außentäter handelt es sich um eine Person, die nicht über einen legalen Zugang zu DV-Anlagen verfügt. Primär versucht dieser Täter, über Datenleitungen/externe Anschlüsse in das System einzudringen; dies ist die typische Vorgehensweise von Hackern. Daneben legen es Außentäter aber auch darauf an, sich einen direkten Zugang zu den Anlagen und Speichermedien zu verschaffen. Im Erfolgsfall sind sie in der Lage, Speichermedien zu entwenden oder zu vervielfältigen. Dabei wird der Einbruch in ein gut gesichertes Rechenzentrum in aller

---

6 NATIONAL SECURITY AGENCY

Regel sehr viel diffiziler zu bewerkstelligen sein als der Diebstahl eines einzelnen PC oder Laptops. Grundsätzlich dürfte aber schon die kurzfristige Besitzentziehung - wie etwa anläßlich der Zollkontrolle bei der Einreise nach China oder Rußland - völlig ausreichend sein, um den kompletten Festplatteninhalt eines Laptops auf einen anderen Speicher zu übertragen. Im Zusammenhang mit China wird ferner berichtet, daß dort die Duplizierung des Speichermediums gelegentlich auch im Auto erfolge. Während der Geschäfts-reisende mit seinen einheimischen Gastgebern im Restaurant speise, "kümmere" sich der Fahrer um die im Auto zurückgelassenen Notebooks oder Laptops.

Innentäter sind demgegenüber mit einer teilweisen oder umfassenden Zugriffsberechtigung ausgestattet, die sie bei ihren Angriffen auf das System mißbräuchlich ausnutzen. Da sie etwaige Außensicherungen nicht zu überwinden brauchen, sind sie in einer sehr viel günstigeren Ausgangsposition als der Außentäter. Ein privilegierter Innentäter, dem beispielsweise die umfassenden Zugangsrechte eines Systemverantwortlichen zustehen, ist in der Lage, sich nahezu unbegrenzte Informationsmöglichkeiten zu erschließen. Präzedenzcharakter nimmt in diesem Zusammenhang zweifellos der bereits weiter oben angesprochene Fall des Spions im Bundeswehr-Rechenzentrum ein. Wenn schon das Entdeckungsrisiko des durchschnittlichen Innentäters als eher gering anzusehen ist, so gestaltet sich die Enttarnung eines derart hochwertig plazierten Agenten noch weitaus schwieriger. Dies mag vielleicht auch eine Erklärung dafür sein, daß etwa 80 % aller einschlägigen Handlungen von den sich äußerst sicher fühlenden Innentätern verübt werden.

1.5 Fazit/ Konsequenzen

Im Grundsatz bleibt festzuhalten, daß das Mißbrauchsrisiko und dabei insbesondere auch die Ausspähungsgefahr beim Betrieb von DV-Anlagen als unverhältnismäßig hoch zu bewerten sind. Dabei bewegt sich - in Anbetracht der enormen Informationsdichte in der EDV - auch die jeweilige Schadenshöhe auf überdurchschnittlichem Niveau.

Als wirksamste Gegenmaßnahme empfiehlt sich vor allem die Vorbeugung. Unter diesem Aspekt hat sich der amtliche Geheimschutz - als präventive Spionageabwehr - schon frühzeitig mit der Thematik befaßt. In den bereits 1980 vom Bundesminister des Innern herausgegebenen "Richtlinien für den Schutz von Verschlußsachen in der automatisierten Datenverarbeitung" (Richtlinien für Daten-VS) sowie in den 1987 erlassenen "Richtlinien für die Übertragung von Verschlußsachen auf Fernmeldewegen sowie für die Abstrahlsicherheit von elektrischem Gerät zur Übertragung, Be- oder Verarbeitung von Verschlußsachen" (VS-Fernmelderichtlinien/VS-FmR) sind die einschlägigen Absicherungsmaßnahmen zusammengefaßt. Zweifelsohne wurden diese Vorschriften zumindest teilweise von der technischen Entwicklung überholt. Das Inkrafttreten entsprechender Nachfolgeregelungen ist bereits absehbar. Zum gegenwärtigen Zeitpunkt können allerdings beide Anweisungen nach wie vor als Ausgangsbasis für Sicherheitsüberlegungen herangezogen werden. Dabei braucht sich ihr Anwendungsbereich im übrigen keineswegs - von ihrer Bezeichnung her - auf den Schutz von ***Verschlußsachen*** zu beschränken, sondern sollte sich ebenso auf die Absicherung offener - vergleichbar empfindlicher - Informationen erstrecken.

Vor diesem Hintergrund werden in der nachfolgenden Darstellung Schwachstellen der EDV umfassend aufgezeigt und gleichzeitig Empfehlungen für entsprechende Schutzmaßnahmen gegeben.

Das primäre Ziel dieser Ausarbeitung geht dahin, die vielfältigen Sicherheitsrisiken der modernen EDV möglichst lückenlos aufzuzeigen. Jedoch wird es nicht

möglich sein, umfassende Schutzkonzepte für sämtliche denkbaren Risikoszenarien darzustellen. Angesichts der Komplexität der Thematik würde dies den vorgegebenen Rahmen dieser Schrift bei weitem sprengen. Im übrigen spielen gerade bei DV-Absicherungsmaßnahmen die individuellen Gegebenheiten des jeweiligen Einzelfalls eine ganz entscheidende Rolle.

Diese Schrift widmet sich ausschließlich dem Thema "DV-Sicherheit". Insofern soll sie nicht zuletzt Sicherheitsverantwortlichen aus der Industrie als Ratgeber bei der Erarbeitung eines innerbetrieblichen Informationsschutzkonzepts dienen. Schließlich kommt der "DV-Sicherheit" heutzutage eine zentrale Rolle bei jedweden Überlegungen zum Informationsschutz zu.

2. Hardware

2.1. Die verschiedenen Systeme

Jeder, der sich mit DV-Sicherheit befaßt, wird sehr schnell erkennen, daß dieses Kriterium eng verzahnt ist mit der technischen Entwicklung; und zwar sowohl in Bezug auf die Fortentwicklung der Systeme als auch im Hinblick auf die rapide Verbreitung der EDV insgesamt. Anders ausgedrückt: Die Absicherung eines einzelstehenden Großrechners aus dem Jahr 1975 ist weitaus einfacher zu bewerkstelligen als die Absicherung eines weitläufigen Client-Server-Systems (mit externen Anschlüssen) von 1992.

2.1.1 Entwicklungen (zeitlich)

1969: Aufbau des militärischen ARPA-Netzes (Keimzelle des heutigen Internet); 1974: Festlegung auf die Protokolle TCP / IP; Anfang der 80er-Jahre: Verbindung des Wissenschaftsnetzes CSnet über Gateways mit dem ARPAnet; Ende der 80er- Jahre: Übergang zum NSFnet

1970: Einführung der 4. Computergeneration -Großrechner- (Mainfraime); in den USA entstehen im Unversitätsbereich erste lokale Netze

1971: Die ersten weltweiten Verbundnetze werden in Betrieb genommen

1975: Der erste Mikrocomputer (ATARI 8800) kommt auf den Markt, es entstehen die ersten lokalen Netzwerke zur Kommunikation in internen Rechnerverbundsystemen

1981: PC-Systeme

1984: Einführung des Bildschirmtext-Systems in der Bundesrepublik Deutschland

1988: Aufkommen vernetzter PC-Systeme (Client-Server-Lösungen)

1989: (März) Einführung von ISDN durch die damalige Deutsche Bundespost Telekom

1990: Verbreitung mobiler PC-Systeme (Datenbanktaschenrechner, Laptop, Notebook)

***1991**:* Erster öffentlicher Breitbanddienst für die Kopplung von privaten Hochgeschwindigkeitsnetzen und -einrichtungen in der Bundesrepublik Deutschland

***1995**:* Multimedia-Hardware (Integration von Daten, Sprache, Bildern)

2.1.2 Entwicklungen (problemorientiert)

Die schematisch dargestellten Entwicklungssprünge in der Informations- und Kommunikationstechnik (IuK) führten insbesondere durch Dezentralisierung und Downsizing zu einer drastischen Erhöhung der Gefahren und Bedrohungen der DV-Systeme. Über vernetzte Systeme können heute praktisch weltweit Informationen abgerufen werden. Außerdem enthalten verteilte Systeme fast an allen Stellen sensible und somit lokal schutzbedürftige Informationen. IT-Sicherheitsmaßnahmen aus dem Bereich der Großrechneranwendung konnten jedoch nicht im gewünschten Umfang dezentralisiert werden. In dezentralen Anwendungen fehlen deshalb häufig infrastrukturelle, technische und organisatorische Vorausssetzungen zur Realisierung von IT-Sicherheitsforderungen. Die dort eingesetzten Systemadministratoren sowie das Betriebspersonal haben vielfach nur geringe Kenntnisse über mögliche Sicherheitsfunktionen und -mechanismen. Dies führt häufig dazu, daß vorhandene Sicherheitseinrichtungen nicht oder nur zum Teil genutzt werden. Sicherheitsfunktionalitäten, insbesondere in Weitverkehrsnetzen, hinken den betrieblich-technischen Entwicklungen deutlich hinterher. Die turbulente Entwicklung im Hardware-, Software- und Netzbereich nach dem Motto "höher, weiter, schneller" läßt kaum die Möglichkeit zu, Sicherheitslücken und Manipulationsschwachpunkte zu erkennen und wirksam zu bekämpfen.

2.1.3 Die Systeme im einzelnen

- Hardware:

Physikalisch materielle Teile eines Computersystems, die nicht verändert oder kopiert werden können.

* *Großrechner*: verfügen über jegliche moderne technische Möglich keit in Kapazität, Peripherie, Rechneranschluß, Datenfernübertragung

* *MDT*: mittlere Datentechnik, ältere Bezeichnung für mittlere und kleinere Datenverarbeitungssysteme

* *Mikrocomputer*: selbständiger Rechnertyp, dessen Merkmale im wesentlichen durch die Art der Mikroprozessoren bestimmt sind, aus denen er sich ableitet (auch Personal-, Home- und Arbeitsplatzcomputer)

* *Workstation*: Rechner in einem Rechnernetz, der nicht als Server dient, sondern die normalen Leistungen eines Rechners für einen Anwender oder Benutzer erbringt

* *Server*: Rechner in einem Verbundsystem oder in einem Netz, der besondere Leistungen übernimmt (z.B. Datenbank-, Kommunikations-, Druckserver)

* *Client*: Arbeitsplatz-PC in einem Client-Server-Netzwerk

- Software:

Gesamtheit oder Teil der Programme für Rechensysteme, wobei die Programme zusammen mit den Eigenschaften der Rechensysteme den Betrieb der Systeme (Betriebssystem), die Nutzung der Systeme zur Lösung gestellter Aufgaben oder zusätzliche Betriebs- und Anwendungsarten ermöglichen (Anwendungssoftware) - Definition nach DIN 44 300 -

.

- Firmware:

Bei mikroprogrammierbaren Rechenanlagen bezeichnet Firmware die Menge aller in einem Prozessor realisierten Programme, die den Befehlsvorrat des Prozessors bestimmen.

- Netz:

System von Leitungen oder Verbindungen, die Rechnersysteme verbinden, um innerhalb dieser kommunizieren zu können:

* *LAN*: Local Area Network; inhouse-Netze, die die Vorteile der Verknüpfung von zentraler, konsistenter Datenhaltung, kostengünstiger gemeinsamer Nutzung teurer

Ressourcen und Gestaltungsfreiheit dezentraler Arbeitsplatzrechner ermöglichen

° *Peer-To-Peer*: Verknüpfung von lokalen Arbeitsplatzrechnern in einem kleinen Netzwerk (max. 40 Benutzer) ohne Servereinsatz; die Steuerung des Netzes erfolgt über Software (Groupware); jeder Rechner im Netz kann den anderen Rechnern Dateien oder Drucker zur Verfügung stellen; Peer-Programme sind eigentlich Netzwerkzusätze für das nicht kommunikationsfähige Betriebssystem MS-DOS

°° *Client/Server*: im lokalen Netz stellt ein spezialisierter PC (Server) dem Arbeitsplatz-PC (Client) seine Festplatte zur Erledigung zentraler, einheitlicher Abläufe zur Verfügung; die Steuerung des Netzes erfolgt über spezielle Netzwerkbetriebssysteme auf den Servern

°° *CN*: Corporate Networks, Behörden- und Unternehmenseigene (private) Kommunikationsnetze

* *MAN*: Metropolitan Area Network als öffentliche Breitbanddienste auf der Basis der Fast-Packet-Technologie; dienen der Kopplung von privaten Hochgeschwindigkeitsnetzen

* *WAN*: Wide Area Network zur (weltweiten) Kopplung von Rechnersystemen und Netzen (z.B. ISDN, Internet)

-Sonstige (periphere) IT-Geräte:

* *USV*: unterbrechungsfreie Stromversorgung

* *NEA*: Netz-Ersatz-Anlage

* *Kryptogeräte:* Geräte zur Ver- und Entschlüsselung von Daten (intern und extern)

-Sprachkommunikation:

* *TK-Anlagen*: Telekommunikationsanlagen, d.h. digitale Telefon- (Nebenstellen-) Anlagen

* *CTI:* Computer-Telefon-Integration, d.h. computerunterstützte Telefonie mit Visualisierung von Telefonievorgängen

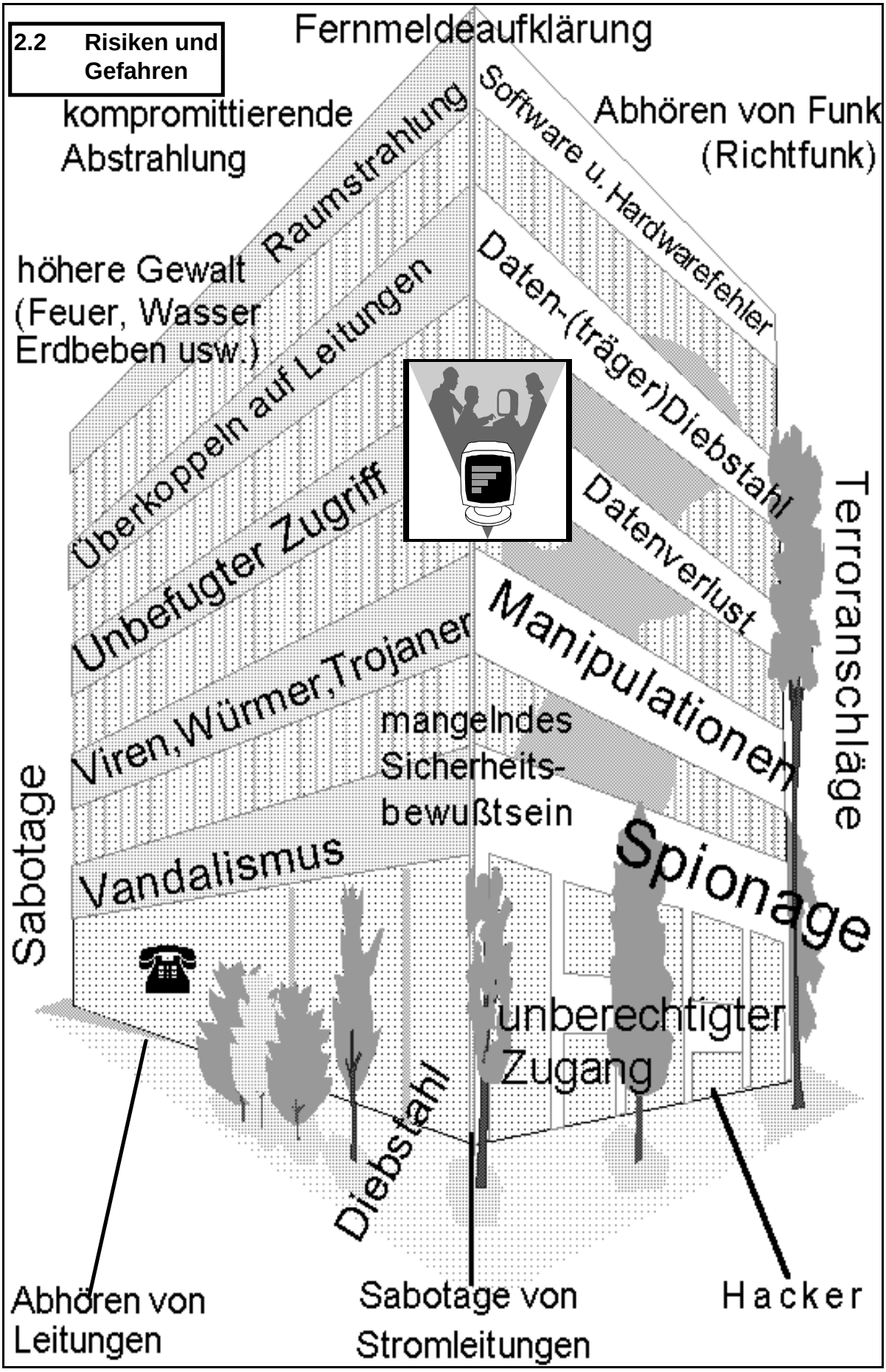
**Telefon / Fax / Anrufbeantworter*

Die im folgenden dargestellten Bedrohungen und Risiken für Systeme der Informationstechnologie (IT) und die Sicherheits- und Schutzmaßnahmen zur Vermeidung von Schadensfällen bzw. zur Minderung des verbleibenden Restrisikos beim Betrieb solcher Anlagen ***orientieren sich schwerpunktmäßig*** an den vernetzten PC-Systemen. Sicherheitsempfehlungen für die Bereiche Großrechner (Rechenzentrumsbetrieb), Datenfernübertragung (Telekommunikation) und sonstige schutzbedürftige Teile von IT-Systemen (Datenträger, Stromversorgung, personelle und organisatorische Maßnahmen) sollen das Bild abrunden.

Ziel ist es, die Sicherheitsverantwortlichen in Behörden und Wirtschaftsunternehmen auf Risiken in der IT hinzuweisen, Schutzmaßnahmen aufzuzeigen und in Teilbereichen Entwicklungen und Diskussionen zur Erhöhung der IT-Sicherheit anzuregen. Es wird jedoch darauf hingewiesen, daß allgemeine Aussagen, wie sie dieser Broschüre zugrundeliegen, einzelfall- und objektbezogen in einem IT-Sicherheitskonzept erfaßt werden sollten. Hierbei wirkt im allgemeinen das Bundesamt für Sicherheit in der Informationstechnik beratend mit und leistet die erforderlichen Hilfestellungen. Auf Landesebene wird diese Aufgabe grundsätzlich von der jeweiligen Landesbehörde für Verfassungsschutz wahrgenommen.

Die Bekämpfung der nachrichtendienstlich gesteuerten Computerspionage ist eine originäre Aufgabe der Verfassungsschutzbehörden.

2.2 Risiken und Gefahren



2.2.1 Einführung in die verschiedenen Kategorien der Bedrohungen

Das bereits dargestellte Bedrohungsszenario für Systeme der IT ist zwangsläufig unvollständig; es soll lediglich exemplarisch potentielle Gefahren und Risiken aufzeigen. Eine sehr anschauliche und ausführliche Beschreibung der Bedrohungssituationen findet sich u.a. im IT-Sicherheitshandbuch des "Bundesamts für Sicherheit in der Informationstechnik" (BSI) - vgl. Anhang. Nach allgemeiner Auffassung lassen sich die verschiedenen Arten der Bedrohung zunächst grob in drei Kategorien einteilen:

1. ***Verlust der Vertraulichkeit (Spionageaspekt)***
2. ***Verlust der Integrität (Sabotageaspekt)***
3. ***Verlust der Verfügbarkeit (Funktionsverlust)***

Eine ***4. Kategorie*** - ***Verlust der Authentizität*** - (Echtheitsbeweis von Daten und Dokumenten) gewinnt im elektronisch unterstützten Rechts- und Zahlungsverkehr zunehmend an Bedeutung.

Im Mittelpunkt dieser Broschüre steht der Schutz gegen nachrichtendienstliche Angriffe und demzufolge die Darstellung möglicher Gefahren, Risiken und Schwachstellen, die erfahrungsgemäß von Computerspionen ausgenutzt werden. Die ergänzend aufgezeigten Abwehrmechanismen entfalten ihre Schutzwirkung selbstverständlich auch im Hinblick auf die übrigen Bedrohungskategorien. Sämtliche Bemühungen, Computerspione abzuwehren, sind darüber hinaus geeignet, andere unbefugte Zugriffe (beispielsweise im Sinne des Datenschutzrechts) zu erschweren bzw. zu verhindern.

2.2.2 Sicherheitskonzepte

Der Prozeß von der Erfassung allgemeiner Bedrohungen bis hin zum Ziel eines individuellen Sicherheitskonzepts, das allen Bedürfnissen des jeweiligen IT-Anwenders gerecht wird, ist nur durch eine ***strukturierte Systemanalyse*** effizient und erfolgversprechend zu realisieren. Diese orientiert sich zweckmäßigerweise

am IT-Sicherheitshandbuch des BSI.
Zur Ermittlung der Schutzbedürftigkeit des IT-Systems ist zunächst eine ***IST-ERFASSUNG*** der IT-Anwendungen und der zu verarbeitenden Informationen erforderlich, die für die Behörde oder das Unternehmen von Bedeutung sind und deshalb geschützt werden müssen. Die anwendungsorientierte Sicht dieses Vorgehens trägt maßgeblich zu einer Transparenz des Verfahrens gegenüber sämtlichen Beteiligten (IT-Anwender, Nutzer, Mitarbeiter, Verfahrensbeteiligte, Führungskräfte, Sicherheitsverantwortliche etc.) bei.

Nach Erfassung der IT-Anwendungen muß der mögliche ***Schaden bewertet werden*** (z.B.: unbedeutend, gering, mittel, groß, existenzgefährdend, in DM-Abstufungen oder nach Geheimhaltungsgraden von offen bis STRENG GEHEIM). Hierbei werden die angestrebten ***Schutzziele definiert***.

Daran schließt sich eine ***BEDROHUNGS-ANALYSE*** an, bei der alle vorstellbaren Bedrohungen ermittelt werden, die Schäden am IT-System verursachen könnten. Im Rahmen dieser Analyse wird der Bezug zwischen den gefährdeten Objekten in den Teilbereichen des IT-Systems (Infrastruktur, Hardware, Datenträger, Paperware, Software, Anwendungsdaten, Kommunikation, Personen) und den im einzelnen den Objekten zuzuordnenden Bedrohungen erfaßt (Schwachstellenanalyse). Je genauer Objekte und Bedrohungen festgehalten werden, desto höher ist der Aufwand dafür. Für ein abgestuftes Sicherheitskonzept, insbesondere wenn hohe Werte zu schützen sind, ist dieses Verfahren jedoch unumgänglich.

Im Rahmen der folgenden ***RISIKO-ANALYSE*** werden die zuvor ermittelten Bedrohungen hinsichtlich ihres Schadensausmaßes (Höhe, Häufigkeit) bewertet. Der solchermaßen herausgearbeitete ***IST-Zustand*** der IT-Sicherheitsmaßnahmen bildet die Basis zur Ermittlung des gewünschten ***SOLL-Zustands*** an Sicherheit. Erfahrungsgemäß hat sich hier bewährt:

- Festlegung risikopolitischer Vorgaben durch die Geschäftsleitung

- Festlegung der Risikoprioritäten und eine Quantifizierung der risikopolitischen Ziele

- Einbeziehung der Risikokomponenten bei unternehmerischen Entscheidungen

- Kontrolle der risikopolitischen Maßnahmen hinsichtlich ihrer Wirksamkeit und ihres ökonomischen Nutzens

- Prüfung der Ausgewogenheit, Praktikabilität und jederzeitigen Wirksamkeit der Schutzmaßnahmen

Bei der Erstellung des IT-Sicherheitskonzepts ***(Abgleich)*** werden nun Maßnahmen ausgewählt, die geeignet sind, die Risiken auf ein erträgliches Maß zu reduzieren. Das Zusammenspiel der getroffenen Maßnahmenauswahl und die Auswirkungen auf die betriebliche Praxis müssen hierbei mit berücksichtigt werden. Eine Wirtschaftlichkeits- (Kosten/Nutzen-) Analyse gibt Aufschluß darüber, ob die Maßnahme im Einzelfall auch angemessen ist. Die noch verbleibenden Restrisiken werden erfaßt und die Tragbarkeit begründet.

Die endgültige risikopolitische Entscheidung muß von der Firmenleitung bzw. Behördenspitze getroffen werden.

Das hier vorgestellte Verfahren zur Erstellung eine IT-Sicherheitskonzepts kann und muß individuell auf die Bedürfnisse der einzelnen Behörde oder des Unternehmens angepaßt werden. Die genau festgeschriebene Vorgehensweise ist nicht in jedem Fall geeignet, komplexe Systeme zu analysieren. Bei vielen Anwendern steht der Aufwand zur Durchführung dieser Analyse in keinem Verhältnis zum angestrebten Schutzziel bzw. zu den zu schützenden Objekten. Der Umfang der Bedrohungs- und Risikoanalyse sollte in engem Bezug zur tatsächlichen Schutzbedürftigkeit der vom Anwender ausgewählten IT-Bereiche stehen. Schutzmaßnahmen für vergleichbare IT-Anwendungen, insbesondere im Bereich der sog. Kleinanwender (Stand-Alone-PC, kleinere LAN), müssen - losgelöst von diesem Verfahren - mit personellen, organisatorischen, infrastrukturellen und technischen Maßnahmen stärker standardisiert werden. Das BSI hat diesem Anliegen mit der Erstellung des ***IT-Grundschutzhandbuchs*** bereits

Rechnung getragen. Bei der eigenständigen Erarbeitung eines IT-Sicherheitskonzepts empfiehlt sich die strikte Beachtung dieses Handbuchs. Dadurch ist gewährleistet, daß (fast) alle schutzwürdigen Belange Berück-sichtigung finden. Bei der Absicherung von IT-Anlagen zum Schutz von Verschlußsachen sollte jedoch die Anwendung und Durchführung des Verfahrens mit der jeweiligen für die Beratung zuständigen Behörde abgestimmt werden. Diese kann außerdem objektbezogene (vereinfachte) Sicherheitskonzepte auf der Basis der gültigen Rechtsvorschriften erstellen, die sich am konkreten Bedarf des Nutzers orientieren.

2.3 Bedrohungen und Schutzmaßnahmen anhand ausgewählter Beispielsfälle

2.3.1 Diebstahl

- Im März 1996 brachen unbekannte Täter in ein deutsches Universitäts-Rechenzentrum ein. Aus 40 Pentium-Rechnern wurden gezielt die Rechnerprozessoren, Arbeitsspeicher und Festplatten entwendet. Allein der Materialschaden belief sich auf ca. 100.000 DM. Der immaterielle Schaden, der sich aus dem Datenverlust, dem Aufwand für die Rekonstruktion der Daten und dem Ausfall der Systeme ergab, konnte nicht beziffert werden. Bemerkenswert hierbei ist, daß bereits vor zwei Jahren ebenfalls durch Diebstahl von Rechnern und Komponenten ein Schaden von etwa 200.000 DM entstanden war.

- Bei einem Landesministerium wurden während des Umzugs in ein neues Dienstgebäude die Netz-PC provisorisch in einem Lagerraum (Tür mit Bauzylinderschloß gesichert) deponiert. Anläßlich der späteren Installation wurde festgestellt, daß 3 PC und die dazugehörigen Drucker verschwunden waren. Unbekannte Täter hatten die Tür fachmännisch nachgeschlossen und die Geräte entwendet.

- Bei einem Großhandelsunternehmen wurden während der Mittagspause 16 Rechner aus den im Erdgeschoß gelegenen Büros von unbekannten Tätern

abgebaut, durch die Fenster auf einen auf dem Bürgersteig abgestellten Pritschenwagen verladen und abtransportiert. Obwohl Mitarbeiter des Unternehmens diese Vorgänge bei der Rückkehr aus der Mittagspause beobachteten, blieben die Täter unbehelligt. Neben dem Sachwerteverlust entstand durch den Datenverlust und den Umstand, daß Disketten mit Sicherungsdaten, die am Arbeitsplatz gelagert wurden, ebenfalls karteikastenweise "mitgenommen" wurden, ein beträchtlicher Schaden.

- Mitte 1996 waren bei einer großen Landesbehörde mehrere Softwarediebstähle zu verzeichnen. Dabei wurde Standardanwendungssoftware entwendet, die im Rechenzentrum offen gelagert war. Obwohl dort eine Gefahrenmeldeanlage installiert ist, kann nicht ausgeschlossen werden, daß es sich bei den Tätern um Externe handelt, da die Anlage außerhalb der regelmäßigen Arbeitszeit nicht scharf geschaltet worden war. Bei Nutzung der vorhandenen Technik (Gefahrenmeldeanlage, Zugangskontrollsystem) hätte sich der Kreis der Täter - auch möglicher Innentäter - zumindest eingrenzen lassen. Außerdem wären Zugänge zum Rechenzentrum zu ungewöhnlichen Zeiten - auch von Berechtigten - protokolliert worden.

Diese Liste ließe sich beliebig fortsetzen. Allein im Jahr 1995, so wird geschätzt, wurden in Industrie und Verwaltung ca. 40.000 PC entwendet. Immer häufiger muß hierbei festgestellt werden, daß nicht nur externe Täter mit teilweise sehr fundierten Orts- und Objektkenntnissen, sondern auch eigene Mitarbeiter in solche Diebstahlsfälle verwickelt sind. Neben dem eingetretenen materiellen Verlust ist von besonderer Bedeutung, daß durch Stillstand der Anlagen, Reparaturen beschädigter Komponenten, Zeitaufwand für die Rekonstruktion der Daten (sofern Datensicherungsmaßnahmen ergriffen worden sind) sowie die Neuerfassung von Daten bei Verlust und Beseitigung von Fehlern in der Hard- und Software oftmals immense Folgeschäden entstehen. Bei einer in Großbritannien durchgeführten Untersuchung gaben 14 % der befragten Unternehmen und Organisationen an, durch Hardware-Diebstahl (bei 889 verwertbaren Antworten 346 erfaßte Fälle) erhebliche finanzielle Einbußen erlitten zu haben. Die in der Bundesrepublik Deutschland durchgeführten Sicherheitsstudien bestätigen die-

sen Trend mit steigender Entwicklung. Besonders aufschlußreich ist hierbei die Tatsache, daß zwar viele Anwender das Problem erkannt haben, jedoch allenfalls bereit sind, Sicherheitsmaßnahmen im zentralen IT-Bereich zu realisieren. Bei dezentralen PC-Lösungen bestehen noch erheblich größere Defizite. Die fehlende Akzeptanz für vorhandene Sicherheitseinrichtungen, die Organisations- und Betriebsabläufe zweifelsohne auch behindern können, erzeugt Schwachstellen, die kaum zu kompensieren sind. Andererseits wird aber mit Hilfe der bereits erwähnten BSI-Handbücher und durch entsprechende Informationen und Hinweise der Sicherheitsbehörden in letzter Zeit zunehmend erreicht, daß sich DV-Anwender nicht erst im konkreten Schadensfall auf IT-Sicherheitsmaßnahmen besinnen.

2.3.2 Sabotage

Bereits 1984 kursierten in diversen Untergrundzeitschriften Anleitungen zur Sabotage von PC-Systemen. Die Möglichkeiten zur Sabotage am Arbeitsplatz wurden anhand einer ganzen Reihe "versehentlicher" Vorkommnisse und "witziger Pannen" des täglichen Lebens geschildert (die Putzfrau "Atta" stellt den flüssigen Abflußreiniger auf dem PC ab, "zufällig" kippt die Flasche um und die Chemikalie ergießt sich in die Lüftungsschlitze des Geräts; "Sally" schlürft ihren Kaffee und spuckt die leider stark versalzene Brühe aus; außerdem gießt sie versehentlich den Rest des "Gesöffs" in die Tastatur; bei einer "Selbstreparatur" versucht "Sally", zunächst den PC durch Vertauschen der Verbindungskabel zum schnelleren Arbeiten zu bewegen; als dies nichts hilft, nimmt sie einige IC aus ihren Sockeln und steckt sie andersherum wieder hinein). Bei diesem Beispiel wird zwar nicht konkret zu strafbaren handlungen aufgefordert, jedoch sind die von der „Hauptdarstellerin“ mit dem sinnigen Namen „Sa.(lly) Botage“ verursachten Schäden geeignet, den DV-Betrieb nachhaltig lahmzulegen. Sie können durchaus als Aufruf zur Nachahmung verstanden werden.

Allein in der linksextremistischen anarchistischen "Szene" kursieren bundesweit ca. 30 bedeutende Szeneblätter, die regelmäßig Sabotageanleitungen verbreiten (z.B. "radikal", Ausgabe Nr. 145 v. Februar 1992: Bauplan für eine zeitver-

zögerte Zündung von Brandsätzen), zu militanten Aktionen aufrufen und "anschlagsrelevante" Ziele veröffentlichen. Diese "Anleitungen" zur Sabotage, die sowohl für technische Laien als auch für sog. Fortgeschrittene gedacht sind, dienen dem Zweck, mit wenig Aufwand, ohne detailliertes technisches Fachwissen, mit geringem Entdeckungsrisiko und persönlicher Gefährdung der Täter möglichst großen Schaden anzurichten. Längst ist jedoch die Verbreitung solcher Sabotageanleitungen in Papierform dem praktisch weltweiten elektronischen Versand gewichen. Gerade das Internet bietet für solche Aktionen nahezu ungeahnte Möglichkeiten. Beispielhaft hierfür ist ein Maildokument aus einer Internet-Mailbox aus dem Jahr 1995, in dem auf weit über 100 Seiten detailliert beschrieben wird, wie Sprengkörper, Bomben und Selbstlaborate ge-baut werden können. Chemische, physikalische und elektrotechnische Grund-lagen, Beschaffung von Chemikalien und zusätzlichen Hilfsmitteln, Mischungsverhältnisse und Wirkungsweise werden hier ebenso genau beschrieben wie Bauanleitungen für Container und Zünder. Welche Folgen solche Sabotagehandlungen haben können, zeigt eine nur unvollständige Auflistung von Anschlägen auf Rechenzentren, Behörden und Unternehmen mit IT-Bezug in Baden-Württemberg und anderen Bundesländern:

- 20. März 1983: versuchter Sprengstoffanschlag auf die Niederlassung der Fa. IBM in **Reutlingen** durch "Revolutionäre Zellen" (RZ)

- 15. Dezember 1984: Sprengstoffanschlag auf das Regionale Rechenzentrum in **Reutlingen** durch militante Unterstützer der RAF; Sachschaden: ca. 5.000.000,-- DM

- 20. Januar 1985: versuchter Sprengstoffanschlag auf die Außenstelle der "Deutschen Forschungs- und Versuchsanstalt für Luft- und Raumfahrt " (DFVLR) und die Fa. "Rechenzentrum Bau GmbH" in **Stuttgart-Vaihingen**; bei der vorzeitigen Detonation des Sprengkörpers wurde der Täter aus dem RAF-Umfeld getötet, eine Mittäterin schwer verletzt

- 16. November 1986: Sprengstoffanschlag durch "Militante der RAF" auf das IBM-Forschungszentrum in **Heidelberg**

- 26. Februar 1990: Brandanschlag durch "Kämpfende Einheiten" auf die Schule für Kommunikations- und Datentechnik der Fa. Siemens in Bonn-Bad Godesberg

Diese Liste von Sabotageakten bildet nur die Spitze eines Eisbergs. Bis heute kann die Aufzählung mit beliebig vielen Beispiele für kleinere bis extrem hohe Schäden fortgesetzt werden. Herausragend und bezeichnend für die neue Dimension von Sabotagehandlungen sind die 1995 bzw. 1996 verübten Anschläge auf Kabelschächte der Deutschen Telekom AG im Raum Frankfurt am Main. Beim ersten Anschlag am 01. Februar 1995 wurden 7 Glasfaserkabel (3 Ortsnetz- und 4 Fernkabel) von unbekannten Tätern (mit vermutetem Insiderwissen), die sich "Keine Verbindung e.V." nannten, mit einem Bolzenschneider durchtrennt. Auf dem Frankfurter Flughafen fielen daraufhin elektronische Reservierungssysteme aus. Zudem wurden 13.000 Telefonanschlüsse von der Außenwelt abgeschnitten, darunter auch das Klinikum der Universität Frankfurt . Beim zweiten Anschlag wurden von einer Gruppierung, die sich selbst als "K.A.B.E.L.S.C.H.N.I.T.T." bezeichnete, 4 Glasfaserkabel der Telekom (Sachschaden: ca. 100.000,-- DM) und zwei Datenleitungen, die die Datennetze der Stadt Frankfurt am Main und des Rhein-Main-Flughafens verbinden, durchtrennt. Zahlreiche Telefon- und DV-Einrichtungen des Flughafens, darunter auch die der Flugsicherung und wiederum der Universitätsklinik, waren hiervon betroffen. Im Nachgang zu diesen Anschlägen wurden bereits weitere festgestellt, die offensichtlich von Nachahmungstätern verübt wurden. Augenscheinlich fehlendes Insiderwissen führte hier zu weitaus geringeren Schäden.

Das durch den Bundesrechnungshof in einem Bericht an den Deutschen Bundestag (Drucksache 11/7691 v. 28. August 1990) über die Sicherheit der Informationsverarbeitung in Rechenzentren der Bundesverwaltung getroffene Fazit

> "In Rechenzentren der Bundesverwaltung, in denen sensible kassenwirksame, personen- und auch sachmittelbezogene Daten verarbeitet werden, sind die Verfahren ***nicht hinreichend gegenüber Katastrophen oder mögliche Sabotage gesichert***. Für die eingesetzten Verfahren wurden ***keine Risikoanalysen durchgeführt***. Die daraus abzuleitenden umfassenden ***Sicherheitskonzepte fehlten***. Die ***Katastrophenschutzpläne waren unvollständig***. Die ***technische Verfügbarkeit*** der in den Rechenzentren eingesetzten Verfahren ***ist nicht immer***

> ***in ausreichendem Maße gewährleistet***. Bei Rechenzentren wiesen die ***Zugangskontrollen*** zu den einzelnen Sicherheitsbereichen ***Lükken*** auf. ***Gleiches galt für den Schutz der Programme und Daten gegen Manipulation, unberechtigte Kenntnisnahme und Datenverlust***." (Fettdruck nicht im Original)

zeigt sehr deutlich, wo (bis heute) die Schwachstellen in der Sicherheit von Rechenzentren, nicht nur im Behörden-, sondern auch im Wirtschaftsbereich, liegen. Bedrohungen, Risiken und Schäden, die durch Sabotagehandlungen mittels Software- und Programm-Manipulationen (Viren, Minen, Trojanische Pferde, Hackerangriffe u. ä.) entstehen können, werden in eigenen Abschnitten dieser Broschüre dargestellt.

2.3.3 Schutzmaßnahmen/Rechenzentren (RZ-) und PC-Sicherheit

Die Frage, die sich hier stellen muß, lautet: Werden RZ in Zukunft überhaupt noch gebraucht, und wenn ja, wie können diese aussehen?

Durch die komplexe Technologie, die Dezentralisierung von intelligenten Systemen und die Notwendigkeit, diese untereinander zu vernetzen, müssen immer größere Anforderungen an eine zentrale Datenhaltung mit Zugriffsmöglichkeiten sämtlicher Subsysteme auf alle Daten des Systems gestellt werden. Die Datenorganisation, die Verteilung der Daten, Steuerungsfunktionen für den Datenverkehr unter Berücksichtigung der jeweiligen Arbeitslast, permanente Verfügbarkeit der Systeme und Daten, redundante Maßnahmen sowie hohe Anforderungen an Datenkonsistenz und -integrität erhöhen die Anforderungen an den Großrechnerbetrieb in gesicherter Umgebung drastisch. Zusätzlich werden immer häufiger bestehende Rechenzentren weiter zentralisiert und besonders gefährdete Einrichtungen dezentraler Systeme wie z.B. Netz- und Datenbankserver von Client-Server-Lösungen an zentralen Stellen zusammengefaßt. Die neben den Sicherheitsüberlegungen auch unter dem heutigen Kostendruck (System- und Datenbestandspflege, Hardwarefehlerbehebung, Datensicherung, Softwareaktualisierung, Katastrophen-, Notfall-, Wiederanlaufplanung, hiermit verbundener Personalaufwand) notwendigen Maßnahmen sind sämtlich darauf ausgerichtet, wieder mehr zentrale Einrichtungen zu schaffen. Als Fazit bleibt

festzuhalten, daß auch in Zukunft RZ notwendig sind, und die Anforderungen an die RZ-Sicherheit neu überdacht werden müssen.

Bei der Erstellung von Sicherheitskonzepten zur baulich-technischen, elektrotechnischen, organisatorischen und personellen Sicherheit von RZ sollten folgende eventuelle Schwachstellen berücksichtigt werden:

Gebäudeinfrastruktur

Ausgehend von Überlegungen zur ***allgemeinen Sicherheitslage des Gebäudeumfelds*** wie z.B.

- freier Zugang zum Gebäude über öffentliche Wege,
- Vorhandensein eines Zauns sowie dessen Beschaffenheit und Entfernung zum Gebäude,
- kontrollierter Zugang zum Betriebsgelände (einschl. eventueller Besucher- und Mitarbeiterparkplätze),
- Erkennbarkeit des RZ - als solches - von außen,
- Einsatz von Freigeländesicherungen (Videoüberwachung, Zaunsicherungen, Bewegungsmelder, automatische Beleuchtung),
- personelle Schutzmaßnahmen (Kontrolle oder ständige Bestreifung durch Wachdienst, Werkschutz bzw. ständig/zeitweise eingesetztes Pfortenpersonal mit/ohne technische[r] Unterstützung),

und des Gebäudes, wie etwa

- kontrollierter Zugang durch technische und/oder personelle Über- bzw. Bewachung,
- Einsatz von Gefahrenmeldetechnik mit oder ohne Aufschaltung auf den Polizeinotruf,
- zusätzliche bauliche oder technische Maßnahmen der Objektsicherung

sowie des Schutzbedürfnisses für das Objekt selbst (Gefährdungslagebild, Anschlagsrisiko) können die nachfolgend näher dargestellten Grundsicherungsmaßnahmen Berücksichtigung finden (zusätzliche störende Umgebungseinflüs-

se wie Hochwasser- und Überschwemmungsgefahr, Brandlasten, Staub- und Schadstoffemissionen sowie starke elektromagnetische Abstrahlung durch umgebende Einrichtungen, Erdbebengefahr, fehlende Zugangs- oder Zufahrtsmöglichkeiten für Rettungsdienste im Notfall, die den RZ-Betrieb ebenfalls nachhaltig beeinflussen können, müssen dabei allerdings unberücksichtigt bleiben).

Der RZ-Bereich sollte möglichst in zentraler Lage (nicht im EG) im Gebäude gewählt und als Sicherheitsbereich (***Closed-Shop-Betrieb***) betrieben werden. ***Baulich*** sollte das RZ entsprechend den DIN-Vorschriften 1053, Teil 1 (***Mauerwerk*** 240 mm, Druckfestigkeitsklasse der Steine 12, Mörtelgruppe II) oder nach DIN 1045 (***Stahlbeton*** 140 mm, Güte B 25, Armierung aus einlagigen, beidseitig einzubringenden Betonstahlmatten Q 257) errichtet bzw. ertüchtigt werden. Bestehende RZ können auch durch Einbringen von Tiefziehstahlblechen ertüchtigt werden. Die Stärke der Bleche bemißt sich nach dem zu errechnenden Widerstandszeitwert. ***Türen*** zu RZ sollten in Entsprechung zum Mauerwerk nach DIN V 18 103 in einbruchhemmender Ausführung (Klasse ET 3 - Sicherung gegen Einbruchsversuche mit Hebel- und Schlagwerkzeugen - Widerstandszeitwert mehr als 10 min) eingebaut werden. Sofern notwendig, sollten ***Fenster*** ebenfalls einbruchhemmend nach DIN V 18 054 (Klasse EF 3) ausgeführt sein. Diese Fenster enthalten durchbruchhemmende ***Verglasungen*** nach DIN 52 290, Teil 3 (Klasse B 3). Zur Ertüchtigung oder Nachrüstung bestehender Objekte eignen sich auch einbruchhemmende ***Rolläden*** oder ***Gitterkonstruktionen***. Möglich sind auch **Schutzjalousien** in einbruch-, durchwurf-, durchbruch- oder sprenghemmender Ausführung. Fenster und Türen können u.U. auch mit ***Sicherheitsfolien*** ertüchtigt werden. Im allgemeinen werden durchwurfhemmende Folien nach DIN 52 290, Teil 4, eingesetzt. Wesentlich hierbei ist , daß diese sorgfältig mit dem Fenster- oder Türrahmen verbunden werden. Grundprinzip ist dabei, die Folien auf jener Seite zu verkleben, hinter der sich die zu schützenden Objekte oder Personen befinden, also überwiegend innen. Bei Fensterfolien kommt als erwünschter Nebeneffekt hinzu, daß bis zu 90 % der UV-Strahlung des Sonnenlichts absorbiert wird. Außerdem sind diese Folien auch als Alarm-Sicherheits- oder elektromagnetische Abschirmfolie erhältlich.

Als ***mechanische Grundschutzmaßnahme*** empfiehlt sich der Einsatz geprüfter, höherwertiger ***Schlösser*** (Profilzylinder nach DIN V 18 254, Klasse 2 für Innen- und Klasse 3 für Außentüren; VdS-anerkannte Profilzylinder der Klasse A - entspricht DIN Klasse 2 - oder B - entspricht DIN Klasse 3) und entsprechender ***Schutzbeschläge*** nach DIN 18 257 (Klasse ES 2 oder ES 3). Es wird angeraten, Schutzbeschläge mit Zylinderabdeckung zu verwenden, da diese einen hohen Schutz gegen die bekannte "Kernziehmethode" bieten. Beim Einsatz von Profilzylindern ist zu beachten, daß Zylinder von ***Schließanlagen*** im Vergleich zu Einzelschließungen in der Regel eine verminderte Aufsperrsicherheit aufweisen. Deshalb sollten Sicherheitsbereiche mit Schlössern, die nicht in eine Schließanlage einbezogen sind, ausgestattet werden. Angemerkt sei, daß der Schutz durch eine Schließanlage oder durch Einzelschlüssel nur dann gewährleistet ist, wenn die Nachweise über Schlüsselträger, ausgegebene Schlüssel und Zugangsberechtigungen auf dem aktuellsten Stand sind. Ebenso müssen sämtliche Reserve- und Notschlüssel in geeigneter Form verwaltet und aufbewahrt werden. Dies gilt im übrigen auch für die Ausführungen zu Zugangskontrollanlagen und deren Identifikationsträgern. Im staatlichen Geheimschutz ist die Aufbewahrung von Schlüsseln zu Stahlschränken und Räumen, in denen Verschlußsachen verwahrt werden, sowie von Gefahrenmeldeanlagen zum Schutz dieser Einrichtungen in speziellen Schlüsselbehältern vorgeschrieben.

Zur Steuerung des berechtigten Zugangs zum RZ sollten ***Zugangskontrollanlagen*** (ZKA) eingesetzt werden. Diese müssen einen erhöhten Schutz gegen Überwindungsversuche bei gleichzeitiger hoher Verfügbarkeit des Systems bieten. Damit tatsächlich nur befugten Personen der Zutritt ermöglicht wird, muß eine eindeutige Zuordnung des Identifikationsmerkmalträgers (Schlüssel, Identifikationskarte mit Codierung, PIN-Nummer oder biometrisches Kennzeichen) zu einem Benutzer gegeben sein. Diese Träger sowie die Ein- und Ausgabeeinheiten des Systems müssen gegen Auslesen geschützt sein. Sämtliche Durchgänge sind durch die ZKA auf ihren ordnungsgemäßen Zustand zu überwachen. Informationsträger, Ein- und Ausgabeeinheiten, Stellglieder und Leitungen müssen gegen Sabotage- und Zugriffsversuche gesichert werden. Zusätzliche Merk-

male wie Zeit- und Raumzonen, Doppelnutzungssperren, Personenzählungen, Zwei-Personen-Kontrolle, Durchgangsüberwachung, Parallelverschluß von Durchgängen, Flucht- und Rettungswegesteuerung, Registriereinrichtungen, Datensicherung, Batteriepufferung und Störungsanzeigen sollten realisiert werden können.

Bei der ***Planung von Türen*** (Tür-Engineering) müssen die zuvor dargestellten Schutzmaßnahmen (Einbruchschutz, mechanischer Schutz durch Schlösser, Zutrittskontrolle) mit der Fluchtwegesicherung in Einklang gebracht werden, um Schutzzielkonflikte zu vermeiden. Für ***Notausgänge*** ist vorgeschrieben, daß Verschlüsse an solchen Türen sofort - von innen - nach einer einzigen kontinuierlichen Handbewegung freigegeben werden müssen. Hierzu dürfen Schlüssel oder sonstige Hilfsmittel nicht nötig sein (§ 10 Arbeitsstättenverordnung/Arb StättVO). Gewährleistet werden kann dieses nur durch sog. Panikverschlüsse mit innenliegendem Türdrücker oder Panikstange bzw. durch elektrische Fluchtwegesysteme, die durch Knopfdruck Haltemagneten an der Tür oder am Fenster freigeben und so den Fluchtweg öffnen. Damit diese Systeme nicht mißbräuchlich verwendet werden können, sind sie in die Zugangskontrollsteuerung zu integrieren und, sofern vorhanden, durch eine Gefahrenmeldeanlage zu überwachen.

In RZ, in denen Verschlußsachen mit Hilfe der IT verarbeitet, gespeichert oder übermittelt werden, ist der Einsatz von ***Gefahrenmeldetechnik*** zwingend vorgeschrieben. Bei der Verarbeitung anderer sensibler Informationen wird der Einsatz von Gefahrenmeldeanlagen (GMA) zur Sicherung des RZ angeraten. GMA zum Schutz von Verschlußsachen müssen den Anforderungen und Prüfungen des "Verbandes der Schadensversicherer e.V." (VdS), den Bestimmungen der DIN VDE O833, den landesspezifischen Verwaltungsvorschriften für Überfall- und Einbruchmeldeanlagen mit Anschluß an die Polizei sowie den besonderen Forderungen des Verfassungsschutzes und des BSI entsprechen. Im Detail werden hier die Anforderungen für die Planung, Errichtung, den Betrieb sowie für die Auftragsvergabe und Abnahmeprüfung geregelt. Sämtliche Komponenten einer GMA - von der Zentrale über Energieversorgung, Melder, Leitungswege,

Kontakte, Schalteinrichtungen und Verteiler bis zu Übertragungsanlagen - sind geprüft und für einen Einsatz im Verschlußsachenbereich zugelassen. Auf eine detaillierte Darstellung dieser Komponenten und deren Wirkungsweise muß verzichtet werden. Entsprechende im Anhang beispielhaft abgedruckte Informationen des Landesamtes für Verfassungsschutz Baden-Württemberg können hierüber Aufschluß geben. Sinn und Zweck einer solchen GMA ist es, Angriffe auf geschützte Objekte und Personen zu erschweren, zu entdecken, unverzüglich an hilfeleistende Kräfte weiterzumelden - insbesondere bei Überfällen auf Personen - und im Rahmen der Beweissicherung zu protokollieren. Außerdem garantiert die GMA - bei sinnvoller Verknüpfung mit ZKA, Fluchtwegesicherung und Brandmeldeanlage -, daß im Normalfall (scharf geschalteter Zustand der Anlage bei Nichtbesetzung) alle Zugänge zum RZ geschlossen und verriegelt sind, im Alarmfall aber trotzdem der schnelle und unkomplizierte Zugang von Rettungskräften zum Objekt gewährleistet ist.

Die größten - teilweise sogar existenzbedrohenden - Schäden können durch Brände in RZ entstehen. Bauliche ***Brandschutzmaßnahmen*** sind deshalb unumgänglich. Dazu ist das RZ zunächst in Brandabschnitte aufzuteilen und das Risiko von Bränden in Abhängigkeit vom zu erwartenden Schadensausmaß im Brandfall zu bewerten. Die in der DIN-Vorschrift 4102 festgelegten baulichen Brandschutzmaßnahmen für Bauteile (Wände, Decken, Stützen, Unterzüge, Treppen usw.) sind in Feuerwiderstandsklassen F 30 - F 180 (Feuerwiderstandszeitwert bei definierter Wärme in min) eingeteilt. Die dort bestimmten Feuerschutzabschlüsse (Türen, Tore, Rolläden usw.), Brandschutzgläser, Lüftungsleitungen, Brandschutzklappen, Kabel- und Rohrabschottungen, Rohrummantelungen, Installationsschächte und -kanäle sowie die baurechtlichen Vorschriften für den baulich-technischen vorbeugenden Brandschutz sollten in ein Brandschutzkonzept für das RZ mit einfließen.

Neben diesen Vorgaben und den (organisatorischen) Maßnahmen zur Vermeidung von Brandlasten innerhalb und außerhalb des RZ-Bereichs sollte - zur frühzeitigen Entdeckung und Meldung von Bränden an die Feuerwehr oder andere hilfeleistende Stellen - eine ***Brandmeldeanlage*** (BMA) installiert werden.

In vielen früheren Fällen hätte eine rechtzeitige Brandfrüherkennung zu einer erheblichen Schadensminimierung beitragen können. Brandmeldeanlagen und ihre angeschlossenen Melder (Rauch-, Wärme-, Handmelder) können im Bedarfsfall durch ***automatische Löschanlagen*** (CO_2- Vollflutung, CO_2 -Objektflutung mit Doppelbodenflutung, Inergen-Vollflutung, Argon-Vollflutung, Inergen- und Argon-Teilflutung, Stickstofflöschanlagen) ergänzt werden.
Maßnahmen wie Feuerwehrschlüsselkästen, besondere Rettungswege und Löschanschlüsse, Aufzugssteuerungen im Brandfall, geordnetes Herunterfahren der Rechner über Notabschaltungen, Abschalten der Energieversorgung und der Klimatechnik sowie Auslösen der Gefahrenmeldeanlage und der Fluchtwegesicherungen können dieses Konzept sinnvoll ergänzen.

Bei RZ in hochwasser- oder überschwemmungsgefährdeten Lagen sind bauliche Maßnahmen zum Schutz der Rechner gegen ***Wasserschäden*** notwendig. Bei besonders gefährdeten Objekten empfiehlt sich der Einbau von Wassermeldeanlagen und Notpumpen. Auch im Gebäude selbst besteht durch Rohrleitungsbrüche die Gefahr derartiger Schäden. Sicherheitshalber sollten solche Rohre nicht über oder am RZ entlang verlegt werden. Vorhandene Rohrleitungen können durch Rückstau- oder Lecksicherungsventile sowie durch Auffangeinrichtungen abgesichert werden. Wasserschäden durch den Löscheinsatz sind nur dadurch zu vermeiden, daß die Feuerwehr umfassende Kenntnis über Art und Umfang des RZ erhält.

Rechner, die beim Betrieb auf ein spezifisches Raumklima angewiesen sind, benötigen eine Klimaanlage. Bei der ***Klimaplanung*** ist besonders zu berücksichtigen, daß die Geräte eine hohe (ständige) Verfügbarkeit haben müssen. Aus sicherheitstechnischen- und Brandschutzgründen sollten Klimaanlagen jedoch nicht unmittelbar im RZ, sondern in einem durch Feuerschutzabschlüsse und Brandschutzklappen gesicherten, benachbarten Raum untergebracht werden. Bei einer sinnvollen Verknüpfung mit der GMA und der BMA kann im Brandfall auch die Klimaanlage geordnet abgeschaltet und über redundante Maß-ahmen (modularer Aufbau der Klimatechnik) - sofern notwendig - trotzdem die Klimatisierung des RZ aufrechterhalten werden. Zu- und Ablufteinrichtungen

der Klimatechnik müssen, da hier z.B. sehr leicht brennbare Flüssigkeiten eingegossen werden können, gegen Sabotage gesichert werden. Da Anschläge auf große Klimaanlagen mit Sicherheit auch den RZ-Betrieb über längere Zeit lahmlegen können, sind auch für diese Anlagen selbst Sabotageschutzmaßnahmen unerläßlich.

1995 haben die Versicherer ***Überspannungsschäden*** (insbesondere durch indirekten Blitzeinschlag) in zweistelliger Millionenhöhe registriert. Eine von einem Versicherungsunternehmen durchgeführte Untersuchung ergab, daß nicht mangelnde Überspannungsschutzeinrichtungen, sondern oftmals nicht EDV-gerechte Verkabelungen ursächlich für diese Schäden waren. Grundlage für eine optimale Überspannungsschutzplanung von Daten- und Stromversorgungsnetzen ist ein sog. EMV-Schutzkonzept. Sowohl der elektrotechnische als auch der datentechnische (auf der Grundlage der Europanorm EN 50 173) Teil sollte von einem Fachmann auf diesem Gebiet erarbeitet werden.

Kurzzeitige Überspannung, Spannungsabfall oder gar Stromausfälle können IT-Systeme sehr stark beeinträchtigen oder schädigen. Ohne die durch Sabotage verursachten Stromausfälle ist derzeit in der Bundesrepublik Deutschland mit Stromausfällen an 10 Tagen im Jahr zu rechnen. Diese Störungen im Energieversorgungsnetz führen oftmals zu Hardwareschäden an der Zentraleinheit, zu Störungen bei der Datenübertragung von der Festplatte bis hin zum gefürchteten "Headcrash" und zu Datenverlusten (Daten, die zum Zeitpunkt der Störung im Zwischenspeicher abgelegt sind, gehen verloren). Betriebssicherheit im Rahmen der Verfügbarkeit der Systeme kann hier nur durch den Einsatz von ***Unterbrechungsfreien Stromversorgungen*** (USV) und ***Netzersatzanlagen*** (NEA) erreicht werden.

Bei USV-Anlagen wird grob in zwei Gruppen unterschieden:

- *Offline-USV*: diese schalten sich (zeitverzögert im Millisekundenbereich) erst bei einem tatsächlichen Spannungsproblem im öffentlichen Energieversorgungsnetz zwischen Stromnetz und angeschlossene DV-Geräte;

sie werden meist im Bereich kleinerer IT-Systeme oder lokaler Netze eingesetzt;

- *Online-USV*: diese versorgen die angeschlossenen Geräte über einen Wechselrichter ständig mit Strom und greifen bei Stromausfall direkt auf die Akkus (Batterien) zu; durch diese Art USV können auch Stromlastschwankungen im öffentlichen Energieversorgungsnetz (kurzzeitige Spannungsspitzen und -abfälle) gefiltert werden; sie versorgen in der Regel größere, zentrale Rechnerkomponenten.

Durch den Einsatz solcher USV und deren unterschiedlichster Variationsmöglichkeiten innerhalb der Systeme und untereinander, kombiniert mit spezieller USV-Steuerungssoftware, können nahezu sämtliche Aspekte einer im Notfall vom öffentlichen Stromversorgungsnetz unabhängigen Stromversorgung abgedeckt werden. Die Kapazität der in USV eingebauten Batterien hängt im wesentlichen von der Größe der Akkus, der gewünschten Überbrückungszeit und der Leistungsfähigkeit der angeschlossenen Geräte ab. Bei der USV-Planung muß deshalb sehr genau festgelegt werden, welche Geräte (am besten alle) an die USV angeschlossen werden. In der Praxis kommen deshalb - auch aus wirtschaftlichen Gesichtspunkten - meistens zweigeteilte Stromversorgungen zum Einsatz. Ein Teil der Geräte wird direkt über das öffentliche Stromversorgungsnetz versorgt, der schützenswerte Teil (insbesondere IT- und Kommunikationseinrichtungen) wird über USV-Anlagen gepuffert. Der Einfachheit halber werden an die USV angeschlossene Steckdosen deshalb farblich gekennzeichnet und festgelegt, welche Geräte zwingend dort angeschlossen werden müssen. Kann die Last der so anzuschließenden Endgeräte (PC, Rechner, Peripherie, Kommunikationseinrichtungen bis hin zur Kaffeemaschine) nicht exakt definiert werden, und sollte die definierte Überbrückungszeit (normalerweise 10 bis 30 min) der Akkus auch bei längeren Stromausfällen nicht ausreichen, müssen derartige USV mit zusätzlichen, netzunabhängigen Aggregaten ausgestattet werden. Die für diesen Zweck eingesetzten Netzersatzanlagen (Notstrom-Diesel-Aggregate) müssen gegen Sabotage geschützt und bauliche Auflagen für Tanks und Betrieb erfüllt werden.

PC-GRUNDSCHUTZ

Zur Erstellung eines PC-Grundschutzkonzepts sollte konsequenterweise das vom BSI entwickelte IT-Grundschutzhandbuch (vgl. Anhang 3) angewendet werden. In dieser BSI-Publikation sind alle Maßnahmen (baulich, technisch, personell, organisatorisch) zum Schutz von PC-Systemen zusammengefaßt und können mit einem genau beschriebenen Verfahren (Schutzbedarfsfeststellung, Schwachstellenanalyse, Sicherheitskonzept) auf die Belange der Nutzer abgestimmt werden. Aus 20 sog. Einzelbausteinen werden diejenigen ermittelt, die das eigene System möglichst realitätsnah abbilden. Dann kann festgestellt werden, welche im jeweiligen Baustein empfohlenen Maßnahmen in welcher Form umgesetzt werden können. Es verbietetet sich, sämtliche in diesem Werk dargestellten Schutzmaßnahmen hier vorzustellen, da dies schon allein aufgrund der Themenvielfalt nicht möglich ist. Außerdem sind im Abschnitt "Rechenzentrumssicherheit" bereits wesentliche Grundschutzmaßnahmen erläutert worden, die in abgewandelter Form auch für den PC-Bereich Gültigkeit haben. Die im BSI-Grundschutzhandbuch im Kapitel "übergeordnete Komponenten" enthaltenen Bausteine "Organisation", "Personal" und "Datensicherungskon-zept" werden im Anhang 1 dieser Broschüre näher betrachtet. Infrastruktur, Gebäude, Brandschutz und Stromversorgung wurden bereits beim "RZ-Schutz" erläutert. Verkabelungsaspekte bei vernetzten PC-Systemen werden im Teil "Netze" behandelt. Welchen Stellenwert diese BSI-Publikation mittlerweile in der Bundesrepublik Deutschland genießt, läßt sich daraus ableiten, daß das Grundschutzhandbuch im Bereich der Bundesbehörden zum Standard erklärt wurde und auch die Datenschutzbeauftragten im Bund und in den Ländern für den Bereich der personenbezogenen Daten die Anwendung dieses Werkes empfehlen bzw. die Realisierung der dort empfohlenen Maßnahmen voraussetzen. Auszugsweise soll am Beispiel der Sicherung eines ***einzelstehenden*** (kein Anschluß an ein lokales Netz) ***DOS- (oder vergleichbaren-)PC*** (Festplatte, Diskettenlaufwerk, Maus, angeschlossener Drucker, graphische Benutzeroberfläche, ein User) dargestellt werden, welche Schutzmaßnahmen zu realisieren sind:

Büroraum (Aufstellungsort PC)

- bei Abwesenheit Türen und Fenster schließen
- ggf. mechanische und technische Sicherungsmaßnahmen
- Zugangsregelungen für den Raum
- Beaufsichtigung von Fremdpersonal

Systembezogene Sicherheit (PC + Peripherie)

- Paßwortschutz
- Bildschirmsperre
- regelmäßiger Einsatz von Virensuchprogrammen
- Verhaltensmaßregeln bei Auftreten von Computer-Viren
- Verschluß der Diskettenlaufwerksschächte
- Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen
- Datensicherungsmaßnahmen am PC
- sichere Aufbewahrung von Datenträgern
- Sicherungskopien der eingesetzten Software
- sporadische Prüfung der Wiederherstellbarkeit von Daten und Dateien über die Datensicherung
- Erstellung einer PC-Notfalldiskette
- Sichern des CMOS-RAM
- Schutzmaßnahmen gegen kompromittierende Abstrahlung
- Überspannungsschutz
- Stromversorgung gewährleisten

Bei ***vernetzten PC-Systemen*** müssen zusätzlich noch Sicherungsmaßnahmen für *DV-Verkabelung*, *aktive Netzkomponenten*, ggf. *Server*, *Zugriffsschutz*, *Netzwerkbetriebssystem*, *Datensicherung* und *Protokollierung* berücksichtigt werden.

Anhaltspunkte für Sicherheitsmaßnahmen zum Schutz personenbezogener Daten bieten auch die "10 Gebote zur Datensicherheit" wie sie in der Anlage zu § 9 Satz 1 des Bundesdatenschutzgesetzes sowie in den entsprechenden Vor-

schriften der Landesdatenschutzgesetze niedergelegt sind. Im "Leitfaden zur PC-Sicherheit für die Landesverwaltung Baden-Württemberg" (herausgegeben vom Innenministerium Baden-Württemberg) sind die Zugangs-, Datenträger-, Speicher-, Benutzer-, Zugriffs-, Übermittlungs-, Eingabe-, Auftrags-, Transport- und Organisationskontrolle sehr anschaulich beschrieben. Erläuterungen zu PC-Sicherheitsprodukten, zu Risiken und Bedrohungen sowie Hinweise zu einfachen Schutzmaßnahmen runden diesen Leitfaden ab.

Mobile PC-Systeme (Laptops und Notebooks) sind in besonderem Maße Sicherheitsbedrohungen ausgesetzt. Verlust durch Diebstahl oder Fahrlässigkeit, Hardwaredefekte durch unsachgemäßen Umgang, fehlende Kontrolle durch Administratoren, Verstöße gegen Softwarelizenzbestimmungen sowie unbefugtes Kopieren von Daten durch Dritte (vgl. Ziffer 1.4 Täterbild) sind nur einige der hauptsächlichen Bedrohungen im mobilen PC-Einsatz. Sicherheitskonzepte für den Umgang mit solchen Systemen sollten in jedem Fall folgende Maßnahmen beinhalten:

- *Nachweis über ausgegebene Laptops oder Notebooks*
- *Nachweis der eingesetzten Software*
- *Verpflichtung zur Datensicherung und Nachweis der Sicherungskopien*
- *Installierung von Virenschutzprogrammen* (insbesondere bei der Möglichkeit, sich über sog. Docking-Units in Netze und Rechner einzuloggen)
- *Import und Export von Daten und Programmen nur durch autorisiertes Personal* (ansonsten müssen solche Funktionen unterbunden werden)
- *Zugriffsschutzeinrichtungen*

Bei *Zugriffsschutzeinrichtungen* sollte Zugriffskontrollprogrammen gegenüber reinen Hardware-Paßwort- (Bios-Paßwort) Lösungen der Vorzug eingeräumt werden, da der reine Bios-Paßwortschutz mit einfachen technischen Mitteln sehr leicht umgangen werden kann. Zusätzlich sollte der *Paßwortschutz* nach dem Prinzip von "Wissen und Besitz" um einen sog. Identifizierungstoken (ID-Token) oder um ein (Chip-) Kartenlesegerät erweitert werden. Der Token (taschenrechnerähnliches Zusatzgerät) erhöht die Paßwortsicherheit, da er ein Paßwort generiert, das nur wenige Minuten Gültigkeit hat. *Kartenlesesysteme* bieten einen erhöhten Zugriffsschutz. *Zugriffsschutzprogramme* ermöglichen auch die Option

der Rechteverwaltung und Freigabe auf dem System. Hierdurch kann festgelegt werden, wem z.B. bestimmte Rechte wie das Ausführen oder Verändern besonderer Programme und Dateien zustehen und wem nicht. Diskettenlaufwerke sollten, sofern sie überhaupt benötigt werden, durch das Zugriffskontrollprogramm gesperrt werden. Einen umfassenden Schutz bieten hier eigentlich nur *Hardwareverschlüsselungssysteme*, die über eine vorhandene PCMCIA-Schnittstelle an den Laptop oder das Notebook angeschlossen werden. Mit solchen Karten werden Funktionalitäten wie Bootschutz, benutzerabhängige Bootsteuerung, automatische Einstellung der User-Rechte, intelligente Paßwortsteuerung, benutzerabhängige Sperrung der Schnittstellen, Kryptierung von Festplatte und Disketten, Virenschutz, wahlweise Dateikryptierung, automatische Aufzeichnung von Protokolldaten, wahlweise 4-Augen-Prinzip bei der Auswertung der Log-Daten und eine Security API mit Bios-Schnittstelle realisiert. Neben einer konsequenten Systemrevision und einer restriktiven Datensicherungspraxis sollten insbesondere die Anwender von solchen Geräten sensibilisiert und auf die vielfältigen Risiken hingewiesen werden. Eine *umfassende Anwenderschulung in sicherheitsrelevanten Funktionsbereichen* garantiert, daß diese in der Praxis auch (richtig) genutzt werden.

Die ***zwei wesentlichen Grundfunktionen im Zugriffsschutz*** nach dem bereits angesprochenen Grundsatz von "Besitz und Wissen " ***sind Paßwortverfahren und rechnergesteuerte Benutzeridentifikation mit Berechtigungsprüfung***. Nur mit Paßwort und zusätzlichem Ausweis (Magnetkarte, Chipkarte, Token, Dongle, Smart-Cards, besondere Startdiskette, mechanischer Schlüssel in Kombination mit einer besonderen Benutzer-ID - Paßwortgüte) kann ein berechtigter Zugriff auf das IT-System erfolgen. Der Hardwarebestandteil oder der mechanische Schlüssel dienen hierbei der Identifikation, der Softwarebe-standteil der Authentisierung des Zugriffsberechtigten. Durch Meldungen in der Presse (u.a. "gefährdete Paßwörter unter Win 95") wird deutlich, daß Paßwort nicht gleich Paßwort ist. In der Praxis (vgl. KES-Sicherheitsstudie 1994) kommt allerdings einem solchen Zugriffsschutzverfahren überragende Bedeutung zu. Die Grundregeln für einen sicheren Paßwortaufbau und dem damit verbundenen Sicherheitsmanagement können den Empfehlungen des Bundesbeauftragten für

den Datenschutz (im Anhang abgedruckt) entnommen werden. Generell gilt, daß Paßworte

- aus Buchstaben, Zahlen, Satz- und Sonderzeichen bestehen sollten
- mindestens 8 Zeichen lang sein sollten
- regelmäßig gewechselt werden müssen (Automatismus des Systems)
- Trivialpaßworte (z.B. 0815, 4711, 26.05.63, 123456, PC, Namen und Vornamen) automatisch vom System zurückgewiesen werden sollten
- vorherige Paßworte nicht mehr weiterverwendet werden dürfen (sog. Paßworthistorie)
- Paßworte mit Einwegverschlüsselungsverfahren in besonders geschützten Bereichen auf den Rechnern abgelegt werden (d.h. eine Rekonstruktion oder Entschlüsselung ist auch durch Systemadministratoren nicht möglich)
- über ein Paßwortmanagement (Unternehmens- oder Behörden-Richtlinien) die Verwendung von Paßwörtern geregelt wird.

ID-Token generieren Paßworte in Abhängigkeit von Datum, Uhrzeit und anderen Variablen, die nur für eine bestimmte Zeit Gültigkeit haben. Mit dem Algorithmus des Token überprüft das IT-System das eingegebenen Paßwort auf seine Gültigkeit. Dadurch, daß der Anwender sein Paßwort nicht mehr auswen-dig zu lernen braucht, können sehr lange, ungewöhnlich zusammengesetzte und kaum mehr nachvollziehbare Paßworte verwendet werden.

Dongles sind spezielle Zusatzstecker, die wie ein Schlüssel den Zugang zum IT-System ermöglichen. Diese Technik ist heute relativ veraltet und wird in der Praxis kaum noch eingesetzt.

Mechanische Schlüssel in Verbindung mit Benutzer-ID in Paßwortgüte, die den Zugriff auf das IT-System dadurch verhindern, daß elektromechanisch ein Zugriff über Tastatur oder Maus unterbunden wird, sollten lediglich in einer komplett gesicherten Umgebung (Sicherheitsbereich) eingesetzt werden; sie bieten gegen professionelle Angreifer nur einen geringen Schutz.

Karten mit Magnetstreifen werden heute sehr häufig eingesetzt. Sie sind jedoch relativ unsicher, die Magnetstreifen mit entsprechenden Lese-/Schreibgeräten gespeichert, kopiert und verändert werden können. Schutzmechanismen gegen unbefugtes Auslesen oder Verändern der auf dem Streifen gespeicherten Daten sind nicht implementiert. Es gibt zwar bereits Kartensysteme, die aufgrund ihrer Herstellungsweise (z.B. infrarot-codierte Karten) eine höhere Manipulationssicherheit aufweisen, aber auch diese können einen vergleichbaren Sicherheitsstandard und Leistungsumfang wie Chipkarten nicht bieten.

Hingegen stellen Smart-Cards oder Chipkartensysteme und Sicherheitsmodule heutzutage in Kombination mit Paßwortverfahren die interessanteste und sicherste Möglichkeit zur Zugriffssteuerung dar. Bei diesen Systemen werden das Paßwort und die Benutzer-ID verschlüsselt auf dem Chip der Karte untergebracht. Paßwortdateien auf dem Rechner selbst, die immer wieder Angriffen - insbesondere durch Hacker - ausgesetzt sind, werden damit überflüssig. Außerdem weisen diese Kartensysteme eine sehr hohe Manipulations- und Abhörsicherheit auf. Mit solchen Kartensystemen wird heute nicht nur der Zugriff auf IT-Systeme selbst, sondern auch auf Service und Dienstleistungen der Systeme (z.B. Zugang zu File- und Mail-Servern, Netzen, Online-Diensten, Datenbanken etc.) ermöglicht. Dazu muß der berechtigte Inhaber die Chip-Karte mit Hilfe eines Paßworts (PIN-Nummer) zur Identifikation aktivieren; separate Sicherheitsmodule im IT-System prüfen sodann stufenweise die Berechtigungen ab und stellen die Authentikation mit dem System sicher. Sicherheitsmodule sind in sich geschlossene Systeme, die Angriffsversuche (Auslesen, Manipulieren) verhindern oder bei erkanntem Angriff den sicherheitsrelevanten Teil sofort und sicher löschen. Neben den Einsatzmöglichkeiten bei Zugriffskontrollsteuerun-gen finden diese Systeme auch breite Anwendung im modernen, bargeldlosen Zahlungsverkehr. Auf diesen Anwendungszweck wird hier jedoch nicht näher eingegangen. Weitere Einsatzgebiete sind Schlüsselaustauschverfahren für Verschlüsselungssysteme, Absicherung von Telekommunikationsanwendungen (Kartentelefone, Mobilfunk, Fax etc.) und Realisierung der digitalen Unterschrift im Rechts- und Zahlungsverkehr.

Die beschriebenen baulichen, technischen und organisatorischen Maßnahmen können nur Anhaltswerte darstellen. Sie müssen bei einer Beratung vor Ort individuell an die Schutzbedürfnisse und die Gefährdungslage des IT-Nutzers angepaßt werden. Neben den Beratungen durch die für den staatlichen Geheimschutz zuständigen Behörden (BSI / Verfassungsschutz), können hierfür auch Sabotageschutzkonzepte der Polizei - insbesondere der Landeskriminalämter - im Rahmen der kriminalpolizeilichen Vorbeugung in Betracht kommen. Die vom Landesamt für Verfassungsschutz Baden-Württemberg bereits erstellten Informations- und Druckschriften zu einzelnen hier angesprochenen Themenbereichen sind im Anhang aufgeführt und können bei Bedarf angefordert werden.

2.3.4 Kompromittierende Abstrahlung (k.A.)

Bereits 1986 ging durch die Stuttgarter Presse die Meldung: "Leichte Arbeit für Wirtschafts- und Datenspione". Darin wurde stark vereinfacht dargestellt, wie Wirtschaftskriminelle und Spione mit simplen, geringfügig adaptierten Fernsehgeräten interessante Objekte anpeilen und über den Fernsehbildschirm alles empfangen könnten, was auf Datenverarbeitungs- und Bildschirmsichtge-räten in der näheren Umgebung verarbeitet werde. Der Leiter des Labors für Nachrichtentechnik der Fachhochschule Aachen, Prof. Erhard Möller, wurde folgendermaßen zitiert:

> "Theoretisch kann das jeder Fernsehtechniker im zweiten oder dritten Lehrjahr. Untersuchungen des Labors haben ergeben, daß sich das Bild eines normalen Terminals - durch verschlossene Türen und Mauern hindurch und sogar um die Ecke herum - noch in 25 Metern Entfernung empfangen läßt. Höherer technischer Aufwand überbrückt leicht auch Hunderte von Metern."

Das hier beschriebene technische Phänomen basiert auf dem wissenschaftlich nachgewiesenen Effekt, daß IT-Systeme und deren periphere Endeinrichtungen (z.B. Datensichtgeräte, Monitore, Drucker, Tastaturen, Modems u.ä.) während ihres Betriebs ständig elektromagnetische Signale abgeben. Diese Signale sind

ein "ungewolltes" Nebenprodukt zur normalen Störstrahlung der Geräte. Diese kann auch die mit dem IT-System verarbeiteten Informationen im Klartext enthalten und abstrahlen; demzufolge lautet die Definition für kompromittierende (bloßstellende) Abstrahlung:

> "Werden von einem elektrischen Gerät, das Informationen verarbeitet, speichert oder überträgt, unbeabsichtigt datenbezogene oder sonstige informationstragende Signale abgestrahlt, die, wenn sie erfaßt und analysiert werden, die zu schützende Information preisgeben, so spricht man von kompromittierender Abstrahlung (k.A.)."

Ursächlich für k.A. sind thermisches Rauschen elektrischer Bauelemente (Widerstände, Halbleiter), Lastschwankungen (Strom- bzw. Spannungsschwankungen auf dem elektrischen Energieversorgungsnetz), von internen Oszillatoen erzeugte Träger sowie hochfrequente Anteile elektrischer Signale.

Die Ausbreitung von k.A. kann erfolgen:

- als hochfrequente Raumstrahlung (elektromagnetische Wellen, die sich wie Radio- oder Fernsehwellen durch den Äther ausbreiten)

- als akustische Raumstrahlung (z.B. bei Druckern oder Kugelkopfschreibmaschinen; die Verbreitung erfolgt über Schall oder Ultraschall und kann mit empfindlichen Mikrophonen aufgenommen werden)

- über kapazitives oder induktives Überkoppeln auf andere, parallel hierzu verlegte elektrische Leitungen oder Datenkabel (auf dem Parallelkabel breitet sich die Abstrahlung aus und kann von diesem noch in großer Entfernung abgegriffen werden)

- als akustische Überkopplung auf andere Geräte - sog. Mikrofonieeffekt (die Schallwandlung in elektrische Signale erfolgt dabei durch schallempfindliche Geräteteile, die unter bestimmten Voraussetzungen ähnlich wie ein Mikrofon arbeiten; die weitere Ausbreitung erfolgt dann entlang metallischer Leiter oder als hochfrequente Raumstrahlung)

- als sog. Mantelwellen über andere metallische Leiter (Heizungsrohre, Rohre von sanitären Installationen und klimatechnischen Einrichtungen sowie sonstige Versorgungsrohre) oder

- durch Manipulation der Geräte von außen (z.B. durch Bestrahlung der Geräte mit Hochfrequenzenergie; hierdurch können die im Gerät ablaufenden

elektrischen Vorgänge so beeinflußt werden, daß die eingestrahlten Wellen nun die zu verarbeitende Informationen mit sich tragen)

Der Empfang und die Auswertung von hochfrequenter Raumstrahlung bis zu einer Entfernung von ca. 100 Metern kann mit handelsüblichen Antennen bewerkstelligt werden. Bei größeren Entfernungen sind Spezialantennen sowie ggf. hochempfindliche Verstärker und Empfänger notwendig. Die Ausbreitung auf metallischen Leitern ist entscheidend von der Gebäudeinfrastruktur abhängig und kann erheblich weiter reichen. Grundsätzlich ist hierbei zu berücksichtigen, daß die Reichweite und der technische Aufwand für die Auswertung einer erfaßten k.A. eines IT-Systems wesentlich von

- der Art des abstrahlenden Geräts,
- der Intensität der - eventuell manipulierten - Strahlung und Qualität ihrer Erfassung (Empfindlichkeit der Meßgeräte)
- der Höhe der elektromagnetischen Dämpfung des Gebäudes/Raumes, in dem das Gerät betrieben wird und
- der Verstärkung vorhandener Abstrahlung durch die Antennenwirkung von metallischen Leitern im Betriebsraum/-gebäude

abhängen und beeinflußt werden.

Da die Abstrahlungsintensität logarithmisch abnimmt, wird sich ein Angreifer bemühen, mit seiner Antenne so nah wie möglich an das zu belauschende Objekt heranzukommen. Bei einem solchen Angriff ist es jedoch nicht notwendig, empfangene Informationen sofort sichtbar zu machen. Der Geräteaufwand zur Auswertung der k.A. reduziert sich u.a. auch dadurch, daß diese aufgezeichnet, zwischengespeichert und unter Laborbedingungen reproduziert werden kann. Alle elektronischen Geräte - auch bauartgleiche Seriengeräte - besitzen aufgrund ihrer Bauteiletoleranzen ein individuelles Abstrahlverhalten, das meßtechnisch ermittelt, durch entsprechende Filtertechnik entzerrt und aufgearbeitet werden kann. Befinden sich in einem Gebäude oder Raum mehrere strahlende IT-Geräte, können deshalb unter Ausnutzung dieser gerätespe-

zifischen Abstrahlung, durch geeignete Meß- und Filtertechnik und durch Einsatz von Antennen mit Richtwirkung einzelne von ihnen ausgewählt werden.
K.A., die sich über das Energieversorgungsnetz ausbreitet, kann mit einem speziellen Netzfilter - im einfachsten Fall mit einem Kondensator - auf dem Netz abgegriffen werden. Das Abstrahlverhalten von IT-Systemen kann durch gezielte Manipulationen an den Geräten, z.B. durch

- Entfernen von Masseverbindungen
- Einbau von Kopplungsbrücken
- (sinnvolles) Entfernen von Abschirmmaterialien
- Abisolieren von Kabelschirmungen und
- Verlängern oder Ausrichten von Leitungen

wesentlich erhöht werden.

Angesichts der bis heute anhaltenden Diskussion über Aufwand und Ertrag beim Abhören kompromittierender Abstrahlung erscheint vor eingehenderen Überlegungen bezüglich etwaiger Schutzmaßnahmen der nachfolgende Hinweis angebracht:

Hersteller von PC-Bildschirmen werben für ihre Geräte häufig mit dem Begriff der "Abstrahlarmut" und berufen sich hierbei auf Schirmungsmaßnahmen nach den Richtlinien MPR II, TCO oder SSI. Maßnahmen nach diesen Richtlinien sollen jedoch ausschließlich mögliche Gesundheitsgefahren für PC-Anwender durch elektromagnetische Wellen und insbesondere Röntgenstrahlen (Kathodenstrahlung von Bildschirmen) ausschließen. Zum einen sind diese Richtlinien nicht geeignet, dieses Risiko gänzlich auszuschließen, da es noch keine empirischen Untersuchungen zum Thema Gesundheitsrisiko gibt und die Meßwerte nach diesen Vorschriften rein theoretischer Natur sind. Zum anderen haben Untersuchungen von unabhängigen Institutionen (z.B. Computerfachzeitschriften) ergeben, daß zwar mit Erfüllung der Normen geworben, bei Nachprüfung, d.h. Nachmessung, jedoch die in den Richtlinien vorgegebenen Grenzwerte nicht oder nur teilweise erreicht werden. Außerdem sind die Meßverfahren und

Grenzwerte für den Nachweis oder die Aufzeichnung von k.A. völlig ungeeignet und ermöglichen keine Bewertung der Sicherheit gegen unbefugtes Abhören oder Mitlesen der Daten.

Mit der Einführung der europäischen Regelungen zur elektromagnetischen Verträglichkeit (EMV) von elektrischen und elektronischen Geräten und der Umsetzung dieser Richtlinien in nationales Recht (EMV-Gesetz v. 9. November 1992) hat sich das Abstrahlverhalten von IT-Geräten durch die in diesen Vorschriften geforderten Grenzwerte und Schirmmaßnahmen insofern verändert, als nach Untersuchungen des Bundesamts für Sicherheit in der Informationstechnik handelsübliche, moderne PC in der Regel über eine Raumstrahlung verfügen, die den Grenzwert von 100 Metern nicht überschreitet. Die Ausbreitung auf metallischen Leitern hängt dagegen von der Gebäudeinfrastruktur ab; sie kann erheblich weiter reichen. Ein Angriff innerhalb des Grenzwertes von 100 Metern ist grundsätzlich um so erfolgversprechender, je kürzer die Distanz zwischen Angreifer/eingesetztem Hilfsmittel (Antenne, Aufzeichnungsgerät) und dem anzugreifenden IT-Gerät ist. Die Praxis zeigt, daß dieses Risiko bei sehr vielen öffentlichen und privaten Gebäuden vorhanden ist, da sich ein potentieller Angreifer völlig unbemerkt in unmittelbarer Gebäudenähe aufhalten könnte. Das diesem Angriffsszenario zugrundeliegende Täterbild geht von einem (nachrichtendienstlich) geschulten Täter mit fachtechnischem Wissen aus, der auch über den nötigen finanziellen Hintergrund verfügt. Aufwand und Erfolg eines solchen Angriffs bemessen sich insbesondere nach den Kriterien:

- unbemerkter Zugang zu nur unzureichend oder nicht kontrollierbaren Bereichen in Gebäudenähe
- keine sonstigen personellen (z.B. Innentäter mit legalem Zugang/Zugriff) bzw. technischen Manipulationsmöglichkeiten (z.B. Hackerangriff, Abhören von externen Leitungen)
- Wert der zu erwartenden Informationen im Verhältnis zum Aufwand

Der erforderliche finanzielle Aufwand zur Nutzung von k.A. bei modernen IT-Geräten liegt im günstigsten Fall bei mehreren tausend DM. Berücksichtigt wer-

den muß jedoch auch, daß für einen Nachrichtendienst die Erkenntnisgewinnung, vor allem wenn keine anderen Zugangsmöglichkeiten gegeben sind, im Vordergrund steht. Nach Auffassung der Sicherheitsbehörden ist diese Form der Informationsbeschaffung auch im Bereich der Organisierten Kriminalität durchaus vorstellbar. Bei Konkurrenzspionageangriffen kann der Wert der so gewonnenen Informationen, insbesondere aus Forschung und Entwicklung, den Aufwand um ein vielfaches überschreiten.

Konkrete Fälle, in denen fremde Nachrichtendienste mit Erfolg das Abhören von k.A. praktiziert hätten, sind bislang (noch) nicht bekanntgeworden. Aus der Hinterlassenschaft des "Ministeriums für Staatssicherheit" (MfS) der früheren DDR konnten jedoch hochmoderne Meß- und Aufzeichnungsgeräte, die in einem Fahrzeug installiert waren, sichergestellt werden. Diese Geräte waren in jedem Fall zur "mobilen" Aufzeichnung von k.A. geeignet. Nach Recherchen des MDR-Fernsehmagazins "Fakt" (Ausgabe vom 31. Juli 1995) und Unterlagen, die der Redaktion der PC-Zeitschrift "Kommunikations- und EDV-Sicherheit" (KES) vorliegen, war beim MfS die "Auswertung informationshaltiger elektromagnetischer Parasitärstrahlung von Bürocomputern" Stand der Technik. In der KES-Ausgabe 95/4 (Seite 42-43) werden die Fälle anhand von Beispielen dargestellt. Einer dieser Vorgänge (vom Parkplatz des Ministeriums für Außenhandel der DDR im damaligen Ost-Berlin aufgezeichnete Korrespondenz des Ministeriums über Wirtschaftsgüterabwicklung) zeigt jedoch, daß hier in aller Ruhe, mit geringem Entdeckungsrisiko und auf "heimischem" Terrain gearbeitet wurde. Das ZDF-Magazin "Zündstoff" vom 24. April 1996 griff in einem Beitrag "Hacker mit Geheimauftrag" dieses Thema ebenfalls auf. Dar-gestellt wurde u. a. die Möglichkeit, über nicht dokumentierte Module in Standardsoftwareprodukten Dateien, die auf lokalen Festplatten von PC gespeichert sind, systematisch zu durchsuchen. Die hierbei gefundenen Daten sollten dann ohne Einflußnahme des Benutzers in bestimmte, für ihn nicht erkennbare Bildschirmdarstellungen umgewandelt, abgestrahlt sowie mittels Satellitenunterstützung empfangen und ausgewertet werden können. Grundsätzlich ist zu diesem Beitrag anzumerken, daß die bereits erläuterten Risiken der kompromittierenden Abstrahlung ernst genommen werden müssen. Die in der Sendung gemachte

Aussage, wonach die abgestrahlten Daten von Satelliten empfangen, weitergeleitet und dann ausgewertet werden könnten, erscheint nach Auffassung von BSI-Fachleuten jedoch überzeichnet.

Als Konsequenz zu den obigen Ausführungen zum Thema "kompromittierende Abstrahlung" sind Schutzmaßnahmen zur Verhinderung dieses Risikos grundsätzlich notwendig. Der Schutzbedarf des Anwenders ist hierbei in hohem Maße von der Sensibilität der zu verarbeitenden Informationen abhängig.

2.3.5 Lauschangriffe / Schutzmaßnahmen

Obwohl sich der wesentliche Teil dieser Broschüre mit den klassischen Angriffszielen der Computerspionage wie PC-Systeme, Rechner und Netze auseinandersetzt, können insbesondere Einrichtungen der Telekommunikation nicht außer Betracht gelassen werden. Die meisten dieser Geräte funktionieren heute bereits nach den Grundprinzipien der PC-Technologie; außerdem lassen sich die unterschiedlichen Technik-Welten kaum mehr voneinander trennen. Die PC-Telefon-Integration, in PC-Systeme integrierte Faxkarten und gemeinsame Übertragungswege sorgen dafür, daß diese Bereiche immer mehr zusammenwachsen. Sicherheitskritisch muß hierbei betrachtet werden, daß es sich bei diesen Einrichtungen um Massenkommunikationsmittel handelt, deren Gebrauch aus dem täglichen Leben nicht mehr wegzudenken ist. Über vier Milliarden Telefongespräche werden in Deutschland jährlich geführt, über zwei Millionen Schnurlostelefone wurden verkauft, und in allen Bereichen ist die Tendenz steigend. Über diese teilweise sehr unsicheren Geräte wird auch eine Vielzahl von sensiblen und vertraulichen Daten ausgetauscht, oftmals in völliger Unkenntnis der damit verbundenen Risiken. Die Ursachen der Erfolge der Computerspionage liegen vor allem in ***menschlichen Schwächen*** begründet: mangelhaftes Sicherheitsbewußtsein auch in Führungsetagen, Mißachtung vorhandener Sicherheitseinrichtungen aus Bequemlichkeit oder Unkenntnis, sorgloser Umgang mit Paßwörtern. ***Es ist ein Irrglaube, daß moderne Kommunikationsmittel automatisch vertrauliche Informationen schützen.*** Telefone und Faxgeräte rangieren deshalb in der "Hitliste" technischer Angriffsziele weit oben. Die durch Lauschangriffe erzielte Informationsflut ist immens, der (technische) Aufwand gering, die Kosten für Abhöreinrichtungen - letztere können im übrigen teilweise legal erworben werden - sind niedrig, und das Entdekkungsrisiko für den Angreifer bleibt vergleichsweise klein. Nach Auffassung von Fachleuten ist der Markt für Sicherheitseinrichtungen zum Schutz der Telekommunikation in Deutschland unterentwickelt, das Bewußtsein für Risiken und Gefahren in Behörden und Wirtschaftsunternehmen fehlt. Auf dem Feld computerunterstützter Straftaten und der Lauschangriffe gibt es - zumindest was die nachrichtendienstliche Seite angeht - lediglich ***rudimentäres Zahlenmaterial***.

Dies liegt einerseits an der Materie selbst, zum anderen aber auch an der hohen Dunkelziffer und an der Zurückhaltung der Betroffenen, Sicherheitsbehörden überhaupt zu unterrichten bzw. an der weitverbreiteten Neigung, einen eingetretenen Schaden möglichst zu verharmlosen.

Neben dem einfachsten aller möglichen Lauschangriffe, dem "bloßen" Mithören des gesprochenen Wortes, kommt bei Lauschangriffen den folgenden Geräten besondere Bedeutung zu:

Anrufbeantworter

Telefonanrufbeantworter modernerer Bauart verfügen meist über die Möglichkeit der Fernabfrage. Mit einer in der Regel dreistelligen Kennziffer - von den Geräteherstellern optimistisch auch als Zugangscode bezeichnet - kann der eigene Anrufbeantworter von unterwegs aus jeder Telefonzelle oder von jedem Telefon aus angewählt werden. Stimmen die über die Telefonleitung übertragene und die im Anrufbeantworter abgespeicherte "geheime" Kennziffer überein, kann das Gerät in seinem vollen Leistungsumfang aus der Ferne bedient werden. Neben dem Abhören aufgezeichneter Telefongespräche kann ggf. auch die Geräteoption "Überwachung von Raumgesprächen" aktiviert werden. Sämtliche im Raum geführten Gespräche können dann mitgehört werden. Leider kann jeder interessierte Unbefugte über ein Zusatzgerät die maximal 1.000 Möglichkeiten bei dreistelligen Kennziffern in kürzester Zeit durchprobieren lassen, um Zugang zum angewählten Anrufbeantworter zu erhalten. Dies läßt erkennen, welches Risiko mit dem Betrieb eines solchen Anrufbeantworters verbunden ist. Bis verbesserte Geräte mit höherem Zugangsschutz marktreif zur Verfügung stehen, gilt die nachfolgende - abgestufte - Empfehlung:

1. Verzicht auf einen Anrufbeantworter

2. Verzicht auf Geräte mit Fernabfragemöglichkeit

3. Bei Geräten mit Fernabfrage:	- 4-stellige Kennziffer - eigene Kennziffern einspeichern, d. h. keine vom Hersteller vorgewählten Ziffern akzeptieren - Option Raumüberwachung kontrollieren - Gerät bei Nichtgebrauch vom Netz trennen
4. Analoge Anrufbeantworter:	- Einsatz eines zusätzlichen Gerätes, das eigentlich zur Überwachung von Gebührendaten (Telefonrechnung) gedacht ist; durch kleinere Programmänderungen ist das Gerät in der Lage, sämtliche Anrufe (mit richtiger und falscher Codenummer) zu protokollieren. Hierdurch werden Angriffsversuche auf den Anrufbeantworter zwar nicht verhindert, aber doch wenigstens dokumentiert.

Schnurlose Telefone

Der Einsatz schnurloser Telefone (Cordless Telecommunications - CT) im privaten und öffentlichen Bereich nimmt rasant zu. Nahezu ebenso stark steigt die Zahl der verkauften Funkempfangsanlagen mit durchstimmbaren Frequenzbereichen (Scanner), mit denen schnurlose Telefone - zumindest bei analogen Übertragungsverfahren zwischen Mobilteil und Basisstation - abgehört werden können. Bedenklich an dieser Tatsache ist, daß im Zuge der seit 1989 forcierten Liberalisierung des Funkempfangs in der Bundesrepublik Deutschland auch der Gebrauch von Scannern, die im übrigen jederzeit geeignet sind, den gesamten Funkverkehr abzuhören, gestattet wurde. Der Markt für schnurlose Telefone war in den vergangenen Jahren geprägt von einer Vielzahl unterschiedlicher, miteinander nicht kompatibler Standards. Erst durch die Einführung des paneuropäischen DECT (Digital Enhanced Cordless Telecommunikations) - Standards im Jahr 1992 konnte bei Herstellern und Benutzern auch eine harmonisierte Sicherheitsstrategie entwickelt werden. Bei den Betrachtungen zur Abhörfestigkeit von schnurlosen Telefonen müssen zunächst die Übertragungsverfahren und die Sprachübertragungsart zwischen Mobilteil

und Basisstation berücksichtigt werden. Die nachfolgende, auszugsweise der Zeitschrift "ntz" (Heft 9/1993) entnommene Tabelle gibt eine Übersicht über die gängigen Standards:

	Standard:	CTO	CT1	CT1+	CT2 (CAI)	DECT
	Produkt verfügbar seit:	1972	1985	1989	1991	1992
	Übertragungsverfahren:	FM	FDMA/FDD	FDMA/FDD	FDMA/FDD	TDMA/TDD
	Sprachübertragung:	analog	analog	analog	digital / 32 kbit/s	digital / 32 kbit/s

CTO = Sammelbegriff für die unterschiedlichsten Spezifikationen der 1. Gerätegeneration
CAI = Common Air Interface
FDMA = Frequency Division Multiple Access
FM = Frequenzmodulation
TDD = Time Division Duplex
TDMA = Time Division Multiple Access

Für alle eingesetzten Übertragungsverfahren sind auf dem freien Markt handelsübliche Geräte erhältlich, mit deren Hilfe die übermittelten Daten rekonstruiert (demoduliert) werden können. Hinsichtlich der Abhörsicherheit der verschiedenen Sprachübertragungsarten gilt, daß das Abhören der Übertragung analoger Informationen (Standards CTO, CT1 und CT1+) mit handelsüblichen Scannern sehr einfach ist. Hingegen ist das Mithören bei der Übertragung digitaler Daten erschwert, da die Sprachinformation aus dem Gesamtdatenstrom selektiert und dekodiert werden muß. Diese Dekodierung ist jedoch ebenfalls mit marktüblichen Geräten möglich. Zusammenfassend kann deshalb gesagt werden, daß weder analoge noch digitale Standards einen Abhörschutz gegen technisch versierte und erst recht nicht gegen professionelle Angreifer bieten. Die beim DECT-Standard vorgesehene Option der Informationsverschlüsselung mit Verschlüsselungsalgorithmen nach diesem Standard ist erst ab 1997 für die Hersteller verbindlich vorgeschrieben. Wirkungsvoll geschützt wird damit aber

nur die Strecke zwischen mobilem Gerät und Basisstation. Der Übergang in das Festnetz oder in Richtfunkstrecken der Telekom oder anderer Netzbetreiber ist damit jedoch noch nicht abgesichert.

Die wichtigsten Mobilfunk-Dienste und -Geräte

C-Netz

Das C-Netz, das älteste Mobilfunknetz in der Bundesrepublik Deutschland, wird von der DeTeMobil betrieben und hat mehr als 700.000 Anschlußteilnehmer. Die Sprache und die Daten für den Verbindungsaufbau werden analog übertragen. Aufgrund dieser Übertragungstechnik können C-Netz-Gespräche sehr leicht mit Scannern abgehört werden. Die durch den Kunden selbst einzustellende Option "Sprachverschleierung" (sog. Mickey-Mouse-Sprache) bietet nur geringen Schutz gegen zufälliges oder gezieltes Abhören, da das zugrundeliegende technische Prinzip (Invertierung) schon bei längerem Mithören durch das menschliche Ohr kompensiert werden kann. Geplant ist, den Datenaustausch für den Verbindungsaufbau und die PIN-Codes für den Zugang zum Netz künftig zu verschlüsseln. Abhängig von der Sicherheit des einzusetzenden Verschlüsselungsalgorithmus kann dann nur noch erschwert festgestellt werden, wer, wann und von wo jemand telefoniert. Ein Abhörschutz für die Sprachübertragung ist damit jedoch noch nicht gegeben.

D1-, D2- und E-Netz

Die digitalen Mobilfunknetze D1 (DeTeMobil), D2 (Mannesmann-Mobilfunk) und E (E-Plus) haben insgesamt ca. 3 Millionen Anschlußteilnehmer. Die Sprachübertragung erfolgt digital nach dem GSM (Global Standard for Mobile Communication) - Standard in den D- und nach dem DCS (Digital Cellular System [Variante von GSM]) - Standard im E-Netz. Mittlerweile können über diese Netze nicht nur Sprache, sondern auch Daten und Faxe übermittelt werden. Ein wirksamer Schutz dieser Netze gegen Abhören ist nur durch Verschlüsselung zu erreichen. Diese Maßnahme ist in den D-Netzen nach GSM- Standard bereits realisiert, jedoch nur auf den Funkübertragungs-strecken. In den leitungs-

gebundenen Netzteilen werden die Informationen nach wie vor offen übermittelt.

Modacom (Mobile Data Communication)

Bei dem 1993 gestarteten Datenfunknetz der DeTeMobil können sich mobile Funkmodems über eine besondere Identifizierungsnummer in das Netz einloggen. Die Funkmodems - gekoppelt an einen mobilen Computer - sind dabei untereinander selbst oder online via Datex-P/ X.25 mit einem Zentralrechner verbunden. Die Datenübertragung erfolgt paketvermittelt. Das Netz ist geeignet für die Übertragung kleinerer und mittlerer Datenmengen oder für Statusmeldungen (Zustände von Anlagen, Meßwertabfragen, Steuerungsdaten u.ä.). Die digitalisierte Datenübermittlung per Funk erfolgt unverschlüsselt und kann deshalb relativ leicht abgehört werden. Die am Beispiel des Modacom vorgestellte Technik und die Abhörbarkeit von offenen Funkübertragungsverfahren gelten im übrigen für alle anderen (öffentlichen und privaten) Datenfunknetze.

Bündelfunk

Bündelfunksysteme (z.B. Chekker, RegioNet, Terrafon-Verbund, Sprintel) bieten regional die Möglichkeit, Daten und Sprache per Funk innerhalb mobiler Einsatzstellen sowie zwischen Mobilteilen und ortsfesten Zentralstellen auszutauschen.

Satellitendienste

Diese Dienste (z.B. Inmarsat-A, -A HSD, -M und -C) sind geeignet für eine mobile, weltweite Daten-, Sprach- und Faxkommunikation. Unter Berücksichtigung der bereits dargestellten Gefahr durch die elektronische Funk- und Fernmeldeaufklärung fremder Nachrichtendienste muß davon ausgegangen werden, daß insbesondere diese Nachrichtenverbindungen in hohem Maße Abhöranngriffen ausgesetzt sind.

Paging-Dienste

Pager können Ton- oder Zeichensignale über Fest- und Funknetzverbindungen an mobile Empfangsstationen übertragen. Derzeit bestehen folgende Paging-

Dienste: Eurosignal, Cityruf-Text, Cityruf-Numerik, Cityruf-Ton, Scall und Omniport. Bei den Diensten, die bis zu 4 Tonsignale übertragen, ist ein Abhören zwar möglich, führt aber zu keinem nennenswerten Ergebnis, es sei denn, die vorher zwischen Sender und Empfänger vereinbarten Bedeutungen der einzelnen Signale sind dem Angreifer bekannt. Die Dienste, die eine kurze Nachrichtenübermittlung (15 bis max. 640 Ziffern und/oder Zeichen) erlauben, können mit Scannern abgehört werden. Eine Zuordnung zum Empfänger der Nachrichten, die sich nicht aus der Nachricht selbst ergibt, ist durch die nur intern bekannte, zum Verbindungsaufbau notwendige Identifikationsnummer eher unwahrscheinlich.

Telefone und digitale Telekommunikationsanlagen

Das Telefon als das am meisten verbreitete Massenkommunikationsmittel war schon immer ein bevorzugtes Angriffsziel fremder Nachrichtendienste. Aufgrund seiner einfachen Wirkungsweise sind Lauschangriffe auf das Telefonnetz und einzelne Gesprächsinhalte sehr leicht möglich. Hinzu kommt, daß heute sehr viele Telefongespräche über Richtfunkstrecken geführt werden. In Anbetracht der enormen Erfolge des MfS bei der strategischen Überwachung der Richtfunkverbindungen entlang der ehemaligen innerdeutschen Grenze kann vor allzu sorglosem Umgang mit dem Telefon nur gewarnt werden. Darüber hinaus hatten das MfS und andere Nachrichtendienste des ehemaligen Ostblocks auf eigenem Territorium Telefonapparate (mit analoger Technik) so manipuliert, daß nicht nur systematisch alle Telefonate, sondern auch sämtliche im Raum geführten Gespräche mitgehört und aufgezeichnet werden konnten.

Die Digitalisierung des Telefonverkehrs im ISDN (Integrated Services Digital Network) und bei privaten Telekommunikationsanlagen (früher: TK-Nebenstellenanlagen) sowie die Umstellung herkömmlicher elektromechanischer Vermittlungstechnik auf computerunterstützte Systeme hat eine Steigerung des Aufwands für technische Aufklärungsmaßnahmen mit sich gebracht. Während früher - bei analoger Technik - das gezielte Abhören einer Telefonleitung einfach und schnell zum gewünschten Erfolg führte, gestaltet sich der Lauschangriff bei digitalen Einrichtungen weitaus schwieriger. Allerdings erge-

ben sich bei modernen TK-Anlagen durch die in solchen Systemen eingesetzte Hard- und Software völlig neue Schwachstellen, die durch gezielte Manipulationen zu Abhörzwecken genutzt werden können.

Täter, die in TK-Anlagen oder -Netze einzudringen versuchen, lassen sich - unabhängig von der jeweiligen Angriffsmotivation (Spionage, Sabotage, Gebührenbetrug, Spieltrieb etc.) - zunächst in zwei Gruppen aufteilen. Wäh-rend sogenannte Phreaker Telefonverbindungen kostenlos ausnutzen wollen, sind Hacker vor allem bestrebt, Daten abzuhören oder zu manipulieren. Beide Gruppen sind gleichermaßen bemüht, sich - mit hoher krimineller Energie und Verwendung fast identischer Angriffsmittel - unberechtigten Zugang zu solchen Anlagen zu verschaffen. Die gebräuchlichsten Angriffsmittel sind:

- Blue Boxes, Red Boxes oder White Boxes (oftmals modifizierte Tonwäh ler); geeignet zur Einrichtung von für den Täter kostenlosen Verbindungen; Bauanleitungen für solche Systeme werden über Untergrundpublikationen oder Mailboxen ebenso verbreitet wie gehackte Rufnummernlisten zum gebührenfreien Telefonieren (insbesondere 0130-Rufnummern)

- War Dialler; Programm zum Erfassen interessanter Telefonnummern mit Statusangaben in bestimmten, vom Angreifer vorgegebenen Bereichen

- Modem; zum Attackieren von Computersystemen und zur Manipulation von Schalteinrichtungen

- Tonwähler; zum Telefongebührenbetrug

- Dietriche, Nachschlüssel; zum unberechtigten und spurlosen Zugang zu Schaltverteilerkästen

- Calling-Card-Codes; die gehackten Codes von Telefonkarten werden zum "kostenlosen" Telefonieren auf Rechnung des Karteninhabers verwendet

Die spektakulären Telefongebührenbetrugsfälle zu Lasten der TELEKOM von Ende 1994/Anfang 1995 zeigen drastisch, wie verwundbar solche Einrichtungen sind.

Nach den Ausarbeitungen des BSI zu Gefährdungen und Schutzmaßnahmen beim Betrieb von digitalen TK-Anlagen können bei modernen Systemen vor allem folgende Risiken eine Rolle spielen:

- Abhören von Telefongesprächen und anderen Nachrichten
- Abhören von Räumen
- Bekanntwerden von Kommunikationsprofilen
- Anlagenausfall durch logische Manipulationen

Als Sofortschutzmaßnahmen werden vom BSI die nachfolgend dargestellten Grundschutzvorgaben empfohlen:

- Absicherung der Wartungszugänge
- Absicherung der Fernwartung
- Revision
- Protokollierung

Als mittel- und langfristige Maßnahmen ist geplant, in Kooperation mit den Anlagenherstellern die Sicherheitsstandards von digitalen TK-Anlagen und Endgeräten zu verbessern und produktunabhängige Überwachungseinrich-tungen zur Erkennung unzulässiger Operationen bei Wartung und Betrieb der Anlagen zu entwickeln. Auf die detaillierten und umfangreichen Schutzmaßnah-men, die in den BSI-Publikationen (vgl. Anhang) zu diesem Thema dargestellt sind, wird hingewiesen. Es wird dringend empfohlen, bei Ausschreibung, Vergabe, Errichtung, Betrieb und Wartung von TK-Anlagen die Vorgaben des BSI zu berücksichtigen.

Telefax

Neben den bereits am Beispiel des Telefons aufgezeigten Risiken - die Über-

tragung von Telekopien läuft im wesentlichen nach ähnlichen technischen Prinzipien und auf gemeinsamen Übertragungswegen ab - sollen hinsichtlich des Einsatzes von Fax-Geräten noch andere Risiken und Schutzmaßnahmen einer näheren Betrachtung unterzogen werden. Durch die enorme Zahl von Fax-Anschlüssen steigt zunächst einmal grundsätzlich die Gefahr der ungewollten Informationsübermittlung durch Fehlvermittlungen und technische Störungen. Im August 1995 wurde beispielsweise bekannt, daß durch technische Störungen und Bedienungsfehler Interna der Commerzbank in Frankfurt am Main wie Tresorskizzen, Kreditauskünfte, Renditeberechnungen, Geburtstagslisten von Mitarbeitern, Vertragsentwürfe, Gehaltslisten und Vorstandsunterlagen an Fax-Anschlüsse von Privatpersonen übertragen worden waren. Menschliche Fehler (Eintippen einer falschen Fax-Nummer) können nach dem Start des Übertragungsvorgangs kaum mehr korrigiert werden oder machen sich erst dann bemerkbar, wenn sensible Daten beim falschen Empfänger bereits "gelandet" sind oder gar in der Presse veröffentlicht werden. Hinzu kommt, daß der Fax-Verkehr keinen seriösen Nachweis darüber erbringen kann, ob ein Dokument tatsächlich übertragen und empfangen wurde. Insbesondere im Rechtsverkehr wird dieses Problem derzeit ziemlich kontrovers diskutiert. Manipulationen durch externe Angreifer (Hacker) sind schwer erkennbar, aber sehr wohl bereits erwiesene Praxis.

Im staatlichen Geheimschutz wird deshalb durch entsprechende Vorschriften (Verschlußsachenanweisung und ergänzende Richtlinien) festgelegt, wie schutzbedürftige Informationen zu behandeln und zu übertragen sind. In der Regel kommen hier - abgestuft nach dem Wert der zu schützenden Information und dem Schutzbedürfnis des Fax-Anwenders - abstrahlarme oder -geschützte Fax-Geräte in Verbindung mit speziell zugelassenen Verschlüsselungsgeräten zum Einsatz.

Durch gestiegene Gebühren für die Fax-Übertragung werden heute bereits vielfach sog. interne oder externe Faxzwischenspeicher eingesetzt, die den Übertragungsvorgang erst zu tarifgünstigen Zeiten ("Mondscheintarif") abwickeln. Die in diesen Mailboxen offen gespeicherten Nachrichteninhalte können ohne

besondere Zugriffsschutzeinrichtungen nahezu unbemerkt durch Hacker gelesen, kopiert oder verändert werden.

Für den Bereich offener Informationen, die aus anderen Gründen (z.B. Datenschutz, besonderes Berufs- oder Amtsgeheimnis, Rechts- oder Kassenwirksamkeit) als sensibel zu betrachten sind, können die im Geheimschutz vorgesehenen Schutzmaßnahmen ebenfalls zur Anwendung kommen. Der vom Landesbeauftragten für den Datenschutz Rheinland-Pfalz herausgegebene Leitfaden (vgl. Anhang) gibt Aufschluß über mögliche und ohne größeren Aufwand zu realisierende Sicherheitsvorkehrungen.

Trends im (mobilen) Telekommunikationsmarkt

Mit den momentan durch die Fachpresse geisternden Begriffen wie "Local Loop", "the last mile" bzw. "verfluchte letzte Meile" ist das Problem verbunden, wie private Endkunden an künftige oder bestehende Kommunikationsnetze angeschlossen werden. Insbesondere durch das zum 1. Januar 1998 wegfallende Monopol der Telekom sind die Wettbewerber am Telekommunikationsmarkt bemüht, hierfür technische (standardisierte) Lösungen zu finden. Völlig unabhängig von den heute angedachten technischen Maßnahmen (bisher wird zumeist die DECT-Technologie favorisiert) ergibt sich unter Sicherheitsgesichtspunkten die entscheidende Frage: Wie können die Vertraulichkeit, Integrität und Verfügbarkeit der übertragenen Sprache, Daten und Bilder gewährleistet werden?

Durch die technischen Lösungen werden die einzelnen Netze und Dienste immer mehr zusammenwachsen. Für den Endkunden wird es oft nicht mehr möglich sein, zu beurteilen, wie und über welche Medien seine Informationen übermittelt werden.

PC-Telefon-Integration (CTI - Computer Telephone Integration), Corporate Networks und City-Netze sind hierbei nur einzelne Stichworte. Mit dem Trend, sämtliche Kommunikationsformen nach einheitlichen Standards auf denselben Medien und Verbindungswegen zu übertragen, steigen jedoch auch die potentiellen Risiken und Angriffs- bzw. Abhörmöglichkeiten.

In dem in seinen wesentlichen Teilen zum 1. August 1996 in Kraft getretenen neuen Telekommunikationsgesetz (TKG) und in dem vom Bundesrat an die Ausschüsse zurückverwiesenen Verordnungsentwurf zur Telekommunikationsdatenschutzverordnung (TDSV) sind die Grundlagen des Fernmeldegeheimnisses und des Datenschutzes teilweise neu geregelt worden. Insbesondere die Regelung des § 87 Abs. 1 TKG, daß

> "die Regulierungsbehörde im Benehmen mit dem BSI, nach Anhörung von Verbraucher- sowie Wirtschaftsverbänden der Hersteller und Betreiber von TK-Anlagen einen Katalog von Sicherheitsanforderungen für das Betreiben von TK- und DV-Systemen erstellen soll, um eine nach dem Stand der Technik und internationalen Maßstäben angemessene Standardsicherheit zu schaffen"

läßt hoffen, daß sich die Abhör- und Manipulationssicherheit von solchen Anlagen erhöht. Ein effektiver Schutz sämtlicher Kommunikationseinrichtungen ist nach Meinung von Fachleuten nur durch den Einsatz geprüfter, hochwertiger Verschlüsselungstechnologie möglich. Deshalb ist diesem Thema ein eigenes Kapitel gewidmet.

Sonstige Lauschmittel

Lauschangriffe auf das gesprochene Wort oder schriftliche Informationen können auch durch in zwei weitere Bereiche aufteilbare Angriffsszenarien erfolgen. Bei optischen und akustischen Lauschangriffen kommen das optische Mitlesen von Daten durch stark vergrößernde Objektive, das Aufmodulieren von Schallwellen auf einen Laserstrahl an Fensterflächen und das akustische Mit-hören mittels Ohr, Stethoskop oder Richtmikrophon in Betracht. Lauschangriffe dieser Art erfordern keinen unmittelbaren Zugang zum abgehörten Besprechungs-, Konferenz- oder Büroraum. Sie können teilweise über recht große Entfernungen erfolgen, sind kaum nachweisbar und haben den Vorteil, daß ein eventuelles Entdeckungsrisiko allenfalls während der Tatausführung besteht. Bei der zweiten Gruppe von Lauschangriffen steht im Vordergrund, Minisender

("Wanzen"), Mikrophone, Lautsprecher oder Körperschallmikrofone in abzuhörende Räume oder Gebäude einzubringen. Bei solchen aktiven Manipulationen ist der Zugang zum Objekt Voraussetzung. Das Entdeckungsrisiko sowohl für den Täter als auch in Bezug auf das Lauschmittel ist dabei ungleich größer als bei der ersten Fallgruppe.

Der häufig kolportierte Einsatz von Minisendern birgt dagegen - gemäß den oben dargestellten Rahmenbedingungen - ein nicht geringes Entdeckungsrisiko für Täter und Tatmittel in sich. Im übrigen ist der Einsatz solcher Geräte nach dem Fernmeldeanlagengesetz verboten. Der Schaden, der damit angerichtet werden kann, ist allerdings beträchtlich. Zu unterscheiden sind hierbei drahtgebundene und netzunabhängige Abhörverfahren. Bei drahtgebundenen Maßnahmen werden Langwellen-Miniatursende- und Empfangsanlagen an das 230-Volt-Netz angeschlossen. Das Stromnetz dient dabei gleichzeitig zur Energieversorgung des Abhörgeräts und als Antenne. Durch diese Art der Übertragung sind die Geräte nur sehr schwer anzupeilen; die Reichweite erstreckt sich auf alle Räume eines Gebäudes mit 230 V-Steckdosen. Nach diesem Prinzip arbeiten auch Netzsteckdosen-Sender. Durch Einstecken des Schukosteckers in eine 230 V-Steckdose wird der Sender in Betrieb genommen und überträgt Raumgespräche über die Stromleitung zum Empfänger. Präparierte Glühlampen und Vorschaltgeräte von Leuchtstofflampen eignen sich ebenso als Behältnisse für drahtgebundene Abhöreinrichtungen. Allerdings sind Glühlampen dann als Lichtquelle nicht mehr funktionsfähig.

Bei drahtunabhängigen Verfahren werden UKW-Kleinstsender (Mikrosender) eingesetzt. Die von dem im Sender integrierten Mikrophon aufgenommenen Schallwellen werden im Niederfrequenzteil des Senders verstärkt, einem Oszillator (eigentlicher Sender im Hochfrequenzteil des Gerätes) zugeführt und von dort zum Empfänger (handelsübliches Radio mit UKW-Teil und Lautsprecher) abgestrahlt. Die Reichweite ist dabei abhängig und somit entscheidend beeinflußbar von der Sendeleistung, der optimalen Antennenanpassung, der Empfindlichkeit des Empfängers und den Geländebedingungen. Durch den Ein-satz ferngesteuerter Miniatursender, die drahtlos ein- und ausgeschaltet wer-den

können, oder durch sprachgesteuerte Sender, die bei Geräuschen auto-matisch in Betrieb gesetzt und nach Ausbleiben des Schallsignals mit geringer Zeitverzögerung wieder abgeschaltet werden können, kann der Batteriestrom (üblicherweise werden eine oder mehrere 1,4 V-Knopf- oder Alkali-Mangan-Zellen eingesetzt, d.h. bei Dauersendebetrieb ist eine Einsatzfähigkeit von wenigen Stunden bis zu mehreren Tagen möglich) gespart und die Betriebsdauer des Minisenders bis zu einem Jahr (bei 10 % Sendebetrieb) erhöht werden. Zur Unterbringung von Minisendern werden häufig Gegenstände des täglichen Gebrauchs wie z.B. Aschenbecher, Tischfeuerzeuge, Unterputzsteckdosen, Bilderrahmen, Streichholzschachteln, Kugelschreiber, Telefone oder andere "dekorative" Gegenstände genutzt. In **Stuttgart** hat unlängst eine Privatfirma ihre Pforten geöffnet, bei der sämtliche bislang angesprochenen Geräte zum Abhören und zum Schutz vor Abhörangriffen gekauft werden können. Nach den derzeit gültigen gesetzlichen Bestimmungen (§ 65 TKG) ist es verboten,

> "Sendeanlagen zu besitzen, herzustellen, zu vertreiben, einzuführen oder sonst in den Geltungsbereich des TKG zu verbringen, die ihrer Form nach einen anderen Gegenstand vortäuschen oder die mit Gegenständen des täglichen Gebrauchs verkleidet sind und aufgrund dieser Umstände in besonderer Weise geeignet sind, das nichtöffentlich gesprochene Wort eines anderen von diesem unbemerkt abzuhören".

Die Verfassungsschutzbehörden der Länder und das BSI können je nach Zuständigkeit, orientiert am Schutzbedarf des Nutzers, den vorhandenen Räumlichkeiten, den personellen und materiellen Schutzmaßnahmen und der Vertraulichkeit der zu schützenden Informationen, baulich / technische und / oder organisatorische Maßnahmen empfehlen. Der größtmögliche Schutz ist nur durch die sinnvolle Kombination beider Schutzmechanismen zu erreichen. Eine fachkompetente Beratung durch BSI / Verfassungsschutz im Bereich des staatlichen Geheimschutzes oder durch eine Fachfirma für den offenen Bereich kann sicherstellen, daß eine Problemlösung realisiert wird, die einen angemessenen Schutz vor Lauschangriffen - bei einem vertretbaren finanziellen und or-

ganisatorischen Aufwand - bietet. Die Ausführung der baulich / technischen Maßnahmen sollte nur durch kompetente Fachfirmen erfolgen.

Auszugsweise können folgende Schutzmaßnahmen generell empfohlen werden:

- Verlagerung des Konferenz-, Besprechungs- oder Büroraumes in einen von außen nicht einsehbaren Gebäudeteil (z.B. fensterloser Raum im Gebäudekern oder im Untergeschoß)

- regelmäßige Überprüfung der Netz-, Telefon- und Datenleitungen auf Manipulationen

- Durchführung organisatorischer Maßnahmen wie z.B.

  - Zugangskontrolle

  - Einrichtung eines überwachten Sicherheitsbereichs

  - Verschluß der Räume bei Nichtbenutzung

  - sichere Verwahrung und Ausgabe der Schlüssel nur gegen Nachweis, Führen von Zutrittsbüchern
  - Beaufsichtigung von Fremd-, Reinigungs- und Wartungspersonal

  - Verzicht auf Telefone (insbesondere schnurlose und Mobilgeräte) und andere Telekommunikationseinrichtungen sowie Gegen-, Wechsel- und Rundsprechanlagen

  - Versiegeln vorhandener Telefon- und Handapparate und Kontrolle der Siegel auf Unversehrtheit vor jeder Besprechung

  - Mechanische Sicherung der TK-Leitungen und Verteilerkästen gegen unbefugten Zugriff (Leitungen unter Putz oder in abschließbaren und verplombten Kabelkanälen verlegen, Verteilerkästen mit Sicherheitsschlössern sichern)

  - Kontrolle von daneben-, darüber- und darunterliegenden Räumen

  - visuelle Überprüfung der Räume in regelmäßigen Abständen und vor wichtigen Besprechungen auf versteckte Abhörsender (dabei auch Steckdosen und Lampen öffnen - vorher Spannung abschalten und gegen Wiedereinschalten sichern -, ggf. Bilder und Uhren abhängen und prüfen)

  - Schließen der Fenster und Herunterlassen der Jalousien (sofern vorhanden) bei Besprechungen

Die folgenden Maßnahmen sollten jedoch nur unter Aufsicht bzw. mit der Unterstützung von Fachpersonal vorgenommen werden:

- Verwendung von Netz-, Telefon- und Datenleitungsfiltern
- Einsatz von Einrichtungen zum Aufspüren von aktiven Minisendern
- Errichtung von akustisch gedämmten Räumen/Kabinen
- Errichtung von elektromagnetisch geschirmten Räumen/Kabinen
- Durchführung von technischen Lauschabwehrprüfungen
- Wiederholungsprüfungen (HF-Dichtungen, Filter, Erdung, Dämpfung usw.)

Abschließend ist noch zu erwähnen, daß der Einsatz von Minisendern und anderen Abhörgeräten ebenfalls sinnvoll und notwendig sein kann. Unter bestimmten rechtlichen Voraussetzungen ist dies ein wirksames Mittel zur Unterstützung der Sicherheitsbehörden bei der Verhütung und Aufklärung von Straftaten. Daß mit diesem Einsatz auch Risiken und mißbräuchliche Verwendungsmöglichkeiten verbunden sein können, zeigt die aktuelle Diskussion über den sog. Großen Lauschangriff.

Methoden und Kosten beim Abhören

Die nachfolgend abgedruckte Tabelle soll das Kapitel über mögliche Gefahren und Risiken durch Lauschangriffe abrunden. Sie stammt von P.R. Bitterli/Fa. Siemens und wurde der Zeitschrift "Funkschau" (Ausgabe 14/95, S. 32) entnommen.

Übertragungs-technik	Abhörmethode	Entdeckungs-wahrscheinlichkeit	Vorkenntnisse *	Anschaffungs-kosten ca. (DM)
Funk	passive Elektronik	unwahrscheinlich	1	150,--
Kabel	Anzapfen im privaten Bereich	vorhanden	2	50,--
Kabel	Anzapfen im Bereich Telekom	vorhanden (eher höher)	2 bis 3	850,--
Kabel	Anzapfen im übrigen Bereich	niedrig bis un-wahrscheinlich	3	850,--
Lichtwellen-leiter	Anzapfen	vorhanden (eher hoch)	3	1700,--
Richtfunk	passive Elektronik	unwahrscheinlich	3	5000,--
Satellit	passive Elektronik	unwahrscheinlich	3 bis 4	13500,--
*Vorkenntnisse:	1=keine; 2=Grundschule, Leitungsverlegung; 3=Elektronisches Wissen, Telekom-Wissen; 4=Elektroingenieur mit geringem Computerwissen			

3. Software

3.1 Betriebssysteme

Zu den Betriebssystemen für den Betrieb von IT-Systemen gehören unbedingt die erforderlichen Softwareprodukte. Grundsätzlich bestehen solche Systeme aus Grundprogrammteilen für jeden Ablauf eines Arbeitsprogramms und aus Zusatzprogrammen, die das Arbeiten mit einer IT-Anlage erleichtern, beschleunigen und verbessern. Zusätzliche Programmteile regeln die Verbindung mit anderen Rechnern. Ein Teil der Grundprogramme wird dabei ständig im Arbeitsspeicher des IT-Gerätes vorgehalten, im Bedarfsfall werden Zusatzprogramme aus einem externen Speicher in den Arbeitsspeicher geladen. Die Kapazität des Arbeitsspeichers ist daher für die Effizienz eines Betriebssystems von entscheidender Bedeutung. In Verbindung mit den in IT-Geräten eingesetzten Mikroprozessoren (z.B. "Pentium") und dem zur internen Datenkommunikation zwischen Prozessor und den übrigen Bauteilen des IT-Gerätes eingesetzten Datenbus ("local bus") bestimmen Betriebssysteme die Leistungsfähigkeit des gesamten IT-Systems. Die derzeit bekanntesten Betriebssysteme sind: DOS (für den einzelnen PC), UNIX (Großrechner), OS/2 (PC; vernetzte PC-Systeme), Windows NT (PC; vernetzte PC-Systeme) und diverse Netzwerkbetriebssysteme (Netware, LAN-Manager, Windows für Workgroups, Vines etc.) für den Netzbetrieb.

Durch die zentrale Steuerung der Zugriffe in einem Rechner und auf seine Speicher kommt dem Betriebssystem auch bei sicherheitsrelevanten Mechanismen eine zentrale Bedeutung zu (Zugriffssteuerung und -kontrolle, Paßwortverfahren, Login/Logon, Dateizugriff, Beweissicherung, Protokollierung und Protokollauswertung, Wiederaufbereitung, Unverfälschtheit, Zuverlässigkeit der Dienstleistungen, Verschlüsselung, Übertragungssicherung). Das NCSC (National Computer Security Center - Teilorganisation des US-amerikanischen [Technik-] Aufklärungsdienstes NSA) hatte in den 80-er Jahren mehrere Dokumente herausgegeben, die sich mit der Verarbeitung sensitiver Daten durch "Standard"-Computersysteme beschäftigten. Dazu wurden in einer Reihe von Publikationen, aufgrund ihrer farbigen Umschläge "Rainbow Series" genannt, Sicher-

heitskriterien entwickelt und Prüfverfahren vorgestellt. Die Anforderungen des NCSC an "sichere" Systeme sind 1983 in den TCSEC (Trusted Computer System Evaluation Criteria), allgemein bekannt als "Orange Book", erstmalig beschrieben worden. Sie dienten zur Bewertung von Betriebssystemen. Weitere "farbige" Dokumente bauen auf dem "Orange Book" auf und dienen z.B. zur Bewertung von "sicheren" Netzwerken und Datenbanksystemen. Seit der Errichtung des BSI im Jahr 1991 wird auch dort kontinuierlich an Regelwerken und Prüfvorgaben für standardisierte Sicherheits- (Software-) Produkte gearbeitet, z.B. IT-Sicherheitskriterien, IT- Evaluationshandbuch, die es ermöglichen, Anwendern geprüfte und zertifizierte Produkte zur Verfügung zu stellen. Im Zuge der internationalen Harmonisierung dieser Vorschriften wurden zunächst die europäischen "Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik" (ITSEC) erarbeitet. Die in den IT-Sicherheitskriterien (ITS) und den ITSEC definierten Grundfunktionen sicherer Systeme (und deren Prüfung) sind in verschiedenen Grafiken dargestellt (vgl. S. 68 - 72).

Im Jahr 1996 wurde die Version 1.0 der "Common Criteria for Information Technology Security Evaluation" (CC) vorgestellt, die nach Abschluß der Probeanwendung die europäischen ITSEC, das "Orange Book" und die kanadischen Kriterien (CTCPEC) ablösen sollen. An der Erstellung dieser Richtlinien waren die USA, Kanada, Großbritannien, Frankreich, die Niederlande und die Bundes-republik Deutschland beteiligt. Ohne auf die komplizierten Details dieser Vor-schriften einzugehen, kann generell gesagt werden, daß damit die Funktionali-tät und die Vertrauenswürdigkeit von IT-Sicherheitsprodukten bewertet werden können. Die Prüfung der Sicherheitsvorgaben gewährleistet, daß die Sicher-heitsfunktionen korrekt umgesetzt werden. Außerdem wird deren Wirksamkeit als Sicherheitsmaßnahmen überprüft und bewertet. Im Ergebnis bleibt festzu-halten, daß durch solche Regelwerke eine breite Basis für standardisierte Soft-ware und andere Sicherheitsprodukte erreicht werden kann. Je häufiger bereits geprüfte, handelsübliche Produkte zu einem erschwinglichen Preis am Markt verfügbar sind, desto größer ist auch die Bereitschaft diese, und nicht "unsichere", einzusetzen.

I. Kriterien der Funktionalität	
Grundfunktionen sicherer Systeme:	
Identifikation	Bestimmung der Identität eines Subjekts
Authentisierung	Nachweis der angegebenen Identität
Rechteprüfung / Rechteverwaltung (Zugriffskontrolle)	Überprüfung, ob ein bestimmtes Subjekt die Berechtigung hat, in der beabsichtigten Art auf das gewünschte Objekt zuzugreifen; Verwaltung der Rechtebeziehungen zwischen Subjekten und Objekten
Beweissicherung (Protokollierung)	a) allgemeine Beweissicherung (Accounting), d.h. generelle Aufzeichnung aller ausgeübten Rechte b) Protokollauswertung (Auditing), d.h. Entdeckung und Auswertung sicherheitsrelevanter Ereignisse, insbesondere der Ausübung nicht zugestandener Rechte
Wiederaufbereitung	Aufbereitung wiederverwendbarer Betriebsmittel vor dem nächsten Gebrauch
Unverfälschtheit	Gewährleistung der Unverfälschtheit und Konsistenz von Daten
Fehlerüberbrückung	Begrenzung der Auswirkungen von Fehlverhalten des Systems (Erkennung und Überbrückung)
Gewährleistung der Funktionalität	Garantie der korrekten Funktionsweise unverzichtbarer Systemkomponenten
Übertragungs-sicherung	Sicherung der Daten beim Transport auf Übertragungswegen durch a) Authentisierung auf Partnerebene, d.h. Garantie, daß während einer Datenübertragung auch tatsächlich die gewünschten Partner miteinander kommunizieren b) Zugriffskontrolle, d.h. Ausschluß der unberechtigten Verwendung von Betriebsmitteln der Datenübertragung c) Vertraulichkeit von Daten (Geheimhaltung der Daten während der Übertragung) d) Integrität von Daten, d.h. an allen dazu erforderlichen Stellen bei der Übertragung müssen die relevanten Daten aus dem Datenstrom rekonstruierbar sein e) Authentisierung des Senders von Daten, d.h. Identifizierung und Authentifizierung des Urhebers eines Datenstromes f) Anerkennung von Daten, d.h. Nachweis des Ursprungs und des Empfangs von Daten

Die Funktionalitätsklassen nach ITS / ITSEC/"Orange Book" im einzelnen				
ITS	*ITSEC*	*Orange Book*	*Erläuterungen*	
F1	F-C1	C1	typisch für Daten-	diese sind im wesentlichen
F2	F-C2	C2	schutzanforderungen	für Betriebssysteme ge-
F3	F-B1	B1	typisch für die	dacht; hierbei steht die
F4	F-B2	B2	Verschlußsachen-	Vertraulichkeit von Daten
F5	F-B2	B3	bearbeitung	im Vordergrund
F6	F-IN	--	Integrität (z.B. Datenbanken, Softwareentwicklungsumgebung)	
F7	F-AV	--	Verfügbarkeit (Fehlerüberbrückung, Gewährleistung der Funktionalität, z.B. bei Prozeßrechnern)	
F8	F-DI	--	Integrität (Identifikation und Authentisierung für beide Partner einer Kommunikation, Übertragungssicherung, Beweissicherung)	
F9	F-DC	--	Vertraulichkeit (Verschlüsselung von Nutzdaten)	
F10	F-DX	--	Zusammenfassung von F8 / F-DI und F9 / F-DC	

II. Qualitätskriterien	
1. Kriterien der Korrektheit	*2. Kriterien der Wirksamkeit*
- Qualität der Sicherheitsanforderungen	- Zuordnung verschiedener Grundfunktionen zueinander und ihre inneren Abhängigkeiten (vordefinierte Funktionalitätsklassen)
- Qualität der Spezifikation der zu evaluierenden Systemteile	- geeignete Auswahl von Grundfunktionen im Hinblick auf die vorab analysierten Bedrohungen
- Qualität der verwendeten Mechanismen	- Integration der verschiedenen Funktionen zu einem wirksamen System
- Qualität der Abgrenzung zu nicht zu evaluierenden Systemteilen	- dort, wo nötig, gegenseitige Unterstützung der einzelnen Funktionen
- Qualität des Herstellungsvorgangs	- im Zusammenhang mit der Bewertung der Korrektheitsaspekte werden eine Reihe von Anforderungen zur Wirksamkeit gestellt
- Betriebsqualität	
- Qualität der anwenderbezogenen Dokumentation	

Die Qualitätsstufen nach ITS / ITSEC im einzelnen			
ITS		*ITSEC*	
Q 0	unzureichend	E 0	unzureichend
Q 1	getestet	E 1	getestet
Q 2	methodisch getestet	E 2	methodisch getestet, Konfigurationskontrolle und kontrollierte Verteilung
Q 3	teilanalysiert	E 3	teilanalysiert (Schaltpläne, Quellcode)
Q 4	informell analysiert	E 4	formales Sicherheitsmodell, Spezifikation / Quellcode
Q 5	semi-formal analysiert	E 5	nachvollziehbare Abbildung, Spezifikation / Quellcode
Q 6	formal analysiert	E 6	Anforderungen und Grobspezifikation in formaler Notation, Konsistenz mit dem formalen Sicherheitsmodell nachweisbar
Q 7	formal verifizierbar	---	---

III. Mechanismen					
Stärke von Mechanismen					
Methoden, Verfahren, Algorithmen etc., mit denen bestimmte Sicherheitsfunktionen in einem IT-System realisiert werden, werden als Mechanismen dieser Grundfunktionen bezeichnet. Diese können unterschiedlich stark ausgeprägt sein, d.h. verschieden hohe Hürden gegenüber Manipulationsversuchen aufbauen.					
Bewertungsskala					
ITS			ITSEC		
1.	ungeeignet	erfüllt nicht die Anforderungen	1.	niedrig	Schutz gegen mehr zufällige Verstöße (insbesondere Bedienungsfehler)
2.	schwach	Abwehr unbeabsichtigter Verstöße	2.	mittel	hält Angriffsversuchen von Experten mit begrenzten Möglichkeiten und Mitteln stand
3.	mittelstark	Schutz bei absichtlichen Verstößen; mit mittlerem Aufwand und normalen Systemkenntnissen zu überwinden	3.	hoch	hält erfahrenen Experten mit praktisch unbegrenzten Ressourcen stand
4.	stark	guter Schutz bei absichtlichen Verstößen; nur mit großem Aufwand bzw. unter Zuhilfenahme aufwendiger Hilfsmittel zu überwinden			
5.	sehr stark	sehr guter Schutz bei absichtlichen Verstößen; nach dem Stand der Technik nur mit sehr großem Aufwand und unter Zuhilfenahme sehr aufwendiger Hilfsmittel zu überwinden			
6.	nicht überwindbar	zur Zeit nicht überwindbarer Schutz			

Mechanismen und Qualitätsstufen (Zusammenfassung)							
gering			zufriedenstellend		gut bis sehr gut	ausgezeichnet	
ITS	Q1		Q2		Q3 - Q4 - Q5	Q6	Q7
ITSEC	E1			E2	E3 - E4 - E5	E6	
niedrig			mittel			hoch	

Vergleich ITS/"Orange Book"								
ITS	--, Q0	--, Q1	F1, Q2	F2, Q2	F3, Q3	F4, Q4	F5, Q5	F5, Q6
"Orange Book"	D	---	C1	C2	B1	B2	B3	A1

Die nach den bisher gültigen Vorschriften (ITSEC) geprüften (zertifizierten) Produkte können beim BSI bezogen oder über die zuständige Landesverfassungsschutzbehörde erfragt werden. Außerdem werden vom BSI regelmäßig aktuelle Listen der freigegebenen Erzeugnisse veröffentlicht bzw. können über die BSI-Mailbox abgerufen werden.

Bei der Verarbeitung sensibler Daten sollten grundsätzlich zertifizierte Betriebssysteme zum Einsatz kommen. Sofern Verschlußsachen verarbeitet werden, ist der Einsatz solcher Systeme sogar zwingend vorgeschrieben. Produkt- und Maßnahmenauswahl sollten jedoch frühzeitig (in der Planungsphase) im Rahmen einer DV-Geheimschutzberatung erörtert werden.

3.2 Anwendungssoftware

Mit Hilfe der Anwendungssoftware werden unmittelbar mit der betrieblichen Abwicklung verbundene Aufgaben gelöst. Beispiele hierfür sind: Textverarbeitungs-, Tabellenkalkulations-, Zeichen-, Datenbankprogramme, graphische Benutzeroberflächen usw. Anhand der am Beispiel von Betriebssystemen aufgezeigten Prüfkriterien werden heutzutage auch solche Anwendungsprogramme geprüft und zertifiziert.

Zwar können diese Programme den geprüften Sicherheitskern von Betriebssystemen nicht manipulieren, jedoch erwachsen aus ihnen andere Sicherheitsrisiken. Bei einem Datenbankprogramm muß beispielsweise geprüft werden, wie die Zugriffsrechte auf einzelne Datensätze und -felder umgesetzt werden, wie sie eingestuft sind, und wie die internen Abfrageprozeduren ablaufen. Zusätzliche Sicherheitssoftwareprodukte (Add Ons) müssen auf die Einhaltung ihrer Sicherheitsfunktionalitäten, die "Stärke" der hierfür eingesetzten Mechanismen und ihre Wirksamkeit im Zusammenspiel mit anderen Soft- und Hardwareeinrichtungen getestet werden. Neben den klassischen Softwareprodukten können grundsätzlich alle IT-Produkte (Hardware, Software, Kombinationen aus beiden, PC-Sicherheitsprodukte, Betriebs- und Netzwerkbetriebssysteme, Netzwerk-Karten, -Router, -Bridges, -Gateways, Chipkartenleser, Smart-Cards, Zugangskontrollanlagen, Datenbanken, Steuerungs- und Kontrollsysteme, X.25- und X.400-Produkte, Büro- und Telekommunikationseinrichtungen u.v.a.m.) nach den ITSEC zertifiziert werden. Die ganze Palette der geprüften Produkte kann, wie bereits erwähnt, beim BSI erfragt werden. Insbesondere standardisierte PC-Sicherheitsprodukte erleichtern den Umgang mit sicherheitsrelevanten Daten. Sie bieten eine geprüfte Sicherheit, sind relativ einfach zu implementieren und verfügen über einen anwenderorientierten Benutzungskomfort. Auch durch Verlage und Verbände (z.B. Soft- und Hardware-Enquête des "Sicherheitsberaters", Sicherheitsproduktliste der "Gesellschaft für Datenschutz und Datensicherung e.V." - GDD, Studie des "Betriebswirtschaftlichen Instituts für Organisation und Automation an der Universität zu Köln" - BIFOA) werden regelmäßig Informationen zu sicheren Produkten veröffentlicht.

3.3 Programm-Manipulationen

Manipulationen an Softwareprogrammen können sowohl die Vertraulichkeit und die Integrität der Daten als auch die Verfügbarkeit der IT-Systeme gefährden. Die Initiierung solchermaßen vorgetragener Angriffe kann sowohl von Innen- wie von Außentätern erfolgen. Angriffe von Innentätern können z.B. sein: Einspielen nicht authorisierter Softwareprodukte, Veränderungen an bestehenden

Programmen, Manipulationen an internen Steuerungseinrichtungen, Speicherung oder Weiterleitung von Daten an Unbefugte und die Schaffung von Zugangs- und Zugriffsmöglichkeiten für externe Angriffe. Die dargestellten Angriffsziele gelten im übrigen auch für externe Angreifer, die durch "Hacking" versuchen, IT-Systeme und deren Programme zu manipulieren. Für den Anwender spielt dabei weniger eine Rolle, ob diese Manipulationen der Ausspähung von Daten durch Datenspione oder durch "normale" Hacker dienen, die sich kostenlose Rechnerleistung, interessante Softwareentwicklungen und Pin-Nummern, z.B. von Kreditkarten, zur Leistungserschleichung verschaffen oder durch ihre Angriffe Daten verändern, manipulieren oder gar löschen wollen. Der hierdurch entstehende Schaden ist in jedem Fall beträchtlich. Angriffe von Außentätern richten sich u.a. auch gegen Telekommunikationseinrichtungen und insbesondere deren Programme. Durch gezielte Manipulationen über direkte Anschlüsse (ISDN, andere öffentliche und private Netze) oder über Fernwartungszugänge werden Leistungsmerkmale der Anlagen so verändert, daß z.B. Raumgespräche mitgehört, Ferngespräche abgehört oder Verbindungsdaten erfaßt werden können.

3.3.1 Sabotage

Durch gezielte Programm-Manipulationen können IT- und TK-Systeme in ihrer Verfügbarkeit stark beeinträchtigt werden. Dies kann letztlich dazu führen, daß diese dann insgesamt oder teilweise über längere Zeit nicht mehr einsatzfähig sind. Eine anonyme Hackergruppe, die sich selbst "Darkspace" nennt, hat zu Beginn des Jahres durch Manipulationen von Internet-E-Mail-Adressenlisten die Rechner der sog. CyberAngels zumindest teilweise lahmgelegt. Bei den "CyberAngels" handelt es sich interessanterweise um eine Gruppe von Freiwilligen, die seit 1995 versucht, im Internet verbotene pornographische Darstellungen, jugendgefährdende Angebote oder "hate-mail" aufzuspüren und Computerkriminalität sowie Online-Mißbrauch einzudämmen. Dabei spüren sie auch Hackern und Virenprogrammierern nach. Bei Manipulationen durch den vielfach in der Presse zitierten "Michelangelo-Virus" wird am 6. März eines jeden Jah-

res die Festplatte mit zufällig ausgewählten Zeichen komplett überschrieben. Welche Dimensionen Sabotagehandlungen durch Programm-Manipulationen annehmen können, kann leicht daran gemessen werden, wenn zu einer definierten Zeit, z.B. in Not- und Katastrophenfällen, lebens- und auch verteidigungswichtige IT- und TK-Systeme "plötzlich" und unvorhergesehen nicht mehr funktionieren. Schutzmaßnahmen gegen Angriffe dieser Art werden in den Teilen "Hacker" und "Netze" vorgestellt bzw. wurden im Abschnitt "Bedrohungen und Schutzmaßnahmen" bereits behandelt.

3.3.2 Viren, Minen, Trojanische Pferde

Die derzeit bekanntesten Programm-Manipulationen gehen fast ausschließlich von Computerviren oder anderen artverwandten Erscheinungen aus. Die bekanntesten dieser Manipulationsarten sollen hier dargestellt werden.

Trojanische Pferde ("trojan horses")

Diese sind Programme oder Teile hiervon, die augenscheinlich eine bestimmte Aufgabe lösen, statt dessen aber unbemerkt zusätzlich oder anstelle der vorgetäuschten Aufgabenerledigung vordefinierte Aufgaben ausführen oder Schäden anrichten, z.B. Computerspiele, die nebenher Dateien durchforsten, kopieren oder zerstören.

Logische "Bomben" ("logical bombs")

Diese verfügen über nahezu ähnliche Schadfunktionen wie trojanische Pferde. Die Schadfunktion selbst wird dabei wie bei einer herkömmlichen Bombe durch einen Zünder (trigger) ausgelöst. Dieser Zünder wird durch den Programmierer auf ein bestimmtes Signal oder einen bestimmten Auslöser programmiert. Eine Zündung erfolgt deshalb entweder durch den "Bomben"-Programmierer selbst oder durch eine Aktion des Anwenders.

Falltüren ("trap doors")

Falltüren dieser Art schaffen unbemerkte Zugänge zu IT-Systemen. Sie werden im täglichen Betriebsablauf nicht benötigt, sind aber trotzdem vorhanden. Beispiele hierfür sind durch Programmierer von Betriebssystemen voreingestellte "Notzugänge" die unter Umgehung des Zugriffsschutzes einen einfachen Zugriff, beispielsweise über Wartungs- oder Fernwirkschnittstellen, ermöglichen sollen.

"Würmer"

Wurmprogramme können von sich selbst Kopien erstellen. Im Gegensatz zu Computerviren infizieren sie aber keine anderen Programme, sondern laufen als eigenständige ab. Durch die ständige Reproduktion und die damit verbundene unkontrollierte Ausbreitung können IT-Systeme so stark überlastet werden, daß ein ordnungsgemäßer Betrieb nicht mehr möglich ist.

Computerviren

Nach allgemeiner Definition ist ein Computervirus eine "nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt". Viren bestehen in der Regel aus einem Reproduktionsteil zur Vermehrung des Virus, einem Erkennungsteil, in dem geprüft wird, ob bereits eine Infektion eines anderen Programms oder Systembereichs erfolgt ist, einem Schadensteil, in dem zumeist absichtliche Schadfunktionen (Überschreiben, Verändern von Programmen oder Daten) programmiert sind, einem Bedingungsteil, in dem z.B. Schadfunktionen in Abhängigkeit von bestimmten Ereignissen (Datum, Anzahl von Aufrufen etc.) vordefiniert sind sowie einem Tarnungsteil, der die Entdeckung des Virus im System erheblich erschweren kann. Die beiden Grundtypen von Viren sind Boot- und File-Viren.

Boot-Viren überschreiben den Boot- oder Partitionssektor mit ihrem Programm. Der Inhalt wird im Original an eine andere Stelle auf dem Datenträger verlagert;

mit dem Einschalten des Geräts wird zunächst der Virus-Code aktiviert und ausgeführt; anschließend erfolgt der normale Start des Rechners. Boot-Viren werden durch das "booten" (Laden des Betriebssystems in den Arbeitsspeicher) mit infizierten Disketten verbreitet. Nach dem Start des Rechners von einer infizierten Diskette wird der Virus sofort im Speicher resident und auf die Festplatte übertragen. Die Boot-Sektoren anschließend verwendeter, nicht schreibgeschützter Disketten werden ebenfalls infiziert. File-Viren lagern sich meistens an Programmdateien an. Beim Aufruf des infizierten Programms wird dabei zuerst der Virus-Code ausgeführt, dann läuft das Programm wie gewohnt ab. Aktiviert werden File-Viren durch den Aufruf des infizierten Programms, z.B. durch eine Diskette. Die Übertragung von File-Viren kann jedoch auch über Datenfernübertragung (Modem) oder durch File-Server in Netzwerken erfolgen. Nach dem ersten Aufruf eines infizierten Programms können dann andere Programm- oder Systembereiche ebenfalls infiziert werden. Schäden, die durch Computerviren entstehen, erreichen allein in der Bundesrepublik Deutschland jährlich dreistellige Millionenbeträge. Quellen von Computerviren sind neben Software-"Raubkopien" auch Originalsoftwareprodukte, auf Rechnern beim Kauf vorinstallierte Software sowie Prüfdisketten von Wartungs- und Servicetechnikern.

Die wesentlichen Aspekte zum Problem der Computerviren sind in der BSI-Schriftenreihe zur IT-Sicherheit, Band 2, dargestellt. Grundschutzmaßnahmen ergeben sich aus den nachfolgenden Kurzhinweisen:

- Datensicherung; von wichtigen Daten sollten mindestens 2 Sicherungskopien existieren, um bei Datenverlusten durch Virenbefall Daten schnell rekonstruieren zu können
- ausschließliche Verwendung von schreibgeschützten Disketten verhindert eine Infektion
- Einsatz von aktueller Anti-Virus-Software
- Bezug von Disketten und andere Datenträger nur aus seriösen Quellen
- Prüfung ein- und ausgehender Disketten (wo notwendig mit Schreibschutz versehen)

- Ändern der Boot-Reihenfolge des Rechners im CMOS-RAM auf "C: , A:"

- Einrichten von mehreren Partitionen (logische Laufwerke)

- Zugangs- und Zugriffsschutz für den Rechner gegen mißbräuchliche Benutzung

- sichere Aufbewahrung von Datenträgern

- Einrichten eines besonderen Viren-Erkennungs- und Bekämpfungsservice

- Erstellung einer Notfall-Diskette (ausführliche Beschreibung im BSI-Heft)

- Maßnahmen bei erkanntem Befall:

  - Ruhe bewahren
  - Rechner ausschalten
  - Fachleute zu Rate ziehen
  - von virenfreier, schreibgeschützter System-Diskette booten
  - Viren- Suchprogramm einsetzen
  - Virus entfernen, mit Viren-Suchprogramm erneut prüfen
  - Daten sichern (falls nicht vorhanden)
  - alle Datenträger untersuchen und ggf. Virus entfernen
  - versuchen, die Quelle der Infektion zu lokalisieren
  - andere Benutzer (bei Datenträgeraustausch) warnen
    Hersteller oder BSI informieren (bei Programm-Disketten), Ersteller informieren (bei Daten-Disketten)

Virensuchprogramme (Viren-Erkennungsprogramme, Viren-Scanner, Viren-Finder etc.) sind wertvolle Hilfsmittel beim Erkennen und Bekämpfen von Computerviren. Bei komplexeren IT-Anwendungen sollte darauf geachtet werden, daß nicht nur die jeweils aktuellste Version zum Einsatz kommt, sondern auch mehrere (mind. zwei, besser drei) Produkte verschiedener Hersteller benutzt werden. Außerdem sollten bei großen, sensiblen Systemen mit hohem Datenträgeraustausch sämtliche ein- und ausgehenden Disketten (oder andere Datenträger) bereits beim Posteingang (oder Ausgang) abgefangen und auf Viren überprüft werden, bevor sie an den eigentlichen Empfänger gelangen. Das Einbringen oder Nutzen nicht authorisierter Software sollte verboten werden. In

vernetzten Systemen kann es sehr sinnvoll sein, zu prüfen, ob nicht Rechner ohne Diskettenlaufwerk eingesetzt werden können. Das BSI hat dazuhin seine "Forderungen an Viren-Suchprogramme" auf der Basis der ITSEC aktualisiert und veröffentlicht die nach diesen Kriterien geprüften Produkte in einer Publikation zu IT-Sicherheitsprodukten.

Im Zuge der weltweiten Vernetzung von Systemen und dem offenen Nachrichtenaustausch kommt den Mailboxen im Rahmen der Virenproblematik in zweierlei Hinsicht besondere Bedeutung zu. Zum einen kann aus solchen Mailboxen eine Vielzahl von häufig virenverseuchten Softwareprogrammen (Shareware, Public Domain) heruntergeladen werden. Zum anderen haben sich Mailboxen auch als hervorragendes Instrument für die gezielte Verbreitung von Viren, Programmen und Programmiertechniken zur Virenerstellung, Virensourcecodes sowie dem Informationsaustausch von Virenprogrammierern erwiesen.

Vier Beispiele aus der Praxis sollen verdeutlichen, wie hoch das Risiko einer Virusinfektion tatsächlich ist, und wie leicht so etwas selbst bei Softwarebezug aus seriösen Quellen passieren kann:

- Im April 1994 verteilte ein Computerhersteller anläßlich einer Informationsveranstaltung zu einem neuen Produkt auch eine Demo-Diskette. Neben den Produktinformationen war auf der Diskette ein "Parity"- (Boot-) Virus zu finden.

- Die Zeitschrift "PC-Professional" verteilte im September 1994 an rund 30.000 Abonnenten eine Diskette mit Scherzprogrammen zu Windows. Bei der Duplizierung der Masterdiskette (zwei Kopien) wurde ein mit dem "Parity Boot B"-Virus infizierter PC eingesetzt. Ergebnis: 10.000 einwandfreie und 20.000 infizierte Disketten.

- Microsoft Großbritannien verteilte Ende Februar 1995 an ca. 200 führende britische Software-Entwickler Disketten mit Beispielsprogrammen zur geplanten Einführung von Windows 95. Die Disketten enthielten neben den Demoprogrammen auch den "Form"- (Boot-) Virus, der zu den verbreitetsten überhaupt gehört

- Mercedes-Benz Deutschland verteilte Ende April 1995 an Journalisten etwa 2.000 Pressemappen mit Informationen zur neuen E-Klasse. Die

beigefügte Diskette enthielt dabei nicht nur dahingehende Informationen, sondern auch einen "Stoned"- (Boot-) Virus.

Eine neuartige Form der Viren soll hier noch kurz beleuchtet werden. Makroviren sind Viren, die nicht ausführbare Dateien infizieren, sondern Dokumente. Sie reproduzieren sich mit Hilfe der Makrosprache und den dazugehörigen Aplikationen. Für die Virenprogrammierer ist dabei von Vorteil, daß diese Viren sehr einfach zu programmieren sind. Der weltweit erste und heute mit am meisten verbreitetste Makro-Virus ist der WinWord-Concept-Virus. Inzwischen exisitieren bereits mehr als 50 solcher Makro-Viren-Typen die teilweise erhebliche Schäden verursachen können. Gefährlich sind diese Virentypen deshalb, weil viele E-Mails als Word-Dateien verschickt werden. Eine große Zahl von Mailprogrammen öffnet zum Betrachten des Mail auch die dazugehörige Anwendung (z.B. WinWord) und infiziert dabei die Systeme. Eine hohe, weltweite Infektionsgefahr in sehr kurzen Zeiten ist deshalb möglich. Eine Beseitigung bei erkanntem Makro-Virenbefall sollte nur durch Fachleute vorgenommen werden.

Als Fazit bleibt festzuhalten, daß die Gefahr durch Programm-Manipulationen, insbesondere durch Computerviren, nicht unterschätzt werden darf. Relativ einfache organisatorische und technische Maßnahmen, wie sie in diesem Teil und auch in der BSI-Veröffentlichung vorgestellt wurden, können IT-Systeme jedoch wirkungsvoll schützen. Die Entwicklung von Schutzmaßnahmen und Anti-Viren-Produkten ist aber auch abhängig von der Kenntnis konkreter Fälle. Bei einem Virenbefall, insbesondere, wenn keine Kenntnisse über die Bekämpfung von Viren vorhanden sind, sollten in jedem Fall Fachleute hinzugezogen werden.

3.3.3 Hacker

In den vorangegangenen Abschnitten wurde immer wieder auf die Gefahr durch externe Angreifer und die Möglichkeiten, durch solche Angriffe an sensible Daten zu gelangen, hingewiesen. Aus Sicht der Bekämpfung der Computerspionage kommen für solche Attacken durch Hacker zwei potentielle Tätergruppen in Betracht. Datenspione versuchen, möglichst unbemerkt über einen längeren

Zeitraum Daten auszuspähen. Datensaboteure verändern oder manipulieren Daten, Programme sowie IT-Systeme und gefährden dadurch insbesondere die Verfügbarkeit des attackierten IT-Systems. Grundsätzliche Zielrichtung von Hackern ist, durch einen externen Zugriff die komplette Kontrolle über das gehackte System zu übernehmen. Neben dem im Teil 1 ausführlich beschriebenen "KGB-Hacker-Fall" machten in der jüngsten Vergangenheit besonders die nachfolgend dargestellten Hackerfälle Schlagzeilen:

- Am 25. Dezember 1994 gelang es Hackern, für mehr als einen Tag die Kontrolle über einen Rechner des Computersicherheitsexperten Tsuomu Shimomura vom amerikanischen San Diego Supercomputer Center zu übernehmen. Dabei kopierten sie eine große Zahl von Sicherheitsprogrammen. Der Angriff erfolgte über das Internet, der Zugriff auf den Rechner wurde mittels "spoofing" (spoof = Parodie), d.h. über Datenpakete mit maskierten IP- (Internet-Protokoll-) Adressen, realisiert. Firewall Systeme (Schutzsysteme für Netze), die nicht speziell gegen diese Art von Attacken konfiguriert sind, können damit ebenfalls überwunden werden. Nur mit Hilfe von Shimomura gelang es FBI-Agenten und US-Marshalls, den vielgesuchten Hacker Kevin David Mitnick zu ermitteln und festzunehmen. Dieser soll u.a. auch den Command Computer des North American Air Defense (NORAD) geknackt haben (Vorbild für den Spielfilm "Wargames") und 1992 in den Rechner der Kommunikationsgesellschaft Pacific Bell eingedrungen sein. Die Bell-Attacke erfolgte während seiner Bewährungsstrafe für einen Hack-Diebstahl von Sicherheitssoftware bei der Firma Digital Equipment im Wert von 1 Million US-Dollar.

- Ein anderer amerikanischer Computer-Hacker, Kevin Lee Poulsen, wurde Mitte April 1995 von einem Gericht in Los Angeles zu 51 Monaten Haft mit drei Jahren Bewährung sowie einem Bußgeld in Höhe von 58.000 US-Dollar verurteilt; dies ist die bis dahin höchste Strafe, die ein US-Gericht gegen einen Hacker verhängt hat. Poulsen hatte u.a. geheime Air-Force-Unterlagen gestohlen und durch Hacking von Telefon-

anlagen verschiedener Radiostationen (die einen Gewinn für den ersten Anrufer zu einer bestimmten Uhrzeit bereithielten) Gewinnspiele manipuliert. Er blockierte dabei bestimmte Telefonleitungen und war somit immer der erste Anrufer. Die dabei erzielten Gewinne waren beträchtlich (zwei Porsche, 22.000 US-Dollar, zwei Hawaii-Reisen) .

- Ein unbekannter australischer Hacker brach Mitte April 1995 in einen Rechner des Internet-Service-Providers AUSnet in Sydney ein; dabei hackte er ca. 1.400 Kreditkartennummern. Welche finanziellen Schäden weltweit damit angerichtet werden können, läßt sich sehr leicht nachvollziehen.

- Mitte März 1996 drangen Hacker in das Computersystem des amerikanischen Los Alamos National Laboratory ein. Selbst mehrere Firewallsysteme wurden dabei mit Leichtigkeit überwunden. Die zum Angriff erforderliche Software stand in einer Internet-Mailbox zum Abruf zur Verfügung. Schäden oder Datendiebstähle waren jedoch nicht zu verzeichnen.

Festzuhalten bleibt, daß Hacker nicht vor geschützten Systemen Halt machen und auch durchaus in der Lage sind, diese zu knacken. Insbesondere Studenten nutzen immer wieder Rechner von Universitäten zu Hacking-Attacken. Über Internet-Mailboxen werden dann weltweit Programme zum Hacken von Paßworten, gehackte Paßwörter, Anleitungen für Hacking-Angriffe, Virenbauprogramme, Kreditkartennummern, Telefonnummern für den Gebührenbetrug u.v.a. mehr angeboten.

Schutzvorkehrungen gegen Hackerangriffe sind teilweise an anderen Stellen der Broschüre ausführlich beschrieben. Die Maßnahmen, Hackerangriffe abzuwehren, Schadensrisiken zu minimieren oder zumindest Angriffe zu erkennen, werden nachfolgend in konzentrierter Form dargestellt:

- zertifizierte Zugriffsschutzeinrichtungen für IT-Systeme
- Sicherung sämtlicher externer Zugangsmöglichkeiten
- Einsatz von Firewall-Systemen
- Verschlüsselung von Daten und Dateien intern und bei der Übertragung
- Protokollierung und Auswertung von System- und Übertragungsprotokollen
- regelmäßige Datensicherung
- Paßwort- und Sicherheitsmanagement
- regelmäßige interne Revision durch Fachpersonal

Bei Hackerangriffen durch Innentäter, die einen geschätzten Anteil von 60 % aller Angriffe ausmachen, helfen in der Regel nur gezielte und durchdachte Zugriffsbeschränkungen. Schon bei der Erstellung des Sicherheitskonzepts sollte genau festgelegt werden, wer wann unter welchen Voraussetzungen legalen Zugriff auf Daten und Dateien haben soll. Protokollierungseinrichtungen helfen im Rahmen der Beweissicherung, unbefugte Zugriffe zu erkennen und nachzuweisen. Zugriffsschutzeinrichtungen sind insbesondere auch bei den Nutzung von Kommunikationseinrichtungen notwendig. Nicht jeder braucht den umfassenden Zugriff auf Netze und Dienste des Unternehmens oder der Behörde und schon gar nicht auf weltweite Serviceeinrichtungen und Dienste wie z.B. das Internet. Sensible Daten innerhalb der Organisation können letztlich nur durch eine hochwertige Verschlüsselung vor mißbräuchlicher Nutzung geschützt werden. Personal mit übergeordneter oder umfassender Zugriffsberechtigung (z. B. Programmierer, System- und Sicherheitsadministratoren) sollte bei bekanntgewordener Beendigung des Arbeitsverhältnisses durch Kündigung oder Entlassung möglichst schnell der Zugriff auf das System entzogen werden. Notfalls müssen diese Personen bis zu ihrem Ausscheiden freigestellt werden. Gerade unzufriedene Mitarbeiter versuchen am Ende ihrer Tätigkeit immer wieder, ihr "geistiges Eigentum" und andere wichtige Daten ggf. zum neuen Arbeitgeber (Konkurrent) mitzunehmen, oder sie hinterlassen auf den IT-Systemen manipulierte Programme, die zu unliebsamen Überraschungen führen können.

4. Netze

4.1 Täterbild

Bei allen Angriffen im Rahmen der computerunterstützten Spionage können bezüglich der Täter folgende Kernaussagen gemacht werden. Die Angriffe erfolgen zumeist unbemerkt, d.h. es ist von einer sehr hohen Dunkelziffer (ca. 85 %) auszugehen. Das Entdeckungsrisiko für einen Außentäter ist erheblich verringert, denn selbst wenn ein Angriff im System bemerkt wird, läßt dies regelmäßig noch keinen Rückschluß auf einen konkreten Täter zu. Die Verfolgung von Angriffswegen über Netze der Daten-Fern-Übertragung (DFÜ) ist schwierig. Täter, die über die DFÜ in Systeme eindringen, können sehr leicht ihren Weg durch die Netze verschleiern. Im Zuge einer weltweiten offenen Kommunikation sind die Zugangsmöglichkeiten zu diesen Netzen nahezu für jedermann ungehindert möglich und erwünscht. Dabei sind Fachkenntnisse kaum erforderlich, die finanziellen Aufwendungen für einen - auch professionell vorgetragenen - Angriff halten sich in Grenzen; jedenfalls ist hier der Beschaffungsaufwand wesentlich geringer als bei einem direkten - personellen - Angriff. Das Entdeckungsrisiko bei einem Innentäter, der sich nur im Rahmen seiner Zugriffsberechtigungen in den Systemen bewegt, ist so hoch oder so gering wie bei einem Innentäter ohne DV-Anknüpfungspunkte. Angriffe von Außentätern sind gewöhnlich auf kurzfristigen Erfolg ausgerichtet, Zugriffe auf sensible Informationen dadurch oft auch vom Zufall abhängig. Eine gezielte Informationsabschöpfung ist nur dort über einen längeren Zeitraum möglich, wo der Täter erkanntermaßen keine oder nur geringe Sicherheitsmaßnahmen überwinden muß. Da das Entdekkungsrisiko jedoch nicht sehr hoch ist, und im Falle einer Entdeckung der Täter in aller Regel nicht direkt ermittelt und belangt werden kann, dürften solche Angriffe (von außen per DFÜ) aggressiver vorgetragen werden.

Angriffe von Innentätern sind dagegen auf langfristigen Erfolg angelegt; sofern Informationen lediglich im Rahmen der formellen Zugriffsberechtigung des Täters abgezogen werden, ist das Entdeckungsrisiko ebenfalls als äußerst gering

anzusehen. Auch diejenigen, die (zunächst) nicht mit der Motivation "Ausspähung", sondern aus anderen Beweggründen (beispielsweise technischer Spieltrieb, Geltungssucht, Gebührenbetrug, Nutzung von Rechnerleistung auf Kosten Dritter) DV-Systeme angreifen und dabei auf sensible Informationen stoßen, können versucht sein, diese "Abfallprodukte" fremden Nachrichtendiensten oder Konkurrenzunternehmen zu verkaufen. Nicht selten werden sie - mit dem Hinweis, gegen entsprechendes Entgelt bestehende Sicherheitslücken zu schließen - sogar den Geschädigten selbst angeboten.

4.2 Struktur, Aufbau, Übertragungseinrichtungen

Netze (LAN, Per-to-Peer, Client/Server, CN, MAN, WAN) wurden bereits bei der Vorstellung der Systeme in Ziffer 2.1.3 definiert. Anhand ausgewählter Teilbereiche aus dem Gesamtkomplex "Netze" sollen nun die gebräuchlichsten Begriffe in der Netztechnologie erläutert werden.

4.2.1 Local Area Network (LAN)/Aufbau - Struktur - Topologie/Schwachstellen

Bei LAN handelt es sich um lokale, d.h. örtlich begrenzte Netze zur gemeinsamen Kommunikation von Rechnern (PC). Dabei können alle angeschlossenen Anwender Daten und Programme gemeinsam nutzen. In einem Client/Server-Konzept sind Arbeitsplatzcomputer (APC = Clients) an einen oder mehrere leistungsfähigere Zentralrechner (File-Server) angeschlossen. Dort werden für eine gemeinsame Nutzung Daten und Programme zentral für alle berechtigten Nutzer zur Verfügung gestellt. Zusätzlich können andere zentrale Abläufe durch Print- (Druck-), Datenbank- und Kommunikations-Server gesteuert werden. Die Steuerung des Netzes erfolgt mit speziellen Netzwerkbetriebssystemen; die APC werden gewöhnlich lokal mit dem Betriebssystem DOS betrieben. Bei Peer-to-Peer-Netzen sind alle angeschlossenen PC gleichberechtigt miteinander vernetzt. Damit können alle Programme und Dateien auch anderen PC zur Verfügung gestellt werden. Das eingesetzte spezielle Peer-Betriebssystem dient dazu, DOS-PC miteinander kommunizieren zu lassen. Unter dem Begriff

der Topologie versteht man die Art und Weise, wie die einzelnen Komponenten eines LAN miteinander verbunden werden. In einem Sternnetz werden alle PC über einen zentralen Rechner direkt (sternförmig) angeschlossen. Bei Ringnetzen sind sämtliche angeschlossenen Geräte ringförmig vernetzt. Wichtigster Vertreter ist das von IBM entwickelte Token-Ring-Verfahren. Busnetze verbinden die angeschlossenen PC über spezielle Netzknoten, so daß jeder mit jedem kommunizieren kann. Das hier am häufigsten eingesetzte Verfahren ist das Ethernet-Prinzip. Die einzelnen Übertragungsmedien (Kabel) innerhalb des Netzes werden in einem eigenen Abschnitt abgehandelt. Die Regelungen im Netz, wer zu welchen angeschlossenen Stationen Zugriff hat, erfolgen über Protokolle. Neben dem Busnetzprotokoll (CSMA/CD) und dem Ringnetzprotokoll (Token-Passing) wird heute meistens das TCP/IP-Protokoll (Transmission-Control-Protocol / Internet-Protocol) zur internen und externen Kommunikation zwischen heterogenen IT-Systemen eingesetzt. Die damit verbundene Übertragungtechnologie (Ethernet: IEEE 802.3 und Token-Ring: IEEE 802.5) wurde durch das "Institute of Electrical and Electronic Engineers" (IEEE) international zum Standard erhoben. Eine andere verbreitete Übertragungstechnik ist das Arcnet, das auf einer Bus-Struktur aufbaut. Zukünftig wird jedoch am häufigsten die FDDI-Technik (Fiber Distributed Data Interface) anzutreffen sein. Diese basiert auf der Lichtwellenleitertechnik (LWL) und ermöglicht eine sehr hohe Datenübertragungsrate auch über große Entfernungen.

Durch LAN potenzieren sich die am Beispiel von Stand-Alone-PC dargestellten Gefahren und Risiken, da durch die Vernetzung eine Vielzahl von Geräten von Angriffen bedroht sein kann. Zusätzlich sind die Übertragungswege und die zentralen Einrichtungen des Netzes gefährdet. Mit der Vernetzung von LAN mit anderen LAN bis hin zu weltweiten Netzverbindungen ist ein nochmaliger Anstieg der Bedrohungssituation verbunden. Als Schutzmaßnahmen für lokale Netze werden deshalb folgende Maßnahmen empfohlen:

- Sicherheit in der Kabelinfrastruktur (vgl. Ziffer 4.3)
- Zugangs- und Zugriffsschutz für zentrale Einrichtungen (Server)

- Einsatz von zertifizierten (Netzwerk-) Betriebssystemen

- Einsatz von zertifizierten PC-Sicherheitsprodukten zur Sicherung besonders gefährdeter Bereiche (z.B. Schnittstellen, Modemanschlüsse etc.)

- Protokollierung (Account- und Auditprotokollfunktion)

- Sicherung der Verfügbarkeit von zentralen Einrichtungen (Servern), z.B. durch Plattenspiegelung, Controller-Doppelung, spezielle Back-Up-Server, Server-Fehlerkorrekturverfahren, Datenspeicherung durch Disk Array-Technologie (z.B. RAID 5-Verfahren - Redundant Arrays of Inexpansive Disks); Einsatz von USV/NEA

- Datensicherung; z.B. zentrale Datenspeicherung und tägliche Datensicherung auf dem File-Server mittels automatischem Bandlaufwerk (Streamer) mit Bandkassetten (Cartridges); wöchentliche Komplettsicherung sämtlicher Daten und Programme auf allen Servern; komplette Monatssicherung

- sichere Aufbewahrung von Datenträgern, d.h. Schutz vor Wasser, Feuer, Einbruch und Diebstahl
  (Datensicherung und Datenträgerhandling werden im Anhang 1 näher erläutert.)

- Virenschutz durch Virenerkennungs-, bekämpfungs- und entfernungsprogramme sowie organisatorische Virenschutzmaßnahmen (vgl. Ziffer 3.3.2)

- Sicherheitsmanagement und -administration

- PC-, Raum-, und Gebäudeschutzmaßnahmen (vgl. Ziffer 2.3.3)

- Verschlüsselung (vgl. Abschnitt 5)

- Einsatz von Firewall-Systemen (vgl. Ziffer 4.6)

Bauliche und technische Sicherheitsmaßnahmen können nur dann ihre Schutzwirkung voll entfalten, wenn sie durch organisatorische und Kontrollmaßnahmen ergänzt und unterstützt werden. Dies können z.B. sein:

- Sensibilisierung und Akzeptanzförderung für Sicherheitsmaßnahmen beim Personal durch Schulung und Weiterbildung

- Festlegung von Kontrollen, deren Durchführung und Konsequenzen bei erkannten Verstößen

- Erstellung jederzeit revisionsfähiger Dokumentationsunterlagen

- Verzicht auf Fernwartung und allgemeine WAN-Zugriffe (Online-Dienste, Internet etc.)

- Organisatorische und personelle Trennung von Sicherheit, Betrieb und Anwendungsbereichen

- Eindeutige Regelung der Verantwortlichkeiten

- Vorschriften für die Nutzung implementierter Sicherheitseinrichtungen (z.B. Paßwortvergabe, -verwaltung, Chipkartenmanagement, Schlüsselverwaltung)

- Regelung der Kommunikationsbeziehungen (wer, wann, mit wem)

- Erstellung von Notfall- und Katastrophenschutzkonzepten (Wiederanlaufplanung)

- evtl. Abschluß von EDV-Versicherungen

Da bei marktüblichen Netzen bisher nicht alle Aspekte der Netzsicherheit berücksichtigt wurden, hat das BSI Überlegungen angestellt, ein sicheres Netz, das sog. SLAN (Secure LAN), zu entwickeln. Gedacht war dieses Netz für den Bereich des staatlichen Geheimschutzes; der Schutz der Vertraulichkeit stand deshalb im Vordergrund. Außerdem sollten sowohl Verschlußsachen- als auch offene Bereiche miteinander verknüpft werden. Auf der Basis eines handelsüblichen LAN (IEEE 802.3) werden einzelne Netzknoten mit speziellen Hard- und Softwareschutzeinrichtungen ausgestattet und VS-Server eingerichtet. Dabei wird das LAN in zwei logische Teilnetze (Verschlußsachen/VS und offener Bereich) geteilt, die physische Verbindung des Netzes jedoch aufrechterhalten. Für den VS-Teil wurden die Geheimschutzbestimmungen als Richtschnur zugrundegelegt. Mit den zusätzlichen Schutzeinrichtungen werden die Aspekte Verschlüsselung, Zugriffsschutz (Chipkarte/Passwort), Beweissicherung, Sicherheitsadministration und Schlüsselverwaltung realisiert. Auf eine tiefergehende technische Darstellung von SLAN wird an dieser Stelle verzichtet. Tests in einer Pilotanwendung haben gezeigt, daß SLAN über eine große Benutzerfreundlichkeit bei hohem Sicherheitsniveau verfügt. Die geschätzten Kosten zur Nachrüstung eines normalen Netz-PC zum VS-APC belaufen sich auf ca. 3.000 DM. Zu berücksichtigen ist dabei, daß die Ausrüstung eines bisherigen PC für die VS-Bearbeitung mit PC-Sicherheitsprodukten in etwa denselben Kostenfak-

tor mit sich bringt. Der Anteil von solchen Sicherheits-PC in einem LAN liegt nach Ermittlungen des BSI bei 10 %. Das modulare Baukastensystem des SLAN erlaubt es, das Netz sukzessive aufzurüsten und an die Sicherheitsbedürfnisse des Anwenders anzupassen. Damit können auch die zusätzlichen Kosten auf längere Sicht in einem überschaubaren Rahmen gehalten werden.

Eine nützliche Hilfe bei der Erstellung von Netzsicherheitskonzepten und der richtigen Maßnahmenauswahl bieten auch Checklisten zu Netz-Sicherheitsstandards, die in der Fachpresse immer wieder veröffentlicht werden (z.B. SecuMedia Verlags GmbH, Kommunikations- und EDV-Sicherheit/KES, Ausgabe 95/4, Seiten 16-17 und 24).

LAN können durch sog. MAN (Metropolitan Area Networks) miteinander verbunden werden. Diese Netze weisen eine große Bandbreite und Übertragungsraten von bis zu 140 Mbit/s auf. 1987 wurde das MAN-Protokoll DQDB (Distributed Queue Dual Bus) als Standard (IEEE 802.6) international anerkannt. MAN werden sowohl von privaten, als sog. Backbone-Netze, als auch von öffentlichen Trägern betrieben. Sie sind in der Lage, die in ihrer Struktur, Topologie und Übertragungstechnik teilweise sehr unterschiedlichen LAN miteinander zu verbinden.

LAN und MAN wiederum können über WAN (Wide Area Networks) praktisch weltweit verknüpft werden. Arten von WAN werden im Teil "Öffentliche Netze" näher erläutert.

Im Bereich der LAN-Technologie sind sog. Wireless LAN (drahtlose Netze) immer mehr auf dem Vormarsch. Durch den Einsatz von Infrarot-Übertragungstechniken für lokale Anwendungen, dem aus der Telefonie bekannten DECT-Standard für die mobile Datenkommunikation oder mit verteilten Frequenzband-Funk-Systemen (2,4 Gigahertz Spread Spectrum), können LAN drahtlos betrieben oder verknüpft werden. Digitale und optische (auf der Lasertechnik basierende) Richtfunksysteme kommen hierfür ebenfalls in Betracht. Aus Sicht der

Datensicherheit und des Datenschutzes sollte jedoch momentan auf den Einsatz solcher drahtloser Netze verzichtet werden. Die Abhörmöglichkeiten beim Funk und auch bei Infrarot-Systemen sind beträchtlich. Geprüfte Systeme dieser Art stehen derzeit (noch) nicht zur Verfügung.

4.2.2 Öffentliche Netze und Dienste

Öffentliche Netze sind praktisch für jedermann zugänglich. Der Verbindungsaufbau erfolgt meistens über Wählverbindungen. Solche können sich aber auch als geschlossene Benutzergruppen darstellen, zu dem nur ein beschränkter Teilnehmerkreis zugangsberechtigt ist. Ein Teil der verschiedenen Netze und Dienste wird nachfolgend erläutert:

ATM (Asynchronous Transfer Mode)

Das ATM-Netz der Deutschen Telekom ist ein universelles Breitbandnetz für die schnelle (bis 155 Mbit/s) und flexible Übertragung von Sprache, Daten und Bildern. Es eignet sich sowohl für öffentliche als auch für private (inhouse) Netze.

Breitbandnetze

Mit der Realisierung von Multi-Media-Anwendungen mußten auch entsprechend schnelle und leistungsfähige Netze zur Verfügung stehen. Als Beispiel hierfür seien genannt: ATM, B-ISDN sowie das VBN (vermitteltes Breitband-Netz), das Übertragungsgeschwindigkeiten von 2 Mbit/s. erlaubt. Sie basieren auf der flächendeckenden Einrichtung von Glasfaserverbindungen und entsprechend standardisierten Übertragungsverfahren. Mit diesen Netzen werden auch die Begriffe Datenautobahn/Datenhighway verbunden. Das neue B-WiN (Breitband-Wissenschafts-Netz) des DFN-Vereins (Verein zur Förderung eines Deutschen Forschungsnetzes e.V.) verbindet ca. 40 deutsche Hochschulen, Forschungsinstitute und wissenschaftliche Rechenzentren. Es ist damit das weltweit größte flächendeckende Kommunikationsnetz auf ATM-Basis.

Btx (Bildschirmtext)

Der ehemalige Dienst der Telekom wurde über Datex-J bis hin zum neuen Online-Dienst "Telekom Online" zu einem Informations- und Dienstleistungsforum ausgebaut, der auch über einen Internetanschluß verfügt. Dabei wird ein WAN-Rechnerverbund als Kommunikationsinfrastruktur genutzt.

Datex-M

Bei Datex-M erfolgt die Datenübertragung durch Breitbandkommunikation. Mittels dieser Datenautobahn können regionale und überregionale LAN verbunden werden. Der in Datex-M international standardisierte SMDS (Switched Multimegabit Data Service) und seine Basistechnologie (DQDB und ATM) garantieren eine volle Kompatibilität zu ATM-Netzen.

Datex-P

Das Datex-P-Netz ist ein öffentliches deutsches Wählnetz, in dem Daten paketvermittelt nach dem CCITT-Standard (Comité Consultatif International de Telegraphique et Telephonique) X.25 übermittelt werden. Nach Untersuchungen des BSI ist in paketvermittelten (X.25) Netzen das Risiko des unbefugten Zugriffs auf vertrauliche Daten ebenso hoch wie bei modernen, leitungsgebundenen Kommunikationsnetzen. Zugriffsschutzeinrichtungen, Sicherheitsdienste und Verschlüsselung sind deshalb bei sensibler Datenkommunikation Pflicht.

Datex-L

Über Datex-L erfolgt die leitungsvermittelte Datenübertragung im IDN (Integriertes Text- und Datennetz, u.a. Telex, Teletex, Datex-L, Datex-P). Die beiden kommunizierenden Anschlüsse müssen dabei mit der gleichen Übertragungsgeschwindigkeit arbeiten.

Frame Relay

Dies ist ein Verfahren, das die Vorteile von Leitungsvermittlung und Paketvermittlung von Texten und Daten miteinander kombiniert. Es handelt sich dabei

um ein auf dem HDLC-Standard (High Level Data Link Control) basierendes Übertragungsprotokoll für den Zugang/Zugriff zu Netzwerken. Dabei können über eine physikalische Schnittstelle mehrere logische Verbindungen zu verschiedenen Zielen aufgebaut werden.

Intelligente Netze

Zur gemeinsamen Nutzung von Computern und Kommunikationseinrichtungen ist geplant, international standardisierte Telefonnetze zu schaffen, über die mit nur einer Nummer sämtliche Leistungsmerkmale moderner Computer- und Telefonkommunikation genutzt werden können.

ISDN (Integrated Services Digital Network)

Hinter diesem Begriff verbirgt sich die digitale Übertragung von Sprache, Daten und Bildern über dieselbe Leitung. Mit ISDN verbinden sich auch sämtliche Merkmale moderner Telekommunikation und TK-Anlagen. Fast die gesamten Neuentwicklungen bei öffentlichen Netzen basieren letztlich auf den technischen Entwicklungen des ISDN und der damit verbundenen Digitalisierung. Aufgrund des hohen Bekanntheitsgrades wird auf eine nähere (technische) Betrachtung von ISDN verzichtet. Informationen zum ISDN können bei der Telekom jederzeit erlangt werden.

Online-Dienste

Mit schnellen Modems oder über ISDN ist der Zugang zu den sog. Online-Diensten sehr leicht möglich. Mit diesen Diensten steht praktisch weltweit eine Fülle von Informationen und Dienstleistungsangeboten für die Nutzer bereit. Bei den derzeit zur Verfügung stehenden Einrichtungen handelt es sich um "America Online", "Compuserve", "Europe Online", "Internet", "Microsoft Online" und das bereits erwähnte "T-Online" der Telekom. Alle Online-Dienste haben unter Sicherheitsgesichtspunkten jedoch eines gemeinsam: Die Daten sind weder vor dem Verlust oder der Manipulation noch vor dem Zugriff durch Unbefugte hinlänglich geschützt. Die Gefahr, sich bei Nutzung dieser Dienste zusätzlich auch Computerviren einzufangen, ist relativ groß. Mit neuen internationalen Vor-

schriften und den derzeit in der Neufassung befindlichen Telekommunikations- und Kundendatenschutzverordnungen sowie dem Telekommunikationsgesetz (TKG) wird der Versuch unternommen, die allgemein anerkannten Regeln des Datenschutzrechts und der Datensicherheit auch in Netzen und Diensten zu realisieren. Damit wird zumindest eine breite Grundschutzbasis geschaffen. Sicherheit bei vertraulichen Daten und Dokumenten kann allerdings nur durch die bereits dargestellten Sicherungsmaßnahmen an lokalen Endgeräten, für die Kommunikationseinrichtungen und durch Verschlüsselung auf den Übertragungswegen erreicht werden.

Die Sicherheit in öffentlichen Netzen ist vor allem durch Abhörangriffe, Manipulationen von Daten und Systemen, Wiederholen (replay), Verzögern oder Verändern von Informationen, Vortäuschen falscher Kommunikationsverbindungen oder Partner sowie durch physische Angriffe auf die Verbindungen und Kommunikationseinrichtungen selbst (Beispielsfälle: "Keine Verbindung e.V."/ "K.A.B.E.L.S.C.H.N.I.T.T." in Ziffer 2.3.2) erheblich gefährdet. Neben standardisierten Netzsicherheitskonzepten auch in öffentlichen Netzen, die zumindest einen Grundschutz für alle Teilnehmer gewährleisten, müssen die eigenen Kommunikationseinrichtungen für den Anschluß an Netze gegen Sabotage und Spionage - wie in den vorangegangenen Kapiteln dargestellt - gesichert werden. Die Informationen selbst können nach dem Stand der Technik nur durch Verschlüsselung vor unbefugtem Mitlesen geschützt werden.

Die standardisierte Telekommunikation ist nach dem OSI- (Open System Interconnection) 7-Schichten-Modell der ISO (International Standardisation Organisation) festgelegt. Damit wurde die Grundlage geschaffen, Netze und Dienste im Sinne einer offenen, universell einsetzbaren und logischen Struktur miteinander zu verknüpfen, d.h. heterogene Rechnersysteme und Netze können nach festgelegten Normen miteinander kommunizieren. Die Anwender in diesen Netzen und Systemen erhalten ihre Daten genau in der Form, wie sie es in ihrem System gewohnt sind. Dieser OSI-Standard entspricht nahezu wortgleich der X.200-Empfehlung des CCITT.

4.3 Kabelinfrastruktur, aktive Komponenten, Verlegesysteme

Neben dem bereits dargestellten EMV-Schutzkonzept (Überspannungsschutz) und der Absicherung des Stromversorgungsnetzes durch USV/NEA muß auch die Datenverkabelung in gesicherter Ausführung erfolgen. Die Kabel selbst und die Netzknoten (aktive Komponenten, auch HUB) müssen gegen Abhören, Sabotage, kompromittierende Abstrahlung und unbefugten Zugriff geschützt werden.

Einen Grundschutz bieten Kabelinfrastrukturplanungen, die auf der Basis der europäischen Norm "Leistungsanforderungen an strukturierte Verkabelungsschemata" (EN 50 173) ausgeführt werden. Diese teilt die Datenverkabelung nach dem Prinzip der Baumstruktur zunächst in drei Bereiche auf. Die Primärverkabelung verbindet den Standortverteiler (SV) mit dem Gebäudeverteiler (GV) oder die GV untereinander. Die Sekundärverkabelung umfaßt den Bereich GV zum Etagenverteiler (EV). Als Abschluß regelt die Tertiärverkabelung die Verbindung zwischen EV und den Anschlußdosen der Endgeräte. Die Verbindung von der Anschlußdose bis zum Endgerät ist anwendungs- und hardwareabhängig und deshalb vom Regelungsumfang der Norm nicht erfaßt. Welche Kabeltypen für welche Anwendungsfälle die Norm vorsieht, kann der folgenden Tabelle entnommen werden:

Baumstruktur	**Kabeltyp**	**Anwendungsbereich**
Primärbereich	LWL-Kabel	für fast alle Anwendungen
Sekundärbereich	Symmetrische oder LWL-Kabel	Sprache und langsame Daten oder Daten mittlerer und hoher Geschwindigkeit
Tertiärbereich	symmetrische oder LWL-Kabel	für fast alle Anwendungen oder nach Bedarf

Lichtwellenleiter bieten im Primär- und Sekundärbereich hohe Übertragungsraten bei großen Übertragungsentfernungen und einen guten Schutz gegen Abhörangriffe. Mit modernen (Licht-) Meßeinrichtungen können nach Erfahrung

des BSI jedoch bereits heute auch LWL-Kabel, ohne diese zu beschädigen, abgehört werden. Einen 100 %igen Schutz garantieren diese deshalb nicht. Symmetrische Kabel, die insbesondere im Tertiärbereich eingesetzt werden, sind verdrillte Kupferleitungen, die sternförmig EV und Anschlußdosen auf der Etage verbinden. Heutzutage werden hierzu Shielded Twisted Pair/STP-, S-STP- (doppelt abgeschirmte Kabel) oder Unshielded Twisted Pair/ UTP-Kabel eingesetzt. Die maximale Leitungslänge ist dabei auf 100 m begrenzt. Symmetrische Kabeltypen und Übertragungsverfahren haben aufgrund ihrer größeren Flexibilität und dem geringeren Leitungsverlegeaufwand in modernen LAN die bisher eingesetzten asymmetrischen Verfahren, z.B. Koaxialkabel (Yellow Cable, RG 58-Cheapernet, ThinEthernet-ThinWire, RG 62), weitestgehend verdrängt. Symmetrische Verkabelungskonzepte werden nach der Norm in 5 Leistungsbereiche aufgeteilt. Die Staffelung erfolgt entsprechend den Übertragungsanforderungen. Vier zusätzliche Klassen (A - D) spezifizieren die jeweilige Anwendung, z.B. Sprache, niederfrequente Anwendungen (A), Datenanwendungen von mittlerer (B) bis sehr hoher Übertragungs- (Bit-) Rate (D). Außerdem bieten diese Klassen Definitionen und Meßvorgaben, die die Nahnebensprechdämpfung (ACR-Werte) definieren. Diesen Werten kommt namentlich bei der Beurteilung der kompromittierenden Abstrahlung besondere Bedeutung zu. Die Zuordnung von Kabeln, Übertragungsverfahren, Standards und Verbindungen kann der Tabelle auf dieser Seite entnommen werden.

Mit einem nach der EN 50 173 strukturierten Verkabelungskonzept werden nicht nur die Anforderungen an moderne LAN (Einhaltung von Standards, EMV-Schutzbestimmungen, Überspannungsschutz, Potentialausgleich etc.) und die Anforderungen an multimediafähige Kommunikationseinrichtungen realisiert, sondern auch wesentliche Aspekte der Datensicherheit verwirklicht. Es empfiehlt sich, im Sekundärbereich generell LWL-Verkabelungen einzusetzen. FDDI als neuer Standard ermöglicht hierbei sehr hohe Datenübertragungsraten (100 MBit/s) bis maximal 2 km Entfernung. Auch im Tertiärbereich sollten aus Sicherheitsgründen LWL-Kabel eingesetzt werden. STP-Verkabelungskonzepte

unter Verwendung geschirmter Anschlußdosen (RJ 45) sind eine vergleichsweise sichere und (noch) billigere Alternative.

Methode	IEEE-Stand.	Verbindungen		Kabeltypen	
		Typ	Bezeichnung	Typ	Bezeichnung
CSMA / CD Ethernet	10Base5 802.3	---	Tap	Ethernet	Yellow-cable
		15-p D-sub	AUI port DB 15	AUI-Kabel	Drop-cable
	10Base2 802.3	BNC	---	RG58-U	ThinEthernet Cheapernet
	10Base-T 802.3 i	RJ-45	UTP port	UTP	Twisted Pair IBM Typ 3 Telefonkabel
		50-p D-sub	Telco		
		RJ-45 shielded	---	STP	
	10Base-FL "FOIRL"	ST SMA	ST fiber F-SMA	50/125 62,5/125 100/140	Glasfaser (LWL)
Token Ring	802.5	9-p D-sub	DB-9	1, 2, 6, oder 9 (STP)	IBM Kabeltyp 1
		IBM Data Connector	---		
		RJ-45 shielded	---		
		RJ 45	---	3 (UTP)	IBM Kabeltyp 3
FDDI	---	FSD	---	62,5/125	LWL

Generell sind bei der Verkabelung folgende Schutzmaßnahmen vorzusehen:

- Verkabelung nach EN 50 173 (Kategorie 5 / Klasse D) **- Empfehlung! -**

- Schutzmaßnahmen, wie sie im Teil LAN-Sicherheit beschrieben sind

- LWL-Kabel sollten so verlegt werden, daß keine (abhörbaren) Schlaufen entstehen und Zugriffe erkennbar werden (Verlegung in abgeschlossenen Verlegesystemen bzw. Steigschächten oder regelmäßige Kontrolle); keine Stecker, Abzweigungen oder andere Anschlüsse als die betriebsnotwendig Vorhandenen; Anfang und Ende des LWL in geschützten Sicherheitsbereichen; LWL-Verbindungen sollten dazu redundant, d.h. als sog. Back-Up-Verbindung ausgelegt werden

- Kabel im Tertiärbereich sind gegen unbefugte Zugriffe durch Verlegung in abschließbaren oder verplombbaren Kabelkanälen zu sichern; alternativ können sie unter Putz oder in nicht zugänglichen Bereichen verlegt werden

- Verlegesysteme (Kabelkanäle) sollten gesichert (abschließbar, verplombt) in nicht leicht zugänglichen Bereichen (z.B. in abgehängten Flurdecken) oder in leicht zu kontrollierenden Bereichen (Büros) eingesetzt werden

- Kabel sollten nur in geschirmter Ausführung eingesetzt werden; dabei ist durch Verlegesysteme oder gänzliche Trennung auf größtmögliche Abstände zwischen DV-, Stark- und Schwachstromkabeln zu achten

- Anschlußdosen sollten nur in geschirmter Ausführung verwendet werden

- Sämtliche Komponenten sind in Plänen zu erfassen und zu dokumentieren

- Aktive Netzkomponenten (Verteiler, Netz-Server) sind gegen unbefugten Zugriff zu schützen, z. B. durch Unterbringung in besonders gesicherten Räumen

- Die nach der Norm EN 50 173 vorgeschriebenen Messungen (mit speziell zugelassenen Meßgeräten) sind durchzuführen und zu dokumentieren

- In Netzen, auf denen Verschlußsachen übertragen werden, sind zusätzlich Messungen und Lauschabwehrmaßnahmen erforderlich. Die Prüfungen und Messungen, einschließlich der Verwendung geprüfter Kabeltypen und Verlegesysteme, sowie die Installationsvorgaben sollten bereits in der Planungsphase mit mit der beratenden Stelle abgestimmt werden

4.4 Datenfernübertragung (DFÜ)

Teilweise ergeben sich hier Überschneidungen mit den in den vorangegangenen Abschnitten dargestellten Maßnahmen und Möglichkeiten in Netzen. Im Teil "DFÜ" sollen deshalb nur Grundlagen sowie Geräte und Mittel beschrieben werden, die es ermöglichen, mit einem PC weltweite Kommunikationsbeziehungen aufzunehmen. Über ISDN oder über ein an einen PC angeschlossenes Modem ist es möglich, über öffentliche Netze Zugang zu weltumspannenden Netzen und Diensten zu erlangen. Dazu wird das Modem an die serielle Schnittstelle des PC und über die TAE-Anschlußdose an eine vorhandene Telefonleitung angeschlossen. Danach wird ein auf dem PC installiertes Softwareprogramm (sog. Terminalprogramm, z.B. Telix, Terminate oder Telemate) ge-

startet. In dem Terminalprogramm müssen die entsprechenden Übertragungsparameter des Modem voreingestellt werden. Modems wandeln digitale Signale des Sende-PC in für die Telefonleitung geeignete analoge Signale um, beim Empfänger werden die ankommenden analogen Signale im Modem wieder digitalisiert; die Abkürzung Modem steht deshalb für Modulator/Demodulator. Damit kann dann der direkte Zugriff auf anwählbare Mailboxen in den Netzen und Diensten erfolgen.

Mailboxen sind computerunterstützte Mitteilungs- und Speichersysteme mit vielfältigen technischen Ausgestaltungs- und Variationsmöglichkeiten; sie werden oft auch als elektronische Briefkästen bezeichnet. Die aus filmischen Darstellungen bekanntere Möglichkeit des Einwählens in eine Mailbox kann auch mit einem sog. Akustikkoppler erfolgen. Der Koppler ist das physikalische Gegenstück zum Telefonhörer und wird mit der seriellen Schnittstelle des PC verbunden. Sobald der Anrufer auf dem Telefonapparat eine Mailbox anwählt und diese sich mit einem Pfeifton meldet, wird der Hörer auf den Koppler geklemmt und die Verbindung steht. Hohe Übertragungsgeschwindigkeiten, wie sie moderne Modems bieten, sind mit diesem Verfahren jedoch bei weitem nicht zu erreichen. Mailboxzugänge lassen sich auch über ISDN-Computer-Steckkarten oder ISDN-Adapter schaffen. Angewählte Mailboxen sind zumeist in zwei Bereiche (Verzeichnisse = "Area" oder "Bretter") aufgeteilt, in persönliche, nur für den Besitzer (User) zugängliche, sowie öffentliche, meist thematisch gegliederte, auf die alle User einer Box Lese- und/oder Schreibzugriff haben. Der Nachrichtenaustausch in Mailboxen kann deshalb sowohl innerhalb als auch außerhalb - in Mailboxnetzen - erfolgen. Die Verbindung von Mailboxnetzen zu anderen Netzen wird über sog. Brücken oder Gateways realisiert. Dies sind Kommunikationsrechner, die das Datenformat der Nachrichten an die Bedürfnisse der jeweils angeschlossenen Netze individuell anpassen.

1983 wurde von Tom Jennings aus San Francisco das erste Netzwerkprogramm für private Mailboxen programmiert. Dieses Programm trägt den Namen FIDO und bildet die Grundlage für das weltweite FIDO-Net. 1985 wurde die erste

deutsche Mailbox an das FIDO-Net angeschlossen. 1987 entwickelte sich das erste deutsche Mailboxnetz, das Zerberus- oder kurz Z-Netz. In diesen Netzen können nicht nur öffentliche Dokumente verschickt und eingestellt werden, sondern auch elektronische Briefe, sog. E-Mail, an spezielle Empfänger adressiert werden. Das derzeit größte Mailboxnetz der Welt ist Compuserve. In über 350 "Foren" (Informationsbereiche für z.B. Programmierer, Hardware- und Vertriebsspezialisten, Beratung durch alle großen EDV-Firmen etc.) und über 1700 angeschlossenen Datenbanken schlummern gigantische Informations- und Datenbestände. Neben Soft- und Hardwareforen gibt es schwerpunktmäßig noch solche für die Bereiche Finanzen, Wirtschaft, Nachrichten und Hobby. Diese können derzeit von ca. 1,5 Millionen Usern in über 100 Ländern der Welt abgerufen werden. Über Compuserve E-Mail sind auch alle Internet-Adressaten erreichbar. Nicht unerwähnt bleiben darf, daß die Nutzung solcher Einrichtungen Geld kostet. Die Gebühren werden über die Telefonrechnung erhoben. Jedes Netz und viele Dienste haben dabei ihre besonderen Grund- und Benutzungsgebühren.

Die anderen Online-Dienste, die sich zur Nachrichtenübermittlung eignen, wurden bereits in Ziffer 4.2.1 vorgestellt. Die dort gemachten Aussagen bezüglich des Abhör- und Manipulationsschutzes gelten hier gleichermaßen für diesen Bereich. Mailboxsysteme und -netze werden heute auch von kriminellen und extremistischen Organisationen und Gruppierungen genutzt. Entsprechende Meldungen über Mailboxen mit härtester (Kinder-) Pornographie und Gewalt bis hin zu Bildern von Leichen und Tätern beim Verstümmeln ihrer Opfer können fast täglich der Presse entnommen werden. Aus dem extremistischen Bereich seien hier die Mailboxen "Comlink", "Spinnennetz" und "Thule" genannt. Diese Mailboxnetze sind international verflochten und mit Zugangs- und Zugriffsschutzeinrichtungen sowie Verschlüsselungsmechanismen ausgestattet, die es Sicherheitsbehörden außerordentlich erschweren, Täter und Strukturen zu erkennen und zu bekämpfen. Die anhaltende öffentliche Diskussion über staatliche Auflagen und Beschränkungen für die Anbieter und Betreiber der Dienste spie-

gelt die vielfältige, auch verbrecherische Nutzung dieser Dienste wider.

4.5 Internet / Firewallsysteme

Das Internet ist mit geschätzten 1,2 Millionen angeschlossenen Rechnern weltweit das größte Dateninformations- und Kommunikationsnetz. Die Palette der angeschlossenen Nutzer reicht vom privaten PC-Anwender bis zu Firmen, Universitäten und Forschungseinrichtungen mit Großrechnern. Neben E-Mail-Service-Diensten besteht ein breites Angebot an sog. Newsgroupes, die zusammen das "Usenet" bilden. In öffentlichen Foren wird in mehreren tausend Gruppen über jeden nur denkbaren Sachverhalt diskutiert. Unter Berücksichtigung bestimmter Verhaltensregeln kann sich jeder an solchen Diskussionskreisen beteiligen. Neben Mail und News bietet das Internet über erweiterte Zusatzdienste (Telnet), in denen man sich der Internetstrukturen bedient, die Möglichkeit, sich via Standleitung in die entferntesten Rechner und Datenbanken einzuloggen. Mit FTP (File Transfer Protocol) ist es möglich, Dateien von einem auf den anderen im Internet angeschlossenen Rechner zu kopieren. Mit "Archie" können Standorte von Programmen und Dateien ermittelt werden. "Gopher" erlaubt die standortunabhängige Suche nach Daten, Dateien und Programmen. Dabei klickt sich der Anwender durch immer mehr verästelte Menüs, bis er die gewünschten Daten gefunden hat. Mit "WAIS" läßt man den Rechner nach Eingabe von Stichwörtern selbst suchen, gefundene Daten werden bei Übereinstimmung mit den Stichwörtern angezeigt und können vom Anwender ausgewählt werden. Das "World-Wide-Web" (WWW) ist der am einfachsten zu bedienende Dienst des Internet. Damit können, durch graphische Benutzeroberflächen unterstützt, Dokumente durch Auswahl von markierten Querverweisen immer weiter aufgeblättert werden.

Die Nutzung des Internet ist jedoch mit einer Reihe von Gefahren für die Datensicherheit und den Datenschutz verbunden. Im wesentlichen besteht die Möglichkeit, daß alle in diesem Netz übertragenen Daten mitgelesen, verändert, wiedereingespielt, mißbräuchlich verwendet oder zerstört werden. Davon

betroffen können auch Benutzernamen und Paßworte sein, die in den Internet-Diensten oftmals offen übertragen werden. Die so gewonnenen Informationen können in Listen zusammengefaßt werden und Hackern und Datenspionen eine nützliche Basis für ihre Angriffe bilden. Die wesentlichsten Schutzmaßnahmen bei der Internetnutzung werden im folgenden noch einmal zusammengefaßt:

- Verschlüsselung
- Einsatz von Zugriffskontrollverfahren
- umfassende Aufklärung und Sensibilisierung der Anwender
- Erstellung von Schutzkonzepten und Benutzerrichtlinien
- personelle und organisatorische Regelungen für den Internet-Zugang sowie solche wer, wann, zu welchen Diensten überhaupt zugriffsberechtigt ist
- Absicherung der zugelassenen Dienste durch Firewallsysteme
- Notfall- und Maßnahmenpläne für erkannte Hackerangriffe

Auf Firewallsysteme soll abschließend noch näher eingegangen werden. Diese bilden sozusagen eine Mauer zwischen lokalem (privatem) und öffentlichem (unsicherem) Netz mit kontrollierten Zu- und Ausgängen für die Internet-User. Jeder Benutzer wird dabei zunächst auf seine Berechtigung überprüft; bei unbefugten Zugriffsversuchen wird der Angriff nicht erst im eigenen Rechner, sondern bereits vorher durch den Firewallrechner abgeblockt. Firewallsysteme, wie sie in der BSI-Informationsschrift "Sicherheitsanforderungen an Internet - Firewalls" beschrieben werden, bestehen aus Software-, Hardware- und Verschlüsselungskomponenten. Das Screened Subnet (Kryptoboxen mit Packetfilterfunktion, Workstation mit zwei Netzwerkanschlüssen und Firewallfunktionalität = Bastion, ein oder mehrere Informationsserver) bildet ein in sich geschlossenes Teilnetz, das zwischen den zu schützenden Rechner/das abzusichernde Netz und das öffentliche Netz geschaltet wird. Nur die Rechner des Screened Subnet sind von außen bekannt und erreichbar (adressierbar); dort wird dann der weitere Zugang geprüft und ggf. ermöglicht. Mit Hilfe eines Security-Manage-ment-Systems werden die Kommunikationsbeziehungen fest-

geschrieben und die Bastion, z.B. mit Schlüsseln für die Verschlüsselung, versorgt. Zusätzliche Netzwerkmanagementeinrichtungen steuern die Kommunikation und die Protokollierung. Auf den Informationsservern werden die Daten abgelegt, die öffentlich zugänglich gemacht werden sollen. Sie stehen (logisch) außerhalb des zu schützenden Netzes. Der gesamte Firewall wird räumlich in einer gesicherten Umgebung (Sicherheitsbereich) betrieben, um ihn vor Sabotage-, Manipulations- oder Spionageangriffen zu schützen. Da Firewalls jedoch individuell auf die Schutzbedürfnisse des jeweiligen Nutzers und des dort eingesetzten LAN abgestimmt werden sollten, empfiehlt sich eine entsprechende Beratung durch Fachleute. Im staatlichen Bereich stehen hierfür neben dem BSI die Landesbehörden für Verfassungsschutz zur Verfügung.

5. Verschlüsselung (Kryptologie)

5.1 Grundlagen

Unter dem Fachbegriff der Kryptologie wird meist das Verschlüsseln (Chiffrieren) von Texten verstanden, um sie vor anderen geheimzuhalten. Mit modernen kryptologischen Verfahren, die sowohl mit Hilfe von Computersystemen entwickelt und ausgeführt als auch zu ihrem Schutz eingesetzt werden, lassen sich Daten nicht nur wirkungsvoll gegen unbefugte Nutzung schützen. Vielmehr ist es auch möglich andere bei der Datenübertragung wichtige Aspekte wie z.B. Echtheitsprüfung (Authentifikation), Datenintegritätsprüfung, elektronische Unterschrift und natürlich Vertraulichkeit (Schutz vor Spionage) zu realisieren.

Bereits in der Antike waren Schlüsselverfahren und Chiffriergeräte bekannt; sie wurden zu militärischen Zwecken eingesetzt. Die "Skytala" der Spartaner war ein zylindrischer Stab, der spiralförmig mit Lederband umwickelt und dann in Längsrichtung des Stabes mit der Nachricht beschrieben wurde. Das abgewikkelte Band konnte vom Empfänger nur dann gelesen werden, wenn er im Besitz eines Stabes derselben Größe war. Damit sind die Grundprinzipien der Kryptologie bereits erläutert: Die Sicherheit des Kryptosystems darf nicht von der Kenntnis des Algorithmus (Verfahren zur Verschlüsselung) abhängen, sondern beruht einzig und allein auf der Geheimhaltung des Schlüssels. Die von Cäsar in seinem Kriegstagebuch "de bello gallico" geschilderte Methode der Verschlüsselung, das Alphabet einfach um 3 Stellen zu verschieben, d.h. er ersetzte A durch d, B durch e, C durch f usw., ist eine der Grundlegenden der Kryptologie und wird (monoalphabetische) Substitution genannt. Das Wort KRYPTO wird nach diesem Verfahren zum Chiffrat nubswr. Die Darstellung hier erfolgt nach dem Prinzip, den Klartext in Groß- und das Zielalphabet (Chiffrat) in Kleinbuchstaben zu schreiben. So einfach diese Methode, so einfach ist auch die Entschlüsselung (Dekryptierung). Die Häufigkeit, mit der bestimmte Buchstaben oder Buchstabengruppen in Texten vorkommen, spiegelt sich im

chiffrierten Text wider. In der deutschen Sprache ist beispielslweise jeder fünfte Buchstabe ein E, jeder neunte ein N und nur jeder hundertste ein P. Außerdem ist die Häufigkeit bestimmter Buchstabengruppen, z.B. UND / xqg (nach Cäsar), sehr verräterisch. Daraus abgeleitet ergeben sich zwei weitere Prinzipien der Kryptologie: Keine Verschlüsselung ist 100 %ig sicher. Der Aufwand (Kosten) zum Brechen des Algorithmus muß größer als der Wert der Information und der Zeitaufwand muß länger sein, als die Information interessant ist.

Durch den Italiener Leon Battista Alberti wurde im 16. Jahrhundert die Cäsarsche Methode dahingehend verfeinert, daß er über ein vorher vereinbartes Schlüsselwort nicht nur ein, sondern mehrere Zielalphabete einsetzte. Das Schlüsselwort regelt dabei die Reihenfolge der Wechsel. Bei der Verschlüsselung des vorherigen Begriffs KRYPTO mit dem Schlüsselwort CODE bedeutet dies, daß durch C als drittem Buchstaben des Alphabets (O=15. / D=4. / E=5.) K um 3 Stellen verschoben und deshalb zum n wird. Durch O wird R um 15 Stellen verschoben und deshalb zum g usw. und zwar solange, bis das Schlüsselwort verbraucht ist. Dann beginnt der Kreislauf (beim T von KRYPTO) von neuem, bis schließlich das Chiffrat ngcuwd entsteht. Diese Methode wird als polyalphabetische Substitution bezeichnet. Mathematisch läßt sich jedoch auch hier in den so chiffrierten Texten eine Regelmäßigkeit erkennen, die der Länge des vereinbarten Schlüsselwortes oder einem Vielfachen hiervon entspricht. Läßt der verschlüsselte Text die Länge des Schlüsselworts erkennen, ist dessen Ermittlung durch die oben erwähnte Häufigkeitsverteilung der Buchstaben dann kaum mehr ein Problem. Zwei Maßnahmen können die dargestellte Kryptoanalyse erheblich erschweren: zum einen die Auswahl sehr langer Schlüssel (-worte) und zum anderen der zusätzliche Einsatz von verwürfelten (permutierten) Zielalphabeten. Bei der zweiten Form der Chiffrierung werden die Zeichen des Klartextes nicht durch andere (nach einer vorher festgelegten Systematik = Substitution) ersetzt, sondern in sich vertauscht. Dieses Verfahren nennt man Transposition. Je häufiger dieser Schritt ausgeführt wird, desto sicherer ist die Verschlüsselung. Fast alle modernen symmetrischen (ein Schlüssel für die Ver- und Entschlüsselung) Verfahren basieren auf den Prinzipien der

Substitution und der Transposition. Dabei wird zunächst der Klartext in gleich lange Blöcke zerlegt, die dann nacheinander (blockweise) verschlüsselt werden. Dann spricht man von Blockchiffreverfahren. Die bekanntesten, der DES- und der RSA-Algorithmus, sollen kurz vorgestellt werden:

Der 1977 von IBM vorgestellte Data Enkryption Standard (DES) war der erste Verschlüsselungsstandard (FIPS PUB 46), der vom US-amerikanischen National Bureau of Standards normiert und veröffentlicht wurde. 1994 erfolgte die Freigabe dieses DES durch das NIST (National Institute of Standards and Technologie) für einen Einsatz in sicheren Systemen für weitere 5 Jahre. Da der DES mit nur einem Schlüssel für die Ver- und Entschlüsselung arbeitet, gehört er zur Gruppe der symmetrischen Verfahren. Diese Verfahren werden oft als "private key-Verfahren" bezeichnet. Dieses Charakteristikum des DES zeigt auch die größte Schwachstelle von symmetrischen Verfahren: Die Sicherheit der Verschlüsselung ist im wesentlichen abhängig von der Geheimhaltung des Schlüssels, den Sender und Empfänger einer Nachricht gleichermaßen zur Ver- und Entschlüsselung benötigen. Die Beteiligten an einer solchen Kommunikation müssen deshalb Vereinbarungen über den gesonderten, sicheren Austausch der Schlüssel treffen (z.B. Kurierdienst). Außerdem werden bei solchen Verfahren in einem Verbund sehr viele Schlüssel gebraucht, z.B. bei 10 Teilnehmern schon 45, bei 100 bereits 4950. Die Schlüsselerstellung und -mittelverteilung sind demzufolge sehr aufwendig, insbesondere, wenn zur Erhöhung der Sicherheit regelmäßige Schlüsselwechsel vereinbart werden. Technisch gesehen arbeitet der DES so, daß der Klartext in konstante 64-Bit-Blöcke zerlegt und in einer sog. Eingangspermutation durch einen 56-Bit-Schlüssel verwürfelt wird. Jeder dieser Blöcke durchläuft mehrfach dieselben Kryptierfunktionen. Da zur Ver- als auch zur Entschlüsselung eines solchen Datenblocks die gleichen Funktionen eingesetzt werden, genügt es bei der Dekryptierung, die Reihenfolge der funktionen einfach umzukehren. Die Datenblöcke werden dabei in zwei gleich große Teilblöcke (32-Bit) aufgeteilt (sog. Feistel-Chiffre). Dann folgen pro Block 16 einzelne Verschlüsselungsschritte (Iterationen). Bei jedem dieser Schritte wird ein eigener, aus dem 56-Bit-

Schlüssel permutierter Teilschlüssel (48-Bit groß) verwendet. Schließlich wird nach einer sog. 32-Bit-Expansion jeder Datenblock einer zur Eingangspermutation inversen Ausgangspermutation unterzogen, bis der gesammte Chiffretext entsteht. Diese Verfahren ist sehr sicher, benötigt in seinen Teilschritten jedoch viel Zeit. Der 1987 vom japanischen TK-Konzern NTT vorgestellte Fast Enkryption Algorithm (FEAL) arbeitet ähnlich wie DES, verwendet dabei aber nur 8 Iterationen. Er ist deshalb zwar schneller, aber nicht so sicher wie der DES.

Eine sichere und schnelle Kombination aus beiden Verfahren stellt der 1990 entwickelte International Data Enkryption Algorithm (IDEA) dar. Wie DES verschlüsselt IDEA blockweise, jedoch mit einem weitaus größeren Schlüssel (128-Bit). Zudem arbeitet er schneller, weil er nur die Hälfte der Iterationen und keine Permutationen durchführt. Dieses Verfahren gilt derzeit als aussichtsreichster Nachfolger für DES.

Das erhebliche Schlüsselmanagement der beiden symmetrischen Verfahren reduziert sich bei asymmetrischen erheblich. Der bekannteste Vertreter ist der nach seinen Entwicklern (Rivest, Shamir, Adleman) benannte RSA-Algorithmus. Zur Ver- und Entschlüsselung werden dabei zwei verschiedene, zueinander passende Schlüssel eingesetzt, die durch ein spezielles Generierungsprogramm erzeugt werden. Da einer von ihnen veröffentlicht und der andere geheim bleibt, nennt man diese Verfahrensweise auch "public key". Der Vorteil dieser Regelung besteht eigentlich darin, daß durch den öffentlichen keine Rückschlüsse auf den geheimen Schlüssel möglich sind und die Schlüsselverteilung sehr einfach vonstatten geht.

Nachteilig ist, daß diese Verfahren in der Kryptierung selbst sehr langsam arbeiten. Beim RSA werden die Schlüsselpaare durch die Faktorisierung großer natürlicher Zahlen (Primzahlen) erzeugt. Das mathematische Prinzip, das hinter dieser Schlüsselerzeugung steckt, ist einfach und einleuchtend. Es ist sehr leicht, auch sehr große Primzahlen miteinander zu multiplizieren, jedoch mathematisch (auch computerunterstützt) praktisch nicht möglich, die so gewon-

nene Zahl wieder in ihre Ursprungsfaktoren zu zerlegen. RSA-Schlüssel haben eine Mindestlänge von 512-Bit. In Sicherheitssystemen werden heute bereits 1028- Bit- und größere Schlüssel implementiert. Beim Verschlüsseln wählt der Sender den öffentlichen Schlüssel des Empfängers aus einer Schlüsseltabelle und verschlüsselt mit diesem seine Nachricht. Nur deren Empfänger kann diese mit seinem zum öffentlichen Schlüssel passenden geheimen Schlüssel wieder entschlüsseln. Der weitere Vorteil dieses Verfahrens liegt darin, mit der Umkehrung des Schlüsselprinzips die Authentisierung von Dokumenten sicherzustellen. Der Absender einer Nachricht verschlüsselt diese, die elektronische Unterschrift oder ein bestimmtes Merkmal mit seinem geheimen Schlüssel. Der Empfänger der Nachricht sucht nun aus der Schlüsseltabelle den öffentlichen Schlüssel des Senders heraus und wendet diesen auf die Nachricht an. Jeder andere öffentliche Schlüssel würde dabei wiederum nur ein Chiffrat erzeugen. Liegt dagegen die Nachricht oder Unterschrift im Klartext vor, ist bewiesen, daß sie nur vom angegebenen Sender stammen kann.

Der Schlüsselaustausch und die Generierung von RSA-Schlüsseln kann in sog. Trust-Centern erfolgen. Dieses ist dabei die von den Kommunikationspartnern beiderseits anerkannte vertrauenswürdige Instanz. Die geheimen Schlüssel der einzelnen Teilnehmer und alle öffentlichen Schlüssel des Kommunikationsverbundes werden z.B. auf Chipkarten verschlüsselt abgespeichert und den Teilnehmern einzeln zur Verfügung gestellt (die Chipkarte enthält dann den eigenen geheimen und alle öffentlichen Schlüssel). Die öffentlichen Schlüssel können auch in einem Rechnersystem (Datenbank = Schlüsseltabelle) eingestellt und abgefragt werden. Damit sichergestellt ist, daß sich hinter dem öffentlichen Schlüssel eines Teilnehmers auch noch der vom Sender gewünschte Empfänger verbirgt, werden bei einer Schlüsselanforderung an das Trust-Center die öffentlichen Schlüssel beider Teilnehmer auf einem sicheren Übertragungsweg an das Trust-Center übergeben, von diesem geprüft, zertifiziert (mit Gültigkeitsdauer) und zurückgegeben. Der Sender verschlüsselt dann seine Nachricht mit dem öffentlichen (zertifizierten) Schlüssel des Empfängers und fügt der Nachricht die Zertifizierung seines Schlüssels bei.

Um die Vorteile von DES und RSA gleichermaßen nutzen zu können, werden heute häufig sog. Hybridsysteme eingesetzt. Zur Verschlüsselung wird DES (Sicherheit), zum Schlüsselmanagement (Schlüsselgenerierung, -verteilung) RSA eingesetzt. Das im Zusammenhang mit der US-amerikanischen Clipper-Chip- Initiative (staatlich kontrollierter Einsatz von hochwertigen Kryptochips- bzw. Verfahren, auf die ggf. auch Sicherheitsbehörden einen Zugriff haben; Verbot aller anderen öffentlichen und privaten Kryptosysteme) in der Presse zitierte PGP (Pretty Good Privacy) von Phil Zimmermann ist hierfür ein gutes Beispiel. Die Datenverschlüsselung erfolgt mittels IDEA, das Schlüsselmanagement mit RSA.

Neben den symmetrischen und asymmetrischen Verfahren existieren noch sog. Einwegverfahren. Sie werden insbesondere bei der Paßwortprüfung in Rechnern eingesetzt. Dabei werden die Paßworte zunächst verschlüsselt und dann so abgespeichert. Eine Entschlüsselung ist dabei nicht möglich. Eingegebene (login), vom Nutzer festgelegte Paßworte werden nach dem Verfahren zunächst wieder verschlüsselt; das so entstandene Chiffrat wird mit dem auf dem Rechner abgelegten Paßwortchiffrat verglichen. Besteht Übereinstimmung der Chiffrate, erfolgt die Freigabe des Systems.

5.2 Hardwareverschlüsselung

Darunter versteht man die interne Verschlüsselung von Daten und Dateien auf den IT-Systemen und bei der Datenfernübertragung (DFÜ) durch spezielle Geräte oder Gerätekomponenten. Dafür sind folgende Lösungen vorgesehen, die miteinander kombiniert werden können:

Die Daten und Dateien werden lokal (auf Fest-, Wechselplatten, Disketten) kryptiert und kryptologisch mit einer Nutzerauthentisierung versehen sowie bei der lokalen Übertragung in einem LAN verschlüsselt übermittelt.

Bei der DFÜ- und ergänzenden Dateikryptierung mit Nutzerauthentisierung von TK-Anlage zu TK-Anlage (sog. Portverschlüsselung) oder von Gerät zu Gerät

(sog. End-to-End-Verschlüsselung) wird die Übertragung verschlüsselt abgewickelt. Lokal kryptierte Daten und Dateien werden bei der Übertragung einfach noch einmal überschlüsselt, was die Sicherheit zusätzlich erhöht. Da Daten und Dateien nur in verschlüsselter Form abgespeichert sind, können zusätzliche materielle Maßnahmen bei entsprechender Umgebungssicherheit entfallen. Netzübergänge (Gateways), z.B. von ISDN auf Mobil- oder Bündelfunk, werden so entwickelt, daß eine durchgängige kryptierte Kommunikation ermöglicht wird. Bei der Anbindung offener an schutzbedürftige Netze erfolgt die Überwachung der entsprechenden Schnittstellen durch Kryptosysteme (z.B. Firewall). TK-Anlagen mit integrierten offenen Verbindungen zu Sprachkryptogeräten werden auf Mißbrauch kontrolliert. Kryptosysteme dürfen dabei die Leistungsfähigkeit der zu sichernden Systeme nicht oder nur unwesentlich beeinträchtigen. Das Kryptodatenmanagement muß dabei sicher ausgestaltet, die Kryptosysteme selbst müssen gegen unbefugten Zugriff (Manipulationsschutz, Abhörschutz) gesichert werden, d.h. der Betrieb von Kryptogeräten darf nur in gesicherter Umgebung (Sicherheitsbereich) erfolgen.

Mittlerweile wurden durch das BSI die verschiedensten Hardwarekryptosysteme nach den ITS/ITSEC geprüft und zugelassen. Sie sind im wesentlichen für die Sprach- und Faxkryptierung in analogen und digitalen Netzen (z.B. analoges Telefonnetz, ISDN, Mobilfunk, BOS-Funk/Behörden und Organisationen mit Sicherheitsaufgaben, Satellitenfunk etc.) sowohl für die End-to-End- als auch für die Portverschlüsselung konzipiert. Für die lokale Daten- und Dateikryptierung stehen PC-Kryptokomponenten (PC-Steckkarten) mit Benutzeridentifizierung und Authentifizierung (Chipkarten/-leser) zur Verfügung. Dies gilt ebenfalls für mobile (Laptop/Notebook) PC. Einzelheiten zu den entsprechenden Geräten und deren Einsatzbereichen können beim BSI erfragt werden. Im staatlichen Bereich müssen bei der Übermittlung von Verschlußsachen bestimmte Vorgaben zwingend eingehalten werden. Für die Datenfernübertragung im ISDN wird das Kryptogerät ELCRODAT 6.2/ED 6.2 empfohlen. Da es sich hierbei um ein multifunktionales, sehr zukunftsträchtiges Gerät handelt, soll es hier näher vorgestellt werden:

Das ED 6.2 ist ein Bus-/Port-Kryptogerät, das auf der Basis von ISDN eingesetzt werden soll. Ausgehend von den zwei Schittstellen, die das ISDN bietet (S_0 -Schnittstelle: zwei 64-KBit B-Nutzkanäle / ein 16-KBit D-Steuerungskanal oder S_{2M} -Schnittstelle: dreißig 64-KBit B-Nutzkanäle / ein 64-KBit D-Steuerungskanal), wird das Gerät in den zwei schnittstellenabhängigen Varianten entwickelt. Einsatzbereich ist die Verknüpfung von mittleren und großen TK-Anlagen (Sprache, Fax) sowie für die Daten- und Bildübertragung nach internationalen Standards. Die bereits vorgestellte lokale Daten- und Dateikryptierung ergänzt das ED 6.2-Konzept. Kryptoverfahren und Kryptodatenmanagement basieren auf BSI-Vorgaben bzw. -Entwicklungen und eignen sich auch für die Sicherung besonders schutzwürdiger Informationen im Sinne des staatlichen Geheimschutzes.

Das hier skizzierte Gerät soll an 1998 alle bisherigen Kryptogeräte mit speziellem Einsatzzweck (nur Sprache, nur Fernschreibbetrieb, nur Daten) ablösen und auf hohem Niveau die Kryptierung sämtlicher Informationen ermöglichen. Die Ausgestaltung des Kryptokonzepts wird derzeit zwischen Bund und Ländern diskutiert. Das ED 6.2 ist ein Gerät der Schutzklasse 3. Im BSI-Konzept für die Zulassung und den Einsatz von Kryptosystemen im staatlichen Geheimschutz stellt sich die Schutzklasseneinteilung nach Schutzziel und Risiko wie folgt dar:

Schutzklasse	Schutzziel	zugelassen für folgende VS-Informationen und Einsatzbedingungen
1 (Standard)	Die unbefugte Kenntnisnahme von/der unbefugte Zugang zu den Informationen mit einfachen Mitteln soll verhindert werden. Ein erfolgreicher Angriff in Einzelfällen wird in Kauf genommen.	⊇ VS-NfD ⊇ lokale Verarbeitung/Übertragung von VS-VERTRAULICH unter besonderen Bedingungen [1]
2 (Hochsicherheit)	Die unbefugte Kenntnisnahme von/der unbefugte Zugang zu den Informationen bei einem qualifizierten Angriff soll verhindert werden. Ein Angriff auf Systemkomponenten, in denen Klartext vorhanden oder das Kryptoverfahren implementiert ist, muß erkennbar sein. Ein geringes verbleibendes Restrisiko wird in Kauf genommen.	⊇ VS-VERTRAULICH ⊇ lokale Verarbeitung von GEHEIM unter besonderen Bedingungen [2]
3 (Höchstsicherheit)	Die unbefugte Kenntnisnahme von/der unbefugte Zugang zu den Informationen sowie ein Angriff auf Systemkomponenten, in denen Klartext vorhanden oder das Kryptoverfahren implementiert ist, muß verhindert werden.	⊇ GEHEIM ⊇ STRENG GEHEIM

[1] Durch zusätzliche materielle, personelle und organisatorische Maßnahmen muß sichergestellt sein, daß für VS-VERTRAULICH verwendete Sicherheitsparameter und das VS-VERTRAULICH-Information enthaltende Chiffrat gegen einen qualifizierten Angriff geschützt sind.

[2] Durch zusätzliche materielle, personelle und organisatorische Maßnahmen muß sichergestellt sein, daß für GEHEIM verwendete Sicherheitsparameter und das GEHEIM-Information enthaltende Chiffrat gegen jeden Angriff geschützt sind.

Für die Bereiche außerhalb des staatlichen Geheimschutzes wurde ein Kryptokonzept (Empfehlung für die Entwicklung und Produktion von Kryptosystemen und deren Einsatz in der Bundesverwaltung außerhalb des staatlichen Geheimschutzes; Entwurfsfassung) entwickelt. Die Darstellung der o.a. Schutzklassen erfolgt dort etwas abgestufter, da die Schutzzieldefinitionen nicht ganz so hoch

sind wie im VS-Kryptokonzept. Bis zu einer endgültigen Fassung soll jedoch noch nicht näher auf diesen Bereich eingegangen werden.

5.3 Softwareverschlüsselung

Bei dem in Ziffer 5.1 bereits vorgestellten PGP handelt es sich um ein Softwareverschlüsselungsverfahren, d.h. kryptographische Funktionen werden durch Softwareeinspielung in die im IT-System vorhandenen Prozessoren realisiert. Dadurch entstehen zwei wesentliche Schwachstellen, die es generell nicht erlauben, Softwareverschlüsselung zum Schutz sensibler Informationen einzusetzen. Zum einen wird die Leistungsfähigkeit des IT-Systems (wesentlich) beeinträchtigt, zum anderen ist das Risiko der Manipulation der Verschlüsselungsroutinen um ein vielfaches höher als bei Hardwarelösungen. Typischerweise sind Softwareverschlüsselungen Anwendungen (Dateiverschlüsselung), die vom Anwender selbst aktiviert werden müssen. Auf die Probleme, die sich hieraus ergeben (Nachlässigkeit, Irrtum, Bequemlichkeit, menschliches Fehlverhalten etc.) muß nicht besonders eingegangen werden. Es ist ja gerade Sinn und Zweck der Kryptierung, vom Nutzer möglichst unbemerkt - ohne Performance- und Leistungsverlust - automatisch alle Daten und Dateien zu verschlüsseln. Solches läßt sich mit Softwarelösungen (automatisiert) fast nicht realisieren. Außerdem können die reinen Kryptokomponenten (Funktionsabläufe, Schlüssel, Verfahren, Schlüsselmanagement) nur dann als sicher und vertrauenswürdig gelten, wenn sie zuverlässig gegen Manipulationen geschützt sind. Dies alles trifft auf Softwareverschlüsselung jedoch nicht zu. Wer sich darüber hinaus solche Software (z.B. PGP) über das Internet herunterlädt, kann noch nicht einmal beurteilen, ob das Programm auch in seinem ursprünglichen Leistungsumfang vorliegt, oder ob es bereits manipuliert oder verfälscht wurde und die Daten ggf. unbemerkt im Klartext "abzweigt ". Bei undokumentierten Programmen ist ohnehin besondere Vorsicht angezeigt.

6. Anhang 1

6.1 Datensicherung (Datenträgerhandling / Wiederanlaufplanung)

Bereits in verschiedenen Passagen der Ausarbeitung wurde die Datensicherung als eine der geeigneten Maßnahmen zum Schutz von Datenbeständen beschrieben. Insbesondere wenn Daten durch Angriffe verlorengehen oder durch Manipulationen zerstört, verändert oder verfälscht werden, zeigt sich die Notwendigkeit einer funktionierenden Datensicherung; dieses Verfahren wird auch als Back-Up bezeichnet. Datenverluste sind nicht allein durch aktive Angriffe zu befürchten, sondern resultieren auch aus Nachlässigkeit, Irrtum, Soft- und Hardwaredefekten oder werden durch höhere Gewalt (Feuer, Wasser, Erdbeben etc.) verursacht. In Anbetracht der heute üblichen, umfangreichen Datenbestände und der teilweise existentiellen Abhängigkeit von Verfügbarkeit und Integrität der Informationen ist es verwunderlich, wie "blauäugig" zumindest manche IT-Anwender ("mir wird schon nichts passieren") vorgehen. Eine funktionierende Datensicherung muß deshalb nach festen Regeln und nach geordneten Verfahren, möglichst automatisiert, ablaufen. Sie darf nicht in das Belieben der einzelnen IT-Anwender gestellt werden, da sie sonst leicht in Vergessenheit gerät. Die Regeln zur Datensicherung werden demzufolge als Back-Up-Strategie bezeichnet. Eine solches Verfahren ist zunächst einmal vom Datenbestand (Umfang, Schutzwert, Bedeutung für das Unternehmen/die Behörde) abhängig. Danach muß entschieden werden, mit welchen Mitteln und Geräten es technisch umgesetzt werden kann. Drei grundlegende Methoden, die einzeln verwendet oder sinnvoll miteinander verknüpft werden können, kommen hierfür in Betracht:

Volldatensicherung (total Back-Up)

Die Datenbestände und Programme werden bei jeder Sicherung komplett auf einem externen Datenträger gespeichert. Damit wird der gesamte Bestand gesichert; dieses Verfahren braucht jedoch viel Zeit.

Teildatensicherung (incremental Back-Up)

Basierend auf der letzten Volldatensicherung werden nur die Dateien erneut gesichert, die sich seit der letzten Volldatensicherung und den darauffolgenden Teildatensicherungen verändert haben. Dieses Verfahren geht relativ schnell und eignet sich für die tägliche Sicherung großer Datenbestände. Zur Wiederherstellung eines Datenbestandes sind deshalb die letzte Volldaten- und alle seitherigen Teildatensicherungen notwendig.

Differentielle Datensicherung (differential Back-Up)

Bei dieser Sicherungsart werden - ausgehend von der letzten Volldatensicherung - alle Dateien, die sich verändert haben, völlig unabhängig davon, ob sie bei der letzten Differentialsicherung bereits gesichert wurden oder nicht, erneut gesichert. Dies hat den Vorteil, daß bei Datenverlusten nur das letzte total Back-Up und das letzte differential Back-Up neu aufgespielt werden müssen, um den Bestand zu rekonstruieren.

Bei der Beurteilung, wie die Daten gesichert werden, muß die Kombination der oben vorgestellten Strategien überdacht und festgelegt werden. Außerdem spielen hier die Auswirkungen von Datenverlusten, ebenso wie der (zeitliche) Aufwand für die Rekonstruktion der Daten, eine wesentliche Rolle. Es gilt dabei der Grundsatz: Je häufiger gesichert wird, d.h. je aktueller die Sicherung ist, desto geringer ist der Aufwand zur Rekonstruktion. In der Praxis hat sich deshalb eine Kombination aus Volldaten- und Teildatensicherung durchgesetzt. Die zeitaufwendige Volldatensicherung läuft gewöhnlich einmal wöchentlich ab (nachts, außerhalb der normalen Betriebszeit), um zum einen auch alle Daten sichern zu können und zum anderen die Betriebsabläufe nicht zu beeinträchtigen, da während der Sicherung nicht auf dem System gearbeitet werden sollte. Sind Dateien von Anwendern geöffnet, d.h. wird mit ihnen gearbeitet, sind sie für die Datensicherung gesperrt und werden nicht mitgesichert. Die Teildatensicherung wird ebenfalls außerhalb der normalen Betriebszeit des Systems durchgeführt. Da diese Art schneller abläuft, werden incremental Back-Ups zumeist täglich automatisiert gefahren. Ist das Verfahren geregelt und festgelegt,

müssen die Mittel der Datensicherung bestimmt werden. Datensicherungsmittel sind Datenträger (Disketten, Bänder, Festplatten, optische Speicher etc.), die jedoch auch Alterungsprozessen und (Hardware-) Defekten ausgesetzt sind. Zur Vermeidung von solchen Ausfällen werden nicht nur ein, sondern mehrere Datenträger verwendet.

Bewährt hat sich dabei in der Praxis das sog. Großvater-Vater-Sohn-Prinzip. Zur Sicherung wird jeweils der nächste Datenträger benutzt, d.h. erst beim 4. Sicherungslauf wird der erste Datenträger ("Großvater") erneut überschrieben. In komplexen Systemen mit großen Datenbeständen wird dieses Prinzip zwar beibehalten, jedoch die Zahl der Sicherungsdatenträger wesentlich erhöht, z.B. pro (Arbeits-)Tag ein Träger. Von Bedeutung ist ferner die Art der Datenhaltung. Erfolgt sie zentral, ist eine automatisierte Datensicherung wesentlich einfacher durchzuführen als in einem verteilten System oder gar bei vielen, nicht vernetzten Einzelgeräten. Neben der Eignung der Datensicherungssoftware kommt es ebenso auf die Auswahl der passenden Hardware an. Bei Einzelplatz-PC wird die Datensicherung durch den PC selbst durchgeführt und der Bestand auf Disketten kopiert. Dieses Verfahren ist sehr zeitaufwendig und wenig sinnvoll in vernetzten Systemen mit großen Datenbeständen. Hier kommen idealerweise Diskettenlaufwerke, Wechselplatten, Bernoulli-Laufwerke, MOD-Laufwerke und verschiedene Varianten von Bandlaufwerken zum Einsatz.

Die heutzutage verwendeten Bandlaufwerke (Streamer) speichern die Daten auf unterschiedlichen Datenträgern. Die hierzu eingesetzten Magnetbänder sind Audio-Cassetten, DAT - Digital Audio Tapes, 8-MM Helical Scan, 1/2" Computer-Cartridges und Data-Cartdriges nach QiC-Standard. Häufigste Vertreter in der Praxis sind Qic-Streamer-Cartridges für kleinere und DAT-Bänder für große Datenbestände. Sicherungslaufwerke gibt es in zwei Versionen: Start/Stop-Laufwerke, mit denen auch einzelne Dateien gesichert werden können, und Voll-Streamer, die in relativ kurzer Zeit komplette Datenbestände kopieren, d.h. sichern können. Dabei muß berücksichtigt werden, daß die Streamer nach Standards arbeiten, die es ermöglichen, die mit ihnen gesicherten Daten auf

allen anderen Laufwerken des Systems wieder sichtbar zu machen. Die Art der Bandsicherung wird entweder als Image-Back-Up (Festplatteninhalt wird komplett auf Band gesichert, ohne daß dabei Rücksicht auf die Plattenorganisation, d.h. Zuordnung der Dateien in der Struktur des Speichers, genommen wird; ein späterer Zugriff auf einzelne Dateien ist deshalb nicht möglich; das Verfahren läuft jedoch sehr schnell ab) oder als File-Back-Up durchgeführt (die Dateien werden getrennt und separat auf dem Band abgespeichert, weshalb sich hier einzelne Dateien auch wieder herstellen lassen; allerdings benötigt das Verfahren sehr viel Zeit).

Zur Hardware gehört auch die geeignete Datensicherungssoftware. Besonders in automatisch ablaufenden Systemen muß die Software über ausgefeilte Parameter verfügen, die es erlauben, die Datensicherung auf die spezifischen Bedürfnisse des Anwenders abzustellen. Außerdem ist die Benutzerfreundlichkeit wesentliches Kriterium, denn Datensicherung wird oftmals nicht von Fachleuten, sondern von normalen DV-Anwendern durchgeführt. Dies macht die genaue Beschreibung der durchzuführenden Back-Up-Maßnahmen erforderlich. Im Konzept ist nicht nur zu regeln, welche Verfahren und Systeme zum Einsatz kommen, sondern auch die organisatorische und personelle Durchführung. Nur klare und verständliche Handlungsanweisungen sowie Kompetenz- und Verantwortlichkeitszuweisungen sichern den korrekten Ablauf der Datensicherung. Besondere Bedeutung hat hierbei auch der Umgang mit den zur Sicherung eingesetzten Datenträgern sowie deren Aufbewahrung (Datenträgerhandling). Datenträger jeder Art sind insbesondere den Bedrohungen durch Diebstahl ausgesetzt. Mit dem PC am Arbeitsplatz ergeben sich für den Innentäter nahezu unbegrenzte Möglichkeiten, Datenträger zu entwenden, große Datenmengen auf mitgebrachte Datenträger unbemerkt zu kopieren und diese aufgrund ihrer geringen Größe unauffällig auch aus Sicherheitsbereichen herauszuschleusen. Über private Datenträger, die am Arbeitsplatz eingespielt werden, werden oftmals ganze Netze mit Viren verseucht. Schutzmaßnahmen gegen die erwähnten Gefahren können deshalb darin bestehen:

- Verbot des Mitbringens und Nutzens privater (behörden- oder betriebs-

fremder) Software

- Einsatz von Arbeitsplatz-PC ohne Diskettenlaufwerk ("discless")

- mechanischer Verschluß der Diskettenlaufwerke durch spezielle Einsätze
- elektronische Verriegelungssysteme, die Laufwerke nur über einen Schlüssel schalter freigeben

- Einsatz ausschließlich schreibgeschützter Disketten

- Prüfung durch Virenscanner

Zusätzliche Gefahren ergeben sich durch Hardwaredefekte an den Datenträgern (Alterung, mechanische Beschädigungen) und durch Manipulationen der auf den Trägern gespeicherten Daten und vor allem Programme. Bei Back-Up-Datenträgern hat dies unter Umständen zur Folge, daß im Notfall keine Datenbestände restauriert werden können und somit erhebliche Datenverluste eintreten. Deshalb sollte bereits beim Kauf von Datenträgern auf gewisse Qualitätsstandards (Stückprüfungsgarantie, geeignete Verpackung zum Schutz vor mechanischer Beschädigung, garantierte Mindestspeicherungsdauer) geachtet werden. Alle in Behörden oder in Wirtschaftsunternehmen eingesetzten Datenträger sollten mit einer spezifischen Kennzeichnung versehen werden. Diese darf - ohne sie zu beschädigen - nicht abgelöst und wieder angebracht werden können. Dadurch wird auch die Arbeit von etwaigem Kontrollpersonal erleichtert.

Träger ohne Kennzeichen dürfen erst gar nicht vorhanden sein. Eingehende fremde Datenträger sind vor ihrem Einsatz auf Viren (durch Virenscanner) zu prüfen. Datenträger, die sensible Daten enthalten, sind unter Verschluß zu verwahren. Im staatlichen Bereich sind Verschlußsachendaten(-träger) in besonderen Stahlschränken oder Aktensicherungsräumen aufzubewahren, die außerhalb der regelmäßigen Arbeitszeit zu bewachen oder durch eine Gefahrenmeldeanlage technisch zu überwachen sind.

Generell gelten für die Aufbewahrung von Back-Up-Datenträgern folgende Empfehlungen:

In Bereichen

- **mit** Brandmeldesystemen sollten Datensicherungsschränke nach RAL-RG 626/9, Ausführung S 60 DIS, und in Bereichen

- **ohne** Brandmeldesysteme Datensicherungsschränke nach RAL-RG 626/9, Ausführung S 120 DIS,

jeweils mit Schlüssel- und Zahlenkombinationsschloß eingesetzt werden. Die Größe kann entsprechend den Nutzerwünschen gewählt werden.
Datensicherungsschränke und -räume sind Verwahrgelasse zur feuergeschützten Aufbewahrung von Informationsträgern, die neben dem Feuerschutz auch einen begrenzten Einbruchs- und Zugriffsschutz bieten. Sie werden auf der Grundlage des VDMA-Einheitsblattes 24991, Teil 1 und Teil 2, bei der TU Braunschweig geprüft. Die Zertifizierung erfolgt durch die "Forschungs- und Prüfgemeinschaft Geldschränke und Tresoranlagen e. V." als akkreditierter Zertifizierungsstelle, die auch die Liste der zertifizierten Produkte herausgibt. Bei Datensicherungsschränken unterscheidet man die Güteklassen S 60 (60 min Beflammungszeit) und S 120 (120 min Beflammungszeit). Die Zusätze hinter der Klassifizierung bezeichnen den Verwendungszweck:

P = Papier aller Art
D = Datenträger, z. B. Magnetbänder, Filme
DIS = Disketten, 1/2" Magnetbandkassetten einschließlich aller anderen Datenträger

Die Unterscheidung beruht auf der Isolationsleistung, die bei DIS-Schränken am höchsten ist.

Datensicherungsräume sind für große Datenbestände vorgesehen; sie werden nur in die Güteklasse R 60 D eingestuft. Disketteneinsätze sind Einsätze zur Aufbewahrung von Disketten, die in Datensicherungsschränken S 60 P und S 120 P eingebaut werden. Dabei ist zu beachten, daß der Einbau auf genehmigte und im Zertifikat aufgeführte Schranktypen begrenzt ist. Soll ein hoher Schutz gegen einen gewaltlosen Zugriff auf vertrauliche Datenträger gewährleistet sein, wird empfohlen, Datensicherungsschränke nach RAL-RG 626/9 zu verwenden, bei denen ein spezielles Riegelwerk und hochwertige Schlösser eingebaut werden. Für die Aufbewahrung von Verschlußsachen des Geheimhal-

tungsgrades VS-VERTRAULICH und höher sind Datensicherungsschränke nach RAL-RG 626/9 vorgeschrieben. Über zugelassene und geprüfte Datensicherungsschränke und -räume geben die Produktinformationen des BSI Auskunft. Darüber hinaus bieten verschiedene Unternehmen Datensicherungsschränke an, die neben dem Feuerschutz auch über einen definierten Einbruchschutz (z. B. Sicherheitsstufe B oder C) verfügen. Anzumerken ist noch, daß bei einer technischen Überwachung von Stahlschränken durch eine Gefahrenmeldeanlage oftmals sog. kapazitive Feldänderungsmelder eingesetzt werden. Einem wissenschaftlichen Gutachten zufolge führt das durch den Melder aufgebaute Magnetfeld nicht zu einer Beeinflussung/Beschädigung der im Schrank verwahrten Datenträger. Solche Schränke oder Räume sollten jedoch baulich in einem anderen Brandabschnitt des Gebäudes untergebracht werden als die zentralen Einrichtungen des IT-Systems. Sämtliche Komponenten der Datensicherung sind in jedem Fall gegen den Zugriff Unbefugter zu schützen.

Wenn magnetische Datenträger nicht mehr gebraucht werden, ist deren Inhalt vor einer Entsorgung oder Wiederverwendung unkenntlich zu machen. Dies gilt auch dann, wenn beispielsweise solche Datenträger zu Reparaturzwecken außer Haus gegeben werden müssen. Für die vom BSI geprüften Löschgeräte gilt, daß sie schutzbedürftige Daten, die auf flexiblen magnetischen Datenträgern gespeichert sind, so vernichten, daß die Datenträger erhalten bleiben und eine Wiederverwendung möglich ist. Bei Löschgeräten wird der zu löschende Datenträger einem starken magnetischen Gleich- oder Wechselfeld ausgesetzt (Durchflutungslöschung). Die Prüfung der Löschgeräte erfolgt durch das BSI auf der Grundlage der Norm DIN 33 858 . Die Klassifizierung der Löschgeräte berücksichtigt sowohl die erzielte Löschdämpfung als auch die Koerzitivfeldstärke der Datenträger (siehe Tabelle).

Anforderungsstufen für Löschgeräte Erzielte Löschdämpfung		zu löschender Datenträger		
		Koerzitivfeldstärke		
45 dB	90 dB	kA/m bis	Oe bis	Beispiele
A 1	B 1	28	350	Magnetbänder nach DIN EN 21 864 Identifikationskarten nach DIN EN 27811, Teil 2 Disketten Typen 102, 102, 201, 202, 203 nach DIN EN 29983
A 2	B 2	60	750	Magnetbandkassetten nach prEN 29 661 Disketten-Typen 204, 301, 302 nach DIN EN 29983
A 3	B 3	400	5.000	Identifikationskarten mit hochkoerzitivem Magnetstreifen

Datenträger sollten nach ihrem letztmaligen Gebrauch nicht einfach entsorgt, sondern vernichtet werden, da die auf ihnen gespeicherten Daten für Datenspione weiterhin wertvoll sein können. Bei der Vernichtung nicht mehr benötigter Datenträger sowie von Ausdrucken (Hard-Copy) sollten die Produktempfehlungen des BSI beachtet werden. Die dort aufgeführten Vernichtungsgeräte (Akten-, Magnetband-, Carbonband- und Mikrofilmvernichter) entsprechen den Sicherheitsstufen 4 und 5 nach DIN 32 757 (Partikelgrößen gemäß DIN 32757, Sicherheitsstufe 4: £ (2 x 15) mm^2 oder £ 30 mm^2 / Sicherheitsstufe 5: £ (0,8 x 13) mm^2 oder £ 10 mm^2. Sie sind für die Vernichtung von vertraulichen Informationsträgern (z. B. Verschlußsachen) geeignet. Für die Informationsträgervernichtung, bei der keine so hohen Sicherheitsanforderungen zu stellen sind, können Vernichtungsgeräte der Sicherheitsstufe 3 verwendet werden. Für sonstige Informationsträger, die nur unlesbar gemacht werden sollen, reichen Geräte der Sicherheitsstufen 2 oder 1 aus. Geräte der Sicherheitsstufen 1 bis 3 sind in der Liste nicht enthalten, sie können jedoch von den aufgeführten Herstellerfirmen geliefert werden. Die in der Auflistung enthaltenen Angaben beruhen auf Herstelleraussagen. Eine Prüfung der Vernichtungsgeräte durch eine unabhängige Prüfstelle auf der Grundlage der DIN 32 757 erfolgte nicht.

Bei besonders sicherheitskritischen Daten oder bei großen Datenbeständen empfiehlt sich, die Back-Ups extern zu lagern. Extern bedeutet hier zunächst,

daß die Lagerung in einem separaten Gebäude des Unternehmens oder der Behörde erfolgt. Die Sicherheitsstandards sind dieselben wie im eigenen Bereich. Nur in Ausnahmefällen sollte die Aufbewahrung sensibler Datenträger durch externe Dienstleistungsanbieter erfolgen. Kritisch ist hierbei die Gewährleistung der personellen und baulich-technischen Sicherheit. Für Verschlußsachen kann dies nur unter ganz besonderen Voraussetzungen und nach Beratung durch die zuständigen Behörden erfolgen.

Treten jedoch tatsächlich Datenverluste auf, und müssen Sicherungen wieder eingespielt werden, sind bereits im Vorfeld entsprechende organisatorische, technische und personelle Maßnahmen festzulegen. Solche Konzepte werden auch als Wiederanlaufplanung bezeichnet. In IT-Systemen spielen dabei zunächst die Art der Vernetzung, die Hardware und die Form der Datensicherung eine entscheidende Rolle. Das Netz sollte über redundante Kabelwege verfügen, um über zweite Leitungen ausgefallene Verbindungen und Schnittstellen und damit auch Endgeräte überhaupt noch erreichen zu können. Dies wurde am Beispiel der Sekundär-Verkabelung in LAN bereits verdeutlicht. Automatische Umschalteinrichtungen erleichtern dies erheblich. Die Hardware muß für die einzuspielenden Datenträger geeignet sein. Es nützt beispielsweise wenig, wenn die letzte Sicherung auf 5 1/4"-Disketten durchgeführt wurde und in der Zwischenzeit nur noch 3 1/2"- Diskettenlaufwerke zur Verfügung stehen. Back-Ups von Daten sollten immer aktuell, vollständig sowie jederzeit verfügbar sein. Eine korrekte Wiederanlaufplanung spart im Schadensfall Zeit und Aufwand. Speziell ausgebildetes Personal für solche Maßnahmen sollte eine selbstverständliche Voraussetzung sein und das erstellte Konzept dabei immer wieder auf Praktikabilität und Realisierbarkeit getestet werden. Diese Testläufe sind zu dokumentieren, um erkannte Schwachstellen auszuräumen. Die Entwicklungen in der Hardware-, Software- und Netzkonfiguration bedingen auch das Fortschreiben der Back-Up-Konzepte einschließlich der Wiederanlaufplanung. Bei allen Vorstellungen zum Schutz der IT-Systeme handelt es sich nicht um statische Festschreibungen, sondern um Planungen, die immer wieder den technischen Innovationen in der eigenen IT-Entwicklung angepaßt werden müssen. Bei Totalaus-

fällen von IT-Komponenten oder des gesamten Systems muß auch eine Konzeption für die Ersatzbeschaffung berücksichtigt werden. Dieses reicht von Herstellerleistungen (Ersatzgarantie von zentralen Einrichtungen, z.B. Servern oder aktiven Netzkomponenten) während einer bestimmten Zeit bis hin zu parallelen (redundanten) Konfigurationslösungen. Dabei werden folgende Lösungsmöglichkeiten unterschieden:

"kaltes" Back-Up: Für den Notfall stehen Ersatzräume zur Verfügung, die bei Bedarf mit den erforderlichen DV-Einrichtungen ausgestattet werden können. Die Wiederanlaufzeit ist dabei maßgeblich von der Beschaffungszeit der Ersatzkomponenten abhängig.

"warmes" Back-Up: In einem "warmen" Back-Up-Rechenzentrum werden sämtliche notwendigen Einrichtungen bereitgehalten. Dieses Ersatzsystem gewährleistet einen Wiederanlauf in wenigen Stunden. Aufgrund der hohen Investitionskosten werden solche Lösungen von mehreren Unternehmen oder Behörden gemeinsam eingerichtet, betrieben und für den Notfall vorgehalten; eine besondere Form ist hier das mobile Back-Up-RZ, das von Dienstleistungsanbietern vorgehalten wird und unter Berücksichtigung der nutzerspezifischen Gegebenheiten den Wiederanlauf innerhalb von 24 Stunden sicherstellt.

"heißes" Back-Up: Durch eine zweite IT-Austattung direkt vor Ort ist der Wiederanlauf sofort möglich. Redundante Hardware und permanent aktualisierte Datenbestände als Voraussetzung dieser Lösung haben jedoch ihren Preis und müssen deshalb in ei- nem angemessenen Verhältnis zum möglichen Schaden ("worst case") stehen.

Unterstützt werden kann die Wiederanlaufplanung durch sog. Back-Up-Tools. Dies sind Software- und ggf. auch Hardwareeinrichtungen, die zwar teuer, aber unter Umständen sehr nützlich sein können. Sie basieren auf speziellen Datenbanksystemen und unterstützen das Einspielen von Daten sowie die Erstellung von Planungskonzepten. Insgesamt können Back-Up-Konzepte, Back-Up-Tools und Back-Up-Dienstleistungen externer Anbieter den immer wieder in der Fachpresse veröffentlichten Marktübersichten entnommen werden (u.a. "Marktüber-

sicht Back-Up“ des „Sicherheitsberaters“ Ausgabe 6/96, „Back-Up-Report“ der „KES“ - Ausgabe 95/3).

Zum Abschluß dieses Kapitels soll noch einmal grob aufgezeigt werden, welche Komponenten ein Back-Up-Konzept in einem LAN aufweisen sollte:

- automatische Datensicherung nach dem "Großvater-Vater-Sohn-Prinzip", d.h. tägliche Sicherung der Daten (incremental Back-Up), separate wöchentliche sowie zusätzlich monatliche oder quartalsweise Volldatensicherung
- zentrale Datenhaltung auf dem/den File-Server(n), Sicherung der Verfügbarkeit des Servers mit den auf S. 86 dargestellten Maßnahmen
- Einsatz von Streamern zur Datensicherung (QIC- oder DAT-Standard)
- Datensicherungskomponenten gegen unbefugten Zugriff schützen, in einen an deren Brandabschnitt des Gebäudes verlegen
- sichere Aufbewahrung der Datenträger
- spezifische Kennzeichnung von Datenträgern
- Regelung für die Aufbewahrungsdauer von Teil- oder Komplettsicherungen
- ggf. externe Datenträgerlagerung
- Regelungen für die Löschung und Vernichtung von Datenträgern
- Ausbildung des Personals
- organisatorische Regelungen für die Sicherung
- Wiederanlaufkonzept
- Einsatz geeigneter Software-Tools
- Beschaffung geeigneter Hardware
- redundante Auslegung des Netzes zumindest im Sekundärbereich
- Richtlinien für Kontrollen und Maßnahmen bei Sicherheitsverstößen

6.2 Personelle Sicherheitsmaßnahmen

Unter personellen Sicherheitsmaßnahmen im Sinne des staatlichen Geheim-

schutzes versteht man die Sicherheitsüberprüfung von Personen die mit einer sicherheitsempfindlichen Tätigkeit betraut werden sollen. Die Überprüfung richtet sich nach dem "Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes (Sicherheitsüberprüfungsgesetz - SÜG)" vom 20. April 1994 bzw. nach den entsprechenden Landesbestimmungen. Der Begriff der sicherheitsempfindlichen Tätigkeit ist dabei eng mit der Verschlußsachendefinition und/oder dem Tätigwerden in einem Sicherheitsbereich verknüpft. Eine sicherheitsempfindliche Tätigkeit übt demnach aus, wer Zugang zu Verschlußsachen (Verschlußsachen sind im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse, unabhängig von ihrer Darstellungsform. Sie werden entsprechend ihrer Schutzbedürftigkeit von einer amtlichen Stelle oder auf deren Veranlassung eingestuft.) hat, oder ihn sich verschaffen kann, wer Zugang zu Verschlußsachen überstaatlicher Einrichtungen hat oder ihn sich verschaffen kann oder in einem Bereich tätig ist, der durch die zuständige oberste Landesbehörde im Einvernehmen mit dem Innenministerium zum Sicherheitsbereich erklärt wurde.

In Abhängigkeit von den Zugangsmöglichkeiten zu VS-VERTRAULICH und höher eingestuften Verschlußsachen sind drei Arten (einfache, erweiterte, erweiterte mit Sicherheitsermittlungen) der Sicherheitsüberprüfung vorgesehen. Die Voraussetzungen für die jeweilige Überprüfungsart und die dabei durchzuführenden Maßnahmen sind im Gesetz geregelt und erläutert. Die Bestimmungen für die Sicherheitsüberprüfung im staatlichen Geheimschutz sind bindend und nicht nur auf den Behördenbereich beschränkt. Über das "Geheimschutzhandbuch in der Wirtschaft" werden auch für Personen in der Privatwirtschaft, die Zugang zu Verschlußsachen im Rahmen der Abwicklung von öffentlichen Aufträgen haben können, Sicherheitsüberprüfungen nach den geltenden bundes- und landesgesetzlichen Regelungen vorgeschrieben. Die Durchführung solcher Überprüfungen, die Verfahrensvoraussetzungen und die Aufnahme von Wirtschaftsunternehmen in die sog. Geheimschutzbetreuung durch des Bundes oder eines Landes muß im Einzelfall abgeklärt werden. Auf eine breitere Darstellung wird deshalb verzichtet.

Personelle Sicherheitsmaßnahmen außerhalb des staatlichen Bereichs können z.B. sein:

- Klare Regelungen (erneute Schulung, Verpflichtung zur Teilnahme an Schulungs- und Fortbildungsmaßnahmen, förmliche Belehrung, Abmahnung, Umsetzung) bis hin zu arbeitsrechtlichen Konsequenzen (Kündigung) bei erkannten Sicherheitsverstößen

- eindeutige Zuweisung von Kompetenzen und Zuständigkeiten

- Sensibilisierung durch Vorträge, regelmäßige Sicherheitsbelehrungen und Schulungen (Akzeptanzförderung)

6.3 Organisatorische Sicherheitsmaßnahmen

Die meisten der möglichen organisatorischen Schutzmaßnahmen wurden bereits in den entsprechenden Passagen dieser Broschüre aufgezeigt. Die nachfolgende Aufstellung soll noch einmal einen Überblick über diesen Aspekt ermöglichen; sie erhebt jedoch keinen Anspruch auf Vollständigkeit.

- ***Erstellung eines IT-Sicherheitskonzepts***

- ***Grundlegende Festlegung von Verantwortlichkeiten im Rahmen der IT-Sicherheit in einer innerbetrieblichen/innerbehördlichen Organisationsanweisung***

- ***Festlegung von Ansprechpartnern bei IT-Sicherheitsmaßnahmen***

- ***Erlaß arbeitsplatzspezifischer Regelungen, z.B. für Paßwort und Benutzerkennung sowie für das damit verbundene Sicherheitsmanagement***

- ***Dokumentation des gesamten Systems sowie permanente Fortschreibung***

- ***Einführung von Richtlinien für Revision und Kontrolle***

- ***Erarbeitung von Back-Up-Konzept und Wiederanlaufplanung (Datensicherungsvorschriften)***

- ***Durchführung von kontrollierter, zentraler Beschaffung von Hard- und Software***

- ***Verbot des Einbringens privater Software oder Hardware***

- ***Führung von Bestandsverzeichnissen über Hard- und Software***
- ***Kennzeichnung von Datenträgern***
- ***Versiegelung von Gehäusen und (offenen) Schnittstellen***
- ***Einsatz geprüfter (durch das BSI zertifizierter) Produkte***
- ***Grundsätzliche organisatorische und personelle Trennung von Sicherheit und Betrieb***
- ***Schaffung von Zugangs- und Zugriffsregelungen für eigenes sowie für Fremdpersonal (Wartungstechniker etc.)***
- ***regelmäßige Wartung und Systempflege aller Komponenten***
- ***Erlaß von Aufbewahrungs-, Lösch- und Vernichtungsrichtlinien für Datenträger***
- ***Einsatz von Virenscannern, Regelung der Ein- und Ausgangskontrolle***
- ***Erarbeitung von Protokollierungsvorgaben***
- ***Festlegung von Sicherheitsbereichen für zentrale Einrichtungen sowie abgestufte Zugangsregelungen für Liegenschaft, Gebäude, Gebäudeteile und Sicherheitsbereiche***
- ***Festlegung der Kommunikationsbeziehungen (wer, wann, mit wem, auf welchen Medien)***
- ***Erstellung von Verkabelungs- und EMV-Schutzkonzept***
- ***Erarbeitung von Notfall- und Katastrophenschutzkonzepten (vgl. Ziffer 6.4)***

6.4 Notfall-/Katastrophenschutzkonzepte

Bei diesem Themenbereich ergeben sich zwangsläufig Überschneidungen mit dem Teil Wiederanlaufplanung, denn diese ist integraler Bestandteil jeder Notfallplanung, um nach großen Schadensereignissen schnell einen ordnungsgemäßen Betriebszustand wiederherzustellen. Solche Konzepte und Vorsorgemaßnahmen sind insbesondere dann notwendig, wenn die Existenz der Behörde oder des Unternehmens vom Funktionieren des IT-Systems entscheidend ab-

hängt. Nach heutigen Schätzungen ist beispielsweise die Überlebenszeit einer Bank oder einer Handelsgesellschaft nach einem Totalausfall des IT-Systems auf weniger als 3 Tage beschränkt. Umweltkatastrophen (Hochwasser, Überschwemmungen, Erdbeben etc.) lassen sich zwar kaum verhindern, präventive Maßnahmen helfen jedoch, Schäden einzudämmen und Risiken kalkulierbarer zu machen. Katastrophenvorsorge ist nicht nur die Planung bei elementaren Schadensereignissen, sondern sie umfaßt sämtliche Maßnahmen, die geeignet sind, Hard- und Softwareausfälle sowie Datenverluste - wodurch immer sie auch entstehen - zu kompensieren. Solche Konzepte dienen zum Schutz der Verfügbarkeit des IT-Systems.

Viele der in dieser Broschüre vorgestellten Schutzmaßnahmen sind deshalb praktizierte Notfallplanung. Diese Maßnahmen und Handlungsanweisungen sollten (kurz und verständlich) in einem Notfallhandbuch zusammengetragen werden, das im Bedarfsfall den Mitarbeitern und Verantwortlichen auch leicht zugänglich sein muß. Dabei sind nicht nur Schutz- und Wiederanlauf-, sondern auch Beweissicherungsmaßnahmen (bei Datenverlusten durch Diebstahl und Spionage, Manipulation oder Sabotage) zu berücksichtigen. Das eingangs vorgestellte Sicherheitskonzept basiert gerade auf dem Aspekt, alle relevanten Risiken und Bedrohungen zu erfassen und zu analysieren, sollten sie auf den ersten Blick auch noch so abwegig sein. Durch die Bewertung wird deutlich, welche Präventiv- und Nachsorgemaßnahmen dann erforderlich sind.

Deutlich geworden ist gewiß auch, daß eine 100 %ige Sicherheit bei einem geordneten Betriebsablauf nicht erreicht werden kann. Gewisse Restrisiken bleiben und müssen getragen werden. Da Notfall- und Katastrophenschutzpläne sozusagen den Finger auf den wunden Punkt legen, d.h. auch kalkulierte Schwachstellen aufzeigen, müssen sie in zwei Bereiche aufgeteilt werden. Der öffentliche Teil beinhaltet die sog. Alarmpläne, die im Notfall helfen, die richtigen Sofortmaßnahmen einzuleiten. Der vertrauliche Teil (Einsatzpläne für den jeweiligen Notfall) zeigt alle sicherheitsrelevanten Vorgaben, sämtliche Details des IT-Systems, wie evtl. Schwachstellen, und regelt spezifisch die konkreten Maß-

nahmen. Schwerpunktmäßig sollten Notfall- und Katastrophenschutzkonzepte folgende Bereiche abdecken:

- Notfallhandbuch
- Verfügbarkeit von Soft- und Hardware
- Datensicherung (Back-Up-Konzept)
- Wiederanlaufplanung
- Dokumentation (Ersatzdokumentation)
- USV / NEA / Überspannung
- Brandschutz / Klimaplanung
- bauliche, mechanische, elektrische und elektronische Sicherheit

Personelle und organisatorische Vorgaben runden diese ab.

6.5 Versicherungsschutz

Abgeschlossene Versicherungen sind keine Schutzmaßnahmen gegen Datenspione oder andere Angriffe auf die EDV. Sie helfen jedoch, die Kostenfolgen bei Schadensereignissen erträglicher zu gestalten.

Die EDV-Versicherung basiert auf den Bestimmungen der Elektronikversicherung und den allgemeinen Bedingungen für diese (ABE). Sie deckt nahezu sämtliche Gefahrenbereiche der IT-Welt (Diebstahl, Fahrlässigkeit, Bedienungsfehler, Überspannung, Brand, Wasser, Sabotage, Vandalismus, höhere Gewalt, Konstruktions-, Material- und Ausführungsfehler u.v.a. mehr) ab. Ausgeschlossen sind Vorsatz, Krieg, Bürgerkrieg, innere Unruhen, Kernenergie, Erdbeben und deren Folgen sowie betriebsbedingte Abnutzung oder Alterung.

Die EDV-Versicherung ist dabei in die Teilbereiche Elektronik-Betriebsunterbrechung-, Datenträger-, Mehrkosten-, Sach- und Softwareversicherung unterteilt. Zu den einzelnen Versicherungsarten, vertraglichen Bestimmungen, abgedeckten und ausgeschlossenen Risiken sowie zu Beiträgen sollten

beim jeweiligen Versicherungsträger weitere Auskünfte eingeholt werden. Die Notwendigkeit eines Versicherungsschutzes muß durch den Bedarfsträger selbst ermittelt werden.

7. Anhang 2

7.1 Cyber-Terrorismus - eine neue Herausforderung

Mitte dieses Jahres verbreiteten verschiedene deutsche Zeitungen Berichte aus angloamerikanischen Medien, wonach Erpresserbanden aus den USA und aus Rußland amerikanischen und britischen Banken und Versicherungen schon mehr als eine Milliarde DM abgenötigt hätten, indem sie damit drohten, computerisierte Daten zu vernichten.

Beispielsweise sollen die Täter als vorgebliche Marketingexperten DV-Bereiche von Unternehmen vorrangig nach Zugangs-Codes ausgekundschaftet haben. Anschließend hätten sie mit Hilfe ihrer Insider-Kenntnisse ihre Erpressungswaffen eingeschleust und eine im "geknackten" Firmen-Code abgefaßte Drohung an die Unternehmensleitung gerichtet ("Haben wir Sie davon überzeugt, daß wir Ihren Zentralcomputer zum Absturz bringen können?"). Mehrere britische Geldhäuser sollen daraufhin umgerechnet jeweils mehr als 30 Millionen Mark Schutzgeld bezahlt haben. In anderen Fällen traten die Elektronikerpresser allein mit der Erklärung, mittels Hacker-Zugriff seien sie in den Besitz vertraulicher Informationen gelangt, an ihre Opfer heran. Gegen eine entsprechende Kostenerstattung seien sie allerdings bereit, der betroffenen Bank bei der Wiederbeschaffung der sensiblen Kunden-Daten, die gewiß nicht für Journalisten oder Finanzbehörden bestimmt seien, behilflich zu sein. Nicht selten mußten die Betroffenen hernach feststellen, daß sie auf Trickbetrüger hereingefallen waren; der gegen einen hohen Geldbetrag erworbene Diskettenstapel erwies sich nach genauerer Untersuchung als eine Ansammlung älterer Leerdisketten. Eine weitere Tätergruppe drohte ihren Opfern den Gebrauch sog. Herf-Kanonen an. Diese strahlten angeblich Radiowellen höchster Intensität ("einen elektomagnetischen Wind") ab, die hochgezüchtete Elektronengehirne in Sekundenbruchteilen kollabieren ließen und auf diese Weise wertvolle Datenbestände unwiderbringlich vernichten würden. Auch hier nahmen die Erpreßten

letzten Endes lieber die Zahlung eines hohen Geldbetrags in Kauf, als das Risiko eines gravierenden Datenverlustes einzugehen.
Bemerkenswerterweise gibt es nur äußerst dürftige Anhaltspunkte dafür, daß sich die aufgezeigten Ereignisse (tatsächlich) auch so zugetragen haben. Andererseits läßt sich aber ebensowenig von vornherein völlig ausschließen, daß nicht doch raffinierte Elektronikerpresser am Werk sind. Was hat es letztlich mit dem neu aufgetretenen Phänomen des "Cyber-Terrorismus" auf sich?

Diese Informationsschrift hat versucht, deutlich zu machen, daß Computersysteme ausgesprochen verwundbar sind. Jedenfalls ist immer dann, wenn keine oder nur unzulängliche Schutzvorkehrungen getroffen worden sind, damit zu rechnen, daß kaum vorstellbare Bedrohungsszenarien Realität annehmen können. Hinzu kommt die große Angst, insbesondere der Finanzbranche, mit jeglicher Art von Computerkriminalität in Verbindung gebracht zu werden. Schließlich sollen die Kunden darauf bauen können, daß ihre Geldgeschäfte diskret abgewickelt werden, und daß sich ihr Vermögen jederzeit aus den Zahlen der Datenbestände der Bankcomputer wieder in harte Währung zurückverwandeln läßt. Als Resümee bleibt daher festzuhalten, daß der "Cyber-Terrorismus" zwar durchaus eine ernstzunehmende Gefahr darstellt, vorbeugende DV-Absicherungsmaßnahmen allgemeiner Art das Risiko allerdings erheblich verringern können.

Diese Aussage gilt insbesondere auch im Hinblick auf "Cyber-Waffen", die angeblich in Gestalt von Computerviren Software in Datenmüll verwandeln oder als elektromagnetische "Kanonen" Hardware zu Siliziumschrott machen. Als potentielle Angriffsziele kommen dabei sowohl militärische Einrichtungen, die immer mehr von Computertechnik und elektronischer Kommunikation abhängen, als auch zivile Objekte wie Flughäfen, (Kern-) Kraftwerke oder Banken in Betracht. Daß sich die Streitkräfte mit diesem Thema beschäftigen (müssen), dürfte sich wohl von selbst verstehen. Angriffssysteme und Abwehrstrategien spielen dabei gleichermaßen eine Rolle. Eine spezielle Gefahr erwächst daraus, daß auch terroristische Organisationen versucht sein könnten, auf diesem

Gebiet mitzumischen. Zumindest für staatlich gestützte bzw. gelenkte Terrorgruppen dürften die aufwendigen Mittel für elektromagnetische Computersabotage kein Problem darstellen.

8. Anhang 3

8.1 Druckschriften und Publikationen

8.1.1 Druckschriften des Landesamtes für Verfassungsschutz Baden-Württemberg

Auflistung vgl. Seite 134

8.1.2 Publikationen des BSI

Literaturliste des BSI vgl. Seiten 135 - 138

Bitte beachten Sie die Angaben des BSI zum Rückporto bei Anforderung von Unterlagen !

8.1.3 BSI-Mailbox

Informationen zur Mailbox des BSI (BSI-BOX) vgl. Seiten 139 - 141

Bitte beachten Sie das INTERNET-Angebot des BSI unter der Adresse:

http://www.bsi.bund.de

8.1.4 Paßwortregeln

Empfehlungen des Bundesbeauftragten für den Datenschutz vgl. Seite 142

8.1.5 Fax-Übertragung

Leitfaden des Landesbeauftragten für den Datenschutz Rheinland-Pfalz vgl. Seite 143

Nr.:	I n h a l t
1	Anforderungen an Gefahrenmeldeanlagen
2	Anforderungen an Aktensicherungsräume
3	Anforderungen an Aktenverwahrräume
4	Anforderungen an Umschränke
5	Anforderungen an Datensicherungsschränke
6	Hinweise zur Beschaffung von VS-Stahlschränken
7	Hinweise zur Beschaffung von VS-Schlüsselbehältern
8	Hinweise zur Beschaffung von VS-Transportbehältern
9	Hinweise zur Beschaffung von VS-Vernichtungsgeräten
10	Technische Anforderungen an eine VS-Sicherheitstür I
11	Technische Anforderungen an eine VS-Sicherheitstür II
12	Technische Anforderungen an eine VS-Sicherheitstür III
13	Informationen für die Betreiber von CDM-Anlagen
14	Informationen für die Betreiber von SEZU-Anlagen
15	Informationen für die Betreiber von SDN-Anlagen
16	Abhör- und sicherheitstechnische Forderungen an abhör-geschützte Besprechungsräume
17	Abhör- und sicherheitstechnische Forderungen an abhör-geschützte und abhörsichere Räume
18	Abhör- und sicherheitstechnische Forderungen an abhör-geschützte Büroräume
19	Abhör- und sicherheitstechnische Forderungen an abhör-sichere Besprechungsräume
20	VS-NfD - Merkblatt
21	Produktliste
22	Medienverzeichnis
24	Merkblatt Lauschabwehr
26	Aufbau einer Kryptobetriebsstelle

BSI-Kurzinformationen im Faltblattformat

In begrenzter Anzahl gegen Übersendung eines mit 3,00 DM frankierten und adressierten Rückumschlages (C 4) erhältlich:

Fbl Ö 01
Literaturliste

♦

Fbl Ö 02
Sicherheitsmaßnahmen beim PC-Einsatz

♦

Fbl Ö 03
Kurzinformationen zu Computer-Viren

♦

Fbl Ö 04
Überkoppeln auf Leitungen

♦

Fbl Ö 05
Schutzmaßnahmen gegen illegales Abhören

♦

Fbl Ö 06
IT-Sicherheitsberatung

♦

Fbl Ö 07
IT-Sicherheitskriterien und Evaluierung nach ITSEC

♦

Fbl Ö 08
IT-Grundschutz

♦

Fbl Ö 09
Technikfolgen-Abschätzung und IT-Sicherheit

♦

Fbl Ö 10
BSI-Sicherheitszertifikate
Was Anwender wissen sollten

♦

Fbl Ö 11
Digitale Telekommunikationsanlagen
Gefährdungen und Sicherheitsmaßnahmen - Auszug -

♦

Fbl Ö 12
Bloßstellende Abstrahlung
- eine wenig bekannte Gefahr -

♦

Fbl Ö 13
Funktionalität von PC-Sicherheitsprodukten

♦

Fbl Ö 14
Informationen zur Mailbox (BSI-BOX)

♦

Fbl Ö 15
Sicherheit im Internet

BSI-Kurzinformationen im Faltblattformat

In begrenzter Anzahl gegenÜbersendung eines mit 3,00 DM frankierten und adressierten Rückumschlages (C 4) erhältlich:

Fbl Ö 16
Einbruchmeldeanlagen

♦

Fbl Ö 17
Sicherheit durch Verschlüsselung

♦

Fbl Ö 18
Elektronisches Bezahlen

Fbl Ö 19
Makro-Viren

Fbl Ö 20
Digitale Signatur

Fbl Ö 21
Common Criteria

♦

Fbl BSI 7092
Allg. Informationen, Organisationsübersicht
Auszug aus dem BSI-Gesetz

♦

Fbl BSI 7092 E
Informations, Organisational Overview BSI Act

BSI-Kurzinformationen zu Fachthemen

In begrenzter Anzahl gegenÜbersendung eines mit 3,00 DM frankierten und adressierten Rückumschlages (C 4) erhältlich:

Fbl F 01
IT-Sicherheitsschulung

♦

Fbl F 02
Akkreditierung und Lizenzierung

♦

Fbl F 03
BSI-Sicherheitszertifikate
Was Hersteller wissen sollten

♦

Fbl F 04
Formal verifizierte Systeme mit VSE
- eine neue Dimension in der Softwareentwicklung -

♦

Fbl F 05
Das BSI-Sicherheitszertifikat
Was Bundesbehörden wissen sollten

BSI-Broschüren

In begrenzter Anzahl gegenÜbersendung eines mit 3,00 DM frankierten und adressierten Rückumschlages (C 4) erhältlich:

BSI 7148
BSI-Zertifikate
Sicherheit von IT-Produkten und -Systemen

♦

BSI 7233 - Kurzfassung
Gesamtdarstellung des BSI
IT-Sicherheit: Heute und in der Zukunft
- Der Beitrag des BSI -

♦

BSI 7233 - Langfassung
Gesamtdarstellung des BSI
IT-Sicherheit: Heute und in der Zukunft
- Der Beitrag des BSI -
Erscheint voraussichtlich Mitte 1998

♦

BSI 7233 E
IT-Security - Today and in the Future

♦

BSI 7237
Hinweise zu Planung, Bau und Betrieb von Einbruchmeldeanlagen

♦

BSI 7243
10 Sicherheits-Tips für den PC-Benutzer

BSI 7205
Tagungsband zum 4. Deutschen IT-Sicherheitskongreß 8.-11. Mai 1995

Für 85,-- DM inkl. Porto gegen schriftliche Anforderung beim BSI erhältlich.

<u>Bezugsquelle für Kurzinformationen und Broschüren:</u>
Bundesamt für Sicherheit in der Informationstechnik
- Referat I 1 -
Postfach 20 03 63
D-53133 Bonn

Tel. (0228) 9582-347
Fax: (0228) 9582-403

BSI-Schriftenreihe zur IT-Sicherheit im Bundesanzeiger-Verlag

Band 1:

Gefährdungen und Sicherheitsmaßnahmen beim Betrieb von digitalen Telekommunikationsanlagen

hrsgg. vom BSI, 1994
ISBN 3-88784-583-8 19,80 DM

In Vorbereitung:
Neuauflage, erscheint vorraussichtlich Mai 1998

♦

Band 2:

Informationen zu Computer-Viren

hrsgg. vom BSI, 1997
ISBN 3-88784-751-2 39,80 DM

♦

Band 3:

IT-Grundschutzhandbuch 1997
Maßnahmenempfehlungen für den mittleren Schutzbedarf

hrsgg. vom BSI, 1997
ISBN 3-88784-760-1 108,00 DM

In Vorbereitung:
IT-Grundschutzhandbuch 1998
Erscheint voraussichtlich Juni 1998

♦

Band 4:

Produktübersicht
Zertifizierte IT-Produkte
Zugelassene Hardware
Produkte für die materielle Sicherheit

hrsgg. vom BSI, 1994

Auflage vergriffen - kein Nachdruck.
Für weitere Informationen wenden Sie sich bitte an das BSI
oder entnehmen diese dem Internet:
http://www.bsi.bund.de

BSI-Schriftenreihe zur IT-Sicherheit im Bundesanzeiger-Verlag

Band 5:

Chipkarten im Gesundheitswesen

hrsgg. vom BSI, 1995
ISBN 3-88784-620-6 44,00 DM

♦

Band 6:

Informationstechnik zur Fahrerunterstützung im Straßenverkehr

hrsgg. vom BSI, 1995
ISBN 3-88784-621-4 39,80 DM

♦

Band 7:

Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM)

hrsgg. v.d. Europäischen Union, 1993
ISBN 3-88784-641-9 68,00 DM

♦

Band 8:

IT-Sicherheit durch infrastrukturelle Maßnahmen
hrsgg. vom BSI, 1997
ISBN-3-88784-746-6 39,80 DM

Bezugsquelle:
Bundesanzeiger-Verlag
Postfach 10 05 34
D-50445 Köln
Tel.: (0221) 20290
Fax: (0221) 2029-271

Studien zur IT-Sicherheitim Oldenbourg-Verlag

Bedrohungsmodell in KI-Systemenhrsgg. v. U. van Essen und F. Felzmann, 1991
ISBN 3-486-22122-1 48,00 DM

♦

Einführung in die Computersicherheit
hrsgg. v. Heinrich Kersten, 1991
ISBN 3-486-21873-5 48,00 DM

♦

Sicherheit des Betriebssystems VMS
hrsgg. v. U. van Essen, 1991
ISBN 3-486-22114-0 58,00 DM

♦

Sicherheitsaspekte bei der Vernetzung von Unix-Systemen
hrsgg. v. H. Kersten u. M. Weinand, 1991
ISBN 3-486-21947-2 48,00 DM

♦

Sicherheitseigenschaften der Betriebssysteme 386/ix und SCO-Unix
hrsgg. v. H. Kersten u. M. Weinand, 1991
ISBN 3-486-21942-1 48,00 DM

♦

Sicherheit unter dem Betriebssystem Unix
hrsgg. v. H. Kersten u. H. Kreutz, 1991
ISBN 3-486-21937-5 48,00 DM

♦

Sicherheitseigenschaften von Unix System V Release 4 und 4.1 ES
hrsgg. v. J.-U. Aden und M. Weinand, 1993
ISBN 3-486-22585-5 88,00 DM

Bezugsquelle:

Oldenbourg-Verlag
Rosenheimer Straße 145
D-81671 München

Tel. (089) 41120
Fax: (089) 4112-207

Veröffentlichungen im SecuMedia Verlag

Mit Sicherheit in die Informationsgesellschaft
Tagungsband 5. Deutscher IT-Sicherheitskongreß
hrsgg. vom BSI, 1997
ISBN 3-992746-29-2 96,00 DM

♦

Computersimulation
- (K)ein Spiegel der Wirklichkeit
Interdisziplinärer Diskurs Boppard III
zu querschnittlichen Fragen der IT-Sicherheit
hrsgg. vom BSI, 1994,
ISBN 3-992746-25-X 29,00 DM

♦

Patienten und ihre computergerechten Gesundheitsdaten
Interdisziplinärer Diskurs Boppard IV
zu querschnittlichen Fragen der IT-Sicherheit
hrsgg. vom BSI, 1995,
ISBN 3-922746-26-8 29,00 DM

♦

Wie gehen wir künftig mit den Risiken der Informationsgesellschaft um?
Interdisziplinärer Diskurs Boppard V
zu querschnittlichen Fragen der IT-Sicherheit
hrsgg. vom BSI, 1996,
ISBN 3-922746-27-7 29,00 DM

♦

Kulturelle Beherrschbarkeit Digitaler Signaturen
Interdisziplinärer Diskurs Boppard VI
zu querschnittlichen Fragen der IT-Sicherheit
hrsgg. vom BSI, 1997,
ISBN 3-922746-28-4 29,00 DM

Bezugsquelle:

SecuMedia Verlags GmbH
Postfach 1234
D-55205 Ingelheim

Tel. (06725) 9304-0
Fax: (06725) 5994

Sonstige Veröffentlichungen

IT-Sicherheitshandbuch
Handbuch für die sichere Anwendung der Informationstechnik

hrsgg. vom BSI, 1992

Paperback	45,00 DM
Diskettensatz	178,00 DM

Bundesdruckerei
Zweigbetrieb Bonn,
D-53175 Bonn
Tel. (0228) 382020

♦

IT-Sicherheitsbegriffe
Sammlung einheitlicher fachspezifischer Begriffe der Informationstechnik

hrsgg. v. Unterausschuß für Sicherheitsbegriffe im ISIT, 1994
- aktualisierte Loseblattausgabe -

Grundwerk	34,80 DM
Diskette	48,50 DM
Buch und Diskette	78,50 DM

Abeking-Verlag,
D-50354 Hürth-Gleuel
Tel. (02233) 35071/72

♦

Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), 1992

Bezugsquellen:

Amt für amtliche Veröffentlichungen
der Europäischen Gemeinschaften
L-2985 Luxembourg

oder

Kommission der Europäischen Gemeinschaften
Generaldirektion XIII
Rue de la Loi 200
B-1049 Brussels

BSI-FORUM in der KES

(Zeitschrift für **K**ommunikations- und **E**DV-**S**icherheit)

Das Bundesamt für Sicherheit in der Informations-technik veröffentlicht bereits seit 1992 allgemein interessierende Fachaufsätze von Mitarbeitern des Hauses und auch von Gastautoren zu Themen der IT-Sicherheit als eigenständiges BSI-Forum in der Fachzeitschrift KES.

Für 1998 sind unter anderem Beiträge zu folgen-den Themenbereichen geplant:

- ⇨ Sinn und Grenzen der Evaluierung und Zertifizierung von Systemen
- ⇨ BSI-Präsentationen auf der CeBIT 1998
- ⇨ Steganographie
- ⇨ Das Jahr-2000-Problem
- ⇨ Common Criteria/ITSEC
- ⇨ Digitale Signatur/Trustcenter
- ⇨ Java und ActiveX
- ⇨ Haltbarkeit von Datenträgern
- ⇨ Sicherheit aus Bankensicht
- ⇨ Internet-Sicherheit
- ⇨ Serie: Verbreitete Computer-Viren
- ⇨ BSI-Kopiervorlagen

Bezugsquelle:
SecuMedia Verlags GmbH
D-55205 Ingelheim
Tel. (06725) 9304-0
Fax: (06725) 5994

Informationen zur Mailbox des BSI (BSI-BOX)

Die Mailbox des Bundesamtes für Sicherheit in der Informationstechnik, kurz BSI-BOX, soll Hilfestellungen zu Fragen der Sicherheit in der Informationstechnik geben und auf schnellstem Wege auf aktuelle Gefahren und Risiken hinweisen. Der Zugang zur BSI-BOX steht allen Interessenten kostenlos zur Verfügung. Die Mailbox ist über ISDN oder analoges Modem unter (0228) 9580971 erreichbar. Das Modem (analog / ISDN) muß auf 8 Bit, No Parity, 1 Stopbit konfiguriert werden.

Bei der Nutzung von ISDN müssen Sie wie folgt vorgehen:

1) CAPI laden, Unterstützung für X75 aktivieren (V.110 ist ebenfalls möglich)
2) als Fossil-Treiber ("Modem-Emulation", setzt Hayes-kompatible Modembefehle für das CAPI um) z.B. cFos installieren: CFOS i
3) Terminalprogramm mit Int-14 Unterstützung, wie z.B. TELIX - int-14 aufrufen:

   Modem-Initialisierungsstring (ELINK323):

   ATB4E1X4V1S0=0S10=0

   B4 legt bei einem ELINK323-Modem als Protokoll den X75-Modus (64 kBit, synchron) fest.

Der BSI-BOX-Anschluß kann mit ATDP02289580971 erreicht werden.

Nach erfolgreicher Anmeldung gelangt der BSI-BOX-Leser in das Hauptmenü.

Online-Hilfen werden unter den Menüpunkten "[G]enerelle Hilfe" und "[A]lle Befehle" angeboten.

Mittels des Menüpunktes "Wichtige Nachricht" kann sich der BSI-BOX-Leser über die neuesten Änderungen informieren. Der aktive Bereich kann mit Hilfe des Menü-punktes "[B]ereich wechseln" und der Angabe der Bereichsnummer gewählt werden.

Ausschließlich Dateien mit der Dateikennung TXT können mit Hilfe des Menüpunktes "[T]ype" direkt am Bildschirm im Klartext gelesen werden.

Dateien mit der Kennung ZIP sind gepackte Dateien. Diese können nicht direkt gelesen werden, sondern müssen zunächst auf den lokalen Rechner übertragen ("[D]ownload") und dort entpackt werden.

Mit Hilfe des Menüpunktes "[D]ownload" können alle gewünschten Dateien auf den lokalen Rechner übertragen werden.

Zum Packen und Entpacken von Dateien steht im Bereich Allgemeines das Shareware-Produkt PKZIP Version 2.04 (pkz204e.exe) zur Verfügung.

Neben diesem Shareware-Produkt stehen in diesem Be-reich noch weitere Programme zur Verfügung, welche die Kommunikation mit der BSI-BOX unterstützen. Vor Nutzung dieser Programme sind die entsprechenden Lizenzbedingungen zu beachten.

Weitere Informationen:

Bundesamt für Sicherheit
in der Informationstechnik
Referat V 5
Postfach 20 03 63
D-53133 Bonn

Tel.: (0228) 9582-301
Fax: (0228) 9582-427

Im einzelnen sind zur Zeit folgende Bereiche eingestellt:

1. Allgemeines

Hier finden Sie die Hinweise und Hilfestellungen zur Bedienung der BSI-BOX. In diesem Bereich ist die Gesamtliste aller Dateien (GLISTE.TXT) der BSI-BOX abgelegt. Einige nützliche Shareware-Programme, wie z.B. PKZIP (pkz204e.exe) zum Packen und Entpacken der Dateien, sind hier ebenfalls zu finden.

2. Anti-Virus: Allgemeines

In diesem BSI-BOX Bereich werden allgemeine Informationen zum Thema Computer-Viren bereitgestellt. Außerdem stehen hier einige hilfreiche Utility-Programme zur Verfügung. Die hier eingestellten Programme sind teilweise vom BSI, teilweise jedoch auch aus fremder Quelle. Das BSI stellt diese Programme ohne Wertung zur allgemeinen Verfügung, übernimmt jedoch keine Garantie für deren korrekte Funktion.

3. Anti-Virus: Digest (Unterbereich zu Anti-Virus)

In diesen BSI-BOX-Bereich werden die Artikel aus "VIRUS-L Digest" eingestellt. "VIRUS-L Digest" ist die Zusammenfassung der Artikel aus der Newsgroup "comp.virus". Newsgroups sind Diskussionsforen zu allen möglichen Fachgebieten und werden als Netzdienst im Internet angeboten. VIRUS-L Digest / comp. Virus ist eine moderierte Newsgroup, d.h. neue Artikel in dieser Gruppe werden vom Moderator gelesen, bevor sie in die Gruppe eingestellt werden. Der Moderator hält so die Informationsqualität dieser Gruppe auf einem hohen Niveau. Das Referat V 2 des BSI stellt den VIRUS-L Digest - nach Absprache mit dem Moderator - kommentarlos in diesen BSI-BOX-Bereich, damit auch Benutzern ohne entsprechenden Internet-Zugang diese Informationsquelle zur Verfügung steht. Für den Inhalt der Artikel ist der jeweilige Autor und nicht das BSI verantwortlich.

4. Anti-Virus: FAV (Unterbereich zu Anti-Virus)

In diesen BSI-BOX-bereich werden Beschreibungen und Hinweise zu "Frequently Asked Viruses (FAV)" eingestellt. Die Beschreibungen kommen in der Regel aus eigenen Analysen des entsprechenden Virus und geben Auskunft über Art, Funktionsweise, Schadensfunktion und Entfernung des Virus. Die Beschreibungen stehen in deutsch (*.TXT) und englisch (*.DOC) zur Verfügung. Außerdem werden in diesen Bereich aktuelle Hinweise zu Computer-Viren eingestellt.

5. Anti-Virus: Shareware (Unterbereich zu Anti-Virus)

In diesem Bereich werden Anti-Viren-Shareware-Programme eingestellt. Diese Programme dürfen im privaten Bereich eingesetzt werde. Die Lizenzbedingungen der Programme sind zu beachten. Fragen sind an den jeweiligen Hersteller zu richten. Das BSI stellt diese Programme ohne Wertung zu allgemeinen Verfügung und übernimmt keinerlei Gewähr für deren korrekte Funktionsweise.

6. Beratung

Hier findet der Nutzer der BSI-BOX eine Beschreibung der Organisation der Abteilung VI "Beratung und Unterstützung" mit den Angaben zum Spektrum der Dienstleistungen: Grundlagenentwicklung, Schulung, begleitende Beratung, individuelle Sicherheitsanalysen und Informationsdienst. Es werden Aussagen zum Anspruch auf die Beratungsfleistungen gegeben, und neben der Beschreibung, wie auf welchen Weg ein Beratungsersuchen an das BSI zu stellen ist, werden Hinweise auf die BSI-Kostenverordnung gegeben.

7. BSI: wir über uns

Kurzbeschreibung der gesetzlichen Grundlagen für das BSI, Organigramm des Hauses und detaillierte Vorstellung der einzelnen Abteilungen.

8. Sicherheitskriterien

In diesem Bereich stehen die Kriterien zur Bewertung der Sicherheit von Systemen der Informationstechnik und Veröffentlichungen in deren Umfeld sowie Diskussionsbeiträge hierzu zur Verfügung. Ferner werden Informationen über die aktuelle Entwicklung in diesem Bereich gegeben.

9. Systemsicherheit: Allgemeines

Dieser Bereich und seine Unterbereiche enthalten Informationen und Hilfen zur Systemsicherheit in Form von Literaturangaben, Empfehlungen, Notfallhilfen und Programmen. Sie bein-

halten Beiträge zu den Themen Betriebssysteme (DOS, Unix, LAN, WAN, etc.), Folgen und Nebenfolgen, alternative Sicherheitsphilosophien, Abstrahlsicherheit sowie organisatorische und materielle Sicherheit. Durch das BSI herausgegebene Beiträge sind als solche gekennzeichnet. Beiträge die nicht auf diese Art gekennzeichnet sind, wurden unkommentiert in diesen Bereich kopiert. Hierdurch soll dem Benutzer eine zusätzliche Hilfe gegeben, aber keine explizite Empfehlung durch das BSI ausgesprochen werden. Für den Inhalt der Artikel bzw. die Funktionalität der Programme ist der jeweilige Autor und nicht das BSI verantwortlich.

10. Systemsicherheit: CERT

(Unterbereich zu Systemsicherheit)

Dieser Bereich enthält Veröffentlichungen des CERT "Computer Emergency Response Team". Hier werden Warnungen, Hinweise und Empfehlungen zu entdeckten Sicherheitslücken verschiedener Systeme erläutert. Die Beiträge werden unkommentiert in diesen Bereich kopiert. Für den Inhalt der Artikel ist der jeweilige Autor und nicht das BSI verantwortlich.

11. Systemsicherheit: UNIX

(Unterbereich zu Systemsicherheit)

Dieser Bereich enthält Informationen und Porgramme zur Systemsicherheit in UNIX-Systemen und -Netzwerken. Durch das BSI herausgegebene Beiträge sind als solche gekennzeichnet. Beiträge die nicht auf diese Art gekennzeichnet sind, wurden unkommentiert ind iesen Bereich kopiert. Hierdurch soll dem Benutzer eine zusätzliche Hilfe gegeben, aber keine explizite Empfehlung durch das BSI ausgesprochen werden. Für den Inhalt der Artikel bzw. die Funktionalität der Programme ist der jeweilige Autor und nicht das BSI verantwortlich.

12. Veranstaltungen/Schulungen

Hinweise auf Kongresse, Workshops und sonstige Veranstaltungen des BSI (BSI-Kongreß, Boppard usw.) bzw. mit Beteiligung des BSI (CeBIT, SiTech, Online, internationale Sicherheitskongresse usw.) sowie auf Schulungen und Workshops im Rahmen der Beratung.

13. Veröffentlichungen: BSI

Hauseigene Veröffentlichungen (ggf. in Form von Hinweisen/Zusammenfassungen); Veröffentlichungen zur Beratungstätigkeit, der Zertifizierung / Akkreditierung , Virus-Meldung, allgemeine Pressemitteilungen des BSI, BSI-Forum ind er KES, laufende Beiträge des BSI.

14. Zertifizierung/Akkreditierung

Darstellung des Verfahrens der Zertifizierung sowie Listen/Zertifikate der zertifizierten Produkte, (BSI und international).

Darstellung der Grundlagen und des Verfahrens der Akkreditierung.

DER BUNDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ

Empfehlungen zur Paßwortgestaltung und zum Sicherheitsmanagement

I. Paßwortregeln

Grundsatz: "Für den Benutzer leicht zu merken, für einen Fremden schwer zu erraten."

1. Nirgends notieren! Niemandem mitteilen!
2. Nur dem Benutzer bekannt.
3. Mindestlänge: 6 Stellen
4. Vor- und Familiennamen nie allein verwenden, sondern:
5. Stets alphanumerisch gestalten (Buchstaben und Zahlen/Zeichen).
6. Keine Trivialpaßwörter (z. B. 4711. 12345 oder andere nebeneinander liegendeTasten. gast usw.) verwenden; möglichst vom System automatisch abweisen lassen.
7. In angemessenen Zeitabständen (möglichst automatisch gesteuert) ändern: nicht zu oft!
8. Automatisch verhindern, daß (aus Bequemlichkeit) als neues wieder das alte Paßwort gewählt wird.
9. Für besonders wichtige Funktionen/sensible Daten: Zusatzpaßwort ("4-Augen-Prinzip"). Oder: Zwei Personen kennen je das halbe Paßwort.
10. Paßwort des Systemverwalters - nur ihm bekannt - für Vertretungsfall versiegelt aufbewahren.

II. Sicherheitsmanagement

1. Jede Person erhält eine eigene Benutzerkennung ("User"). Benutzerkennung werden grundsätzlich nur für Bedienstete der Stelle eingerichtet: für Fremde (Wartung usw.) nur zur kontrollierten Inanspruchnahme.
2. Benutzerkennungen werden nur für den Zeitraum eingerichtet, in dem sie tatsächlich benötigt werden.
3. Die Datei der Paßwörter und Benutzerkennungen sind besonders zu schützen, i. d. R. durch kryptographische Verschlüsselung.
4. Automatische Begrenzung der Anzahl der Anmeldungs-Fehlversuche (maximal drei, danach: Sperrung der Benutzerkennung)
5. Protokollierung der Fehlversuche und Information des Systemverwalters und/ oder Benutzers.
6. Anzeige der letzten korrekten Anmeldung zur Kontrolle durch Berechtigten (Tag, Uhrzeit, Terminal usw.)
7. Zeitliche Begrenzung der Zugangsberechtigung, z. B. auf die Bürozeit.
8. Verhindern, daß Anmeldung mit Funktionstaste möglich ("auto-log-in").
9. Automatisches Sperren oder Abmelden des Terminals/APC nach längerer Nichtbenutzung, z. B. nach 5 Minuten.
10. Bei Verbindung des Systems mit dem öffentlichen Wählnetz: Zusätzliche Sicherungsmaßnahmen (Rückrufautomatik usw.)

FAX MIT RISIKO

Eine Telefaxübertragung kann einen Eingriff in das Persönlichkeitsrecht bedeuten. So hat das Oberlandesgericht Nürnberg in einem Urteil (Az.: 1 0 2547/91) entschieden, daß die Übermittlung per Firmenfax eines Anwaltschreibens, das persönliche Angelegenheiten zum Inhalt hat, einen erheblichen Eingriff in das Persönlichkeitsrecht des Betroffenen darstellt und damit unzulässig ist. Begründung: Es bestehe die Gefahr, daß der Inhalt Personen zugänglich wird, für die er nicht bestimmt ist.
Um die entsprechende Sicherheit zu gewährleisten, hat der Landesbeauftragte für Datenschutz Rheinland-Pfalz einen Leitfaden (s. u.) für den Arbeitsplatz "Datenschutz bei Telefaxgeräten" entwickelt.

LEITFADEN

1. Sie tragen die Verantwortung für die durch Sie übermittelten personenbezogenen Daten. Prüfen sie daher genau deren Sensibilität und entscheiden Sie dann, ob und wie gefaxt werden kann.
2. Beachten Sie die für Ihre Behörde/Dienststelle geltenden Anweisungen für die Nutzung des Telefax-Dienstes.
3. Nutzen Sie nach Möglichkeit alle der Sicherheit dienenden Einrichtungen des Gerätes, insbesondere die Anzeige des erreichten Gerätes.
4. Vergewissern Sie sich vor einer Sendung, ob der Adressat noch unter der Ihnen bekannten Anschlußnummer erreichbar ist.
5. Verständigen Sie sich vor der Absendung besonders sensibler Daten mit dem Adressaten über den konkreten Zeitpunkt der Übermittlung.
6. Gewährleisten Sie - möglichst durch persönliche Anwesenheit am Gerät - während der Übertragung von Dokumenten mit personenbezogenen Daten, daß kein Unbefugter in diese Einsicht nehmen kann.
7. Verständigen Sie sich nach erfolgter Sendung über aufgetretene Mängel und gegebenenfalls deren Behebung.
8. Erleichtern Sie sich und den Empfängern die Nachweisführung:
   - Vorblatt der Behörde/Dienststelle benutzen
   - Kopienblätter numerieren, - bei dafür geeigneten Geräten:
   Originale mit Verifikationsstempel versehen, Protokolle
   sorgfältig und sicher aufbewahren.
9. Faxübertragungen sind "abhörbar". Was am Telefon nicht gesagt werden darf, darf auch nicht gefaxt werden.
10. Beachten Sie bei der Nutzung von Fernkopien auf PC-Basis (z.B. Fax-Karten) auch die damit verbundenen Risiken. Verständigen Sie sich darüber hinaus mit Ihrem Datenschutzbeauftragten.

8.1.6 Innenministerium Baden-Württemberg (IM BW)

"Leitfaden zur PC-Sicherheit für die Landesverwaltung Baden-Württemberg" (Stand: 23.08.94), herausgegeben von der Stabsstelle Verwaltungsstruktur, Information und Kommunikation beim IM BW (SIK), jetzt Stabsstelle für Verwaltungsreform (StaV), Dorotheenstraße 6, 70173 Stuttgart

8.1.7 Zitierte Fachpresse

"Funkschau" Fachzeitschrift für elektronische Kommunikation, DMV Franzis-Verlag, Dernacher Str. 3 d, 85622 Feldkirchen

"KES" Zeitschrift für Kommunikations- und EDV-Sicherheit, SecuMedia Verlags GmbH, Gaulsheimerstr. 17, Postfach 1234, 55 205 Ingelheim.

"Sicherheitsberater" Informationsdienst zu Problemen der Sicherheit in Betrieb, Unternehmen und Verwaltung (ISB), Verlagsgruppe Handelsblatt GmbH, Postfach 10 11 02, 40 002 Düsseldorf.

8.2 Gesetze und Vorschriften

Gesetz über den Verfassungsschutz in Baden-Württemberg (Landesverfassungsschutzgesetz - LVSG) v. 22. Oktober 1991

Gesetz zum Schutz personenbezogener Daten (Landesdatenschutzgesetz - LDSG) v. 27. Mai 1991

Gesetz über die Sicherheitsüberprüfung aus Gründen des Geheimschutzes (Landessicherheitsüberprüfungsgesetz - LSÜG) v. 12. Februar 1996

Gesetz über die Errichtung des Bundesamtes für die Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz - BSIG) v. 17. Dezember 1990

2. Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. Wirtschaftskriminalitätsgesetz - 2. WiKG) v. 15. Mai 1986

Gesetz gegen den unlauteren Wettbewerb (UWG) v. 15. Mai 1986, insb. § 17 Abs. 2

Urheberrechtsgesetz (UrhG) v. 24. Juni 1993, insb. Teil 1, 8. Abschnitt

Betriebsverfassungsgesetz, insb. § 87 Abs. 1, Ziffer 6, §§ 90, 91

Arbeitsstättenverordnung (ArbStättVO) v. 1. August 1988

Gerätesicherheitsgesetz v. 18. Februar 1986, insb. GS-Zeichen

Gesetz über die Haftung für fehlerhafte Produkte (Produkthaftungsgesetz - ProdHaftG) v. 1. Januar 1990

Fernmeldeanlagengesetz (FAG) v. 3. Juli 1989, zuletzt geändert durch § 99 Telekommunikationsgesetz (TKG)

Fernmeldeanlagenüberwachungsverordnung (FÜVO) v. 1. Mai 1995

Telekommunikationsgesetz (TKG) vom 25. Juli 1996

Telekommunikationsdatenschutzverordnung (TDSVO) - derzeit im Gesetzgebungsverfahren

Gesetz über die elektromagnetische Verträglichkeit (EMV-G) v. 9. November 1992

Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zu Artikel 10 Grundgesetz/GG - G10-Gesetz -) v. 13.08.1968 sowie die Entscheidung des Bundesverfassungsgerichts hierzu v. 11. Januar 1995

Verbrechensbekämpfungsgesetz v. 28. Oktober 1994

Strafgesetzbuch (StGB), insb. §§ 93 - 99, 202a, 263a, 269, 270, 303a, 303b.

Zusätzlich können bestimmte Bestimmungen des Umwelthaftungsgesetzes und des Abfallgesetzes bei der Entsorgung von IT-Geräten und Datenträgern, das Handelsgesetzbuch -HGB- (§§ 238 Abs. 1 und 240 Abs. 1 bei Buchführungspflicht und Inventur) für Revision und Bilanz, die Abgabenordnung -AO- (§ 146 Abs. 1) für die Grundsätze ordnungsgemäßer Buch- und Speicherbuchführung, sowie die allgemeinen Bestimmungen des Bürgerlichen Gesetzbuches -BGB- für das IT-Recht eine Rolle spielen.

IT-Richtlinien für die Bundesverwaltung v. 18. August 1988

Verschlußsachenanweisung (VS-Anweisung/VSA) für Baden-Württemberg v. 20. Dezember 1982 sowie die sie ergänzenden Richtlinien (§ 64 VSA); die VSA und die ergänzenden Richtlinien werden derzeit neu gefaßt !

8.3 Normen, Normungsgremien und Standards

Bundesrepublik Deutschland:

BAPT	Bundesamt für Post und Telekommunikation
DATech	Deutsche Akkreditierungsstelle Technik
DEKITZ	Deutsche Normungsstelle für IT-Konformitätsprüfung und -zertifizierung
DIN	Deutsches Institut für Normung
DIN-CERTCO	Gesellschaft für Konformitätsbewertung Berlin
DKE	Deutsche Elektrotechnische Kommission
FuP	Forschungs- und Prüfgemeinschaft Geldschränke und Tresoranlagen
FTZ	Forschungs- und Technologiezentrum der Telekom
RAL	Reichsausschuß für Lieferbedingungen
VDE	Verband Deutscher Elektroingenieure
VDMA	Verband Deutscher Maschinen- und Anlagenbau
VdS	Verband der Schadensversicherer e.V.
ZVEI	Zentralverband Elektrotechnik- und Elektronikindustrie

Europa:

CEN	Comité Européen de Normalisation
CENELEC	Comité Européen de Normalisation Eléctrotechnique
ETSI	European Telecommunications Standards Institute
ECMA	European Computer Manufacturers Association

International:

ANSI	American National Standard Institute
CCITT	Comité Consultarif International Télégraphique et Téléphonique
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
ISO	International Standards Organisation
JTC1	Joint Technical Committee One - gem. technisches Komitee von IEC und ISO, das seine IT-Normen mit dem CCITT abstimmt

Brandschutz

- VdS-Richtlinien

- VDMA-Einheitsblatt 24 991, Teile 1 und 2 i.V. m. RAL-RG 626/7 und /8: Prüfbedingungen für das Brandverhalten von Räumen und Schränken zur Aufbewahrung von Datenträgern sowie für Stahlschränken und sonstigen Behältern

- DIN 4102: Brandverhalten von Baustoffen und Bauteilen

- DIN 10 801: Stahltüren T90

- DIN 18 082: Stahltüren T30

- DIN 18 384: Blitzschutzanlagen bei Gebäuden

- DIN 14 675: Brandmeldeanlagen

- VDE 0800 und 0833: Brandmeldeanlagen

Schutz der Stromversorgung

- DIN 57 675: Grobschutz gegen Überspannung

- VDE 0675: Grobschutz gegen Überspannung

- VDE 0100: Standards bei Leuchten, Starkstromanlagen

- VDE 0631: Standards bei Leuchtstofflampen

- VDE 0510: Unabhängige Stromversorgung durch Akkumulatoren und Batterien

- EN 50 173: Schutz gegen Überspannung

Schutz vor Sabotage, Vandalismus und Diebstahl

- VdS-Richtlinien, z.B. Form in VdS 3007

- Technische Anforderungen des Landesamtes für Verfassungsschutz (vgl. Druckschriftenverzeichnis)

- Liste geprüfter Produkte der Kommission vorbeugende Kriminalitätsbekämpfung (KVK)

- RAL-RG 625/4: Wertschutzraum und Wertschutzraumtür

- RAL-RG 626/7 und /9: (Datensicherungs-) Schränke

- DIN VDE 0833: Gefahrenmeldeanlagen
- DIN V 18 054: Einbruchhemmende Fenster

- DIN V 18 103: Einbruchhemmende Türen

- DIN 52 290: Verglasungen

- DIN V 18 254: Profilzylinder

- DIN 18 257: Schutzbeschläge

- VdS 2156 und 2157: Profilzylinder

- VDMA-Einheitsblatt 24 991, Teil 1 i.V.m. RAL-RG 626/2, /9, /10, 621/10 und /20: Prüfbedingungen für Stahlschränke und sonstige Behälter

- DIN 32 757: Vernichten von Informationsträgern

- DIN 33 858: Löschen von magnetischen Datenträgern

IT-Evaluation (Prüfung und Zertifizierung)

- IT-Sicherheitskriterien (ITS)

- IT-Security Evaluation Criteria (ITSEC)

- Common Criteria (CC)

- Auf die Darstellung der vielen international gültigen Normen und Standards nach ANSI, CCITT, IEEE und ISO wird verzichtet.