Diplomarbeit

Universität Hamburg
Fachbereich Informatik
Arbeitsbereich AGN
(Anwendungen der Informatik in Geistes- und Naturwissenschaften)

Ein IT-Sicherheitskonzept für eine wissenschaftliche Einrichtung

am Beispiel des Fachbereichs Informatik der Universität Hamburg

Teil III
Erläuterungen

Jens Nedon
Fibigerstraße 275
22419 Hamburg

Betreuer:
Prof. Dr. Klaus Brunnstein
Dr. Hans-Joachim Mück

Hamburg
30. September 1999

Inhaltsverzeichnis

Anhang G

Gefährdungskatalog nach dem BSI-Grundschutzhandbuch

Quellenangabe:
Auszug aus dem BSI - IT-Grundschutzhandbuch 1998 [BSI1998].
Im IT-Grundschutzhandbuch sind zu den Beschreibungen der Gefährdungen oftmals Beispiele angegeben; diese sind aus Platzgründen hier weggelassen worden. Für eine vertiefte Betrachtung wird auf die Quelle verwiesen.

G.1 Gefährdungskatalog Höhere Gewalt

G 1.1 Personalausfall
Durch Krankheit, Unfall, Tod oder Streik kann ein nicht vorhersehbarer Personalausfall entstehen. Desweiteren ist auch der Personalausfall bei einer regulären Beendigung des Arbeitsverhältnisses zu berücksichtigen, insbesondere wenn die Restarbeitszeit z. B. durch einen Urlaubsanspruch verkürzt wird.
In allen Fällen kann die Konsequenz sein, daß entscheidende Aufgaben aufgrund des Personalausfalls im IT-Einsatz nicht mehr wahrgenommen werden. Dies ist besonders dann kritisch, wenn die betroffene Person im IT-Bereich eine Schlüsselstellung einnimmt und aufgrund fehlenden Fachwissens anderer nicht ersetzt werden kann. Störungen des IT-Betriebs können die Folge sein.

G 1.2 Ausfall des IT-Systems
Der Ausfall einer Komponente eines IT-Systems kann zu einem Ausfall des gesamten IT-Betriebs führen. Insbesondere zentrale Komponenten eines IT-Systems sind geeignet, solche Ausfälle herbeizuführen, z. B. Klima- und Stromversorgung, LAN-Server, Datenfernübertragungseinrichtung.
Technisches Versagen (z. B. G 4.1 Ausfall der Stromversorgung) muß nicht zwingend als Ursache für den Ausfall eines IT-Systems angenommen werden. Ausfälle lassen sich auch oft auf menschliches Fehlverhalten (z. B. G 3.2 Fahrlässige Zerstörung von Gerät oder Daten) oder vorsätzliche Handlungen (z. B. G 5.4 Diebstahl) zurückführen. Es treten auch Schäden aufgrund

höherer Gewalt (z. B. Feuer, Blitzschlag, Chemieunfall) ein, allerdings sind diese Schäden meist um ein Vielfaches höher.
Werden auf einem IT-System zeitkritische IT-Anwendungen betrieben, sind die Folgeschäden nach Systemausfall entsprechend hoch, wenn es keine Ausweichmöglichkeiten gibt.

G 1.3 Blitz
Der Blitz ist die wesentliche während eines Gewitters bestehende Gefährdung für ein Gebäude und die darin befindliche Informationstechnik. Blitze erreichen bei Spannungen von mehreren 100.000 Volt Ströme bis zu 200.000 Ampere. Diese enorme elektrische Energie wird innerhalb von 50-100 Fehler! Textmarke nicht definiert.s freigesetzt und abgebaut. Ein Blitz mit diesen Werten, der in einem Abstand von ca. 2 km einschlägt, verursacht auf elektrischen Leitungen im Gebäude immer noch Spannungsspitzen, die zur Zerstörung empfindlicher elektronischer Geräte führen können. Diese indirekten Schäden nehmen mit abnehmender Entfernung zu.
Schlägt der Blitz direkt in ein Gebäude ein, werden durch die dynamische Energie des Blitzes Schäden hervorgerufen. Dies können Beschädigungen des Baukörpers (Dach und Fassade), Schäden durch auftretende Brände oder Überspannungsschäden an elektrischen Geräten sein.
Über das regional unterschiedliche Blitzschlagrisiko erteilt der Deutsche Wetterdienst entsprechende Auskünfte.

G 1.4 Feuer
Neben direkten durch das Feuer verursachten Schäden an einem Gebäude oder dessen Einrichtung lassen sich Folgeschäden aufzeigen, die insbesondere für die Informationstechnik in ihrer Schadenswirkung ein katastrophales Ausmaß erreichen können. Löschwasserschäden treten beispielsweise nicht nur an der Brandstelle auf. Sie können auch in tiefer liegenden Gebäudeteilen entstehen. Bei der Verbrennung von PVC entstehen Chlorgase, die zusammen mit der Luftfeuchtigkeit und dem Löschwasser Salzsäure bilden. Werden die Salzsäuredämpfe über die Klimaanlage verteilt, können auf diese Weise Schäden an empfindlichen elektronischen Geräten entstehen, die in einem vom Brandort weit entfernten Teil des Gebäudes stehen.
Ein Brand entsteht nicht nur durch den fahrlässigen Umgang mit Feuer (z.B. Adventskranz, Schweiß- und Lötarbeiten), sondern auch durch unsachgemäße Benutzung elektrischer Einrichtungen (z.B. unbeaufsichtigte Kaffeemaschine, Überlastung von Mehrfachsteckdosen).
Die Ausbreitung eines Brandes kann unter anderem begünstigt werden durch:

- Aufhalten von Brandabschnittstüren durch Keile,
- Unsachgemäße Lagerung brennbarer Materialien,
- Fehlen von Brandmeldeeinrichtungen,
- mangelhaft vorbeugenden Brandschutz (z.B. Fehlen von Brandabschottungen auf Kabeltrassen).

G 1.5 Wasser
Der unkontrollierte Eintritt von Wasser in Gebäuden oder Räumen kann bspw. bedingt sein durch:

- Regen, Hochwasser, Überschwemmung,
- Störungen in der Wasser-Versorgung oder Abwasser-Entsorgung,
- Defekte der Heizungsanlage,
- Defekte an Klimaanlagen mit Wasseranschluß,
- Defekte in Sprinkleranlagen und
- Löschwasser bei der Brandbekämpfung.

Unabhängig davon, auf welche Weise Wasser in Gebäude oder Räume gelangt, besteht die Gefahr, daß Versorgungseinrichtungen oder IT-Komponenten beschädigt oder außer Betrieb gesetzt werden (Kurzschluß, mechanische Beschädigung, Rost etc.). Durch die Unterbringung zentraler Einrichtungen der Gebäudeversorgung (Hauptverteiler für Strom, Telefon, Daten) in Kellerräumen ohne selbsttätige Entwässerung, kann eindringendes Wasser sehr hohe Schäden verursachen.

G 1.6 Kabelbrand
Wenn ein Kabel in Brand gerät, sei es durch Selbstentzündung oder durch Beflammung, hat dies verschiedene Folgen:

- Die Verbindung kann unterbrochen werden.
- Es können sich aggressive Gase entwickeln.
- An Kabeln, deren Isolationsmaterial nicht flammwidrig bzw. selbstverlöschend ist, kann sich ein Feuer ausbreiten. Selbst Brandabschottungen verhindern dies nicht vollständig, sie verzögern die Ausbreitung.
- Bei dicht gepackten Trassen kann es zu Schwelbränden kommen, die über längere Zeit unentdeckt bleiben und so zur Ausbreitung des Feuers führen, lange bevor es offen ausbricht.

G 1.7 Unzulässige Temperatur und Luftfeuchte
Jedes Gerät hat einen Temperaturbereich, innerhalb dessen seine ordnungsgemäße Funktion gewährleistet ist. Überschreitet die Raumtemperatur die Grenzen dieses Bereiches nach oben oder unten, kann es zu Betriebsstörungen und zu Geräteausfällen kommen.
So wird z.B. in einem Serverraum durch die darin befindlichen Geräte elektrische Energie in Wärme umgesetzt und daher der Raum aufgeheizt. Bei unzureichender Lüftung kann die zulässige Betriebstemperatur der Geräte überschritten werden. Bei Sonneneinstrahlung in den Raum sind Temperaturen über 50C nicht unwahrscheinlich.
Zu Lüftungszwecken werden oft die Fenster des Serverraumes geöffnet. In der Übergangszeit (Frühjahr, Herbst) kann das bei großen Temperaturschwankungen dazu führen, daß durch starke Abkühlung die zulässige Luftfeuchte überschritten wird.

G 1.8 Staub, Verschmutzung
Trotz zunehmender Elektronik in der IT kommt sie noch nicht ohne mechanisch arbeitende Komponenten aus. Zu nennen sind Disketten, Fest- und Wechselplatten, Diskettenlaufwerke, Drucker, Scanner etc. Mit steigenden Anforderungen an die Qualität und die Schnelligkeit müssen diese Geräte immer präziser arbeiten. Bereits geringfügige Verunreinigungen können zu einer Störung eines Gerätes führen. Vorhandene Sicherheitsschaltungen in den Geräten führen meist zu einem rechtzeitigen Abschalten. Das hält zwar den Schaden, die Instandsetzungskosten und die Ausfallzeiten klein, führt aber dazu, daß das betroffene Gerät nicht verfügbar ist.

G 1.10 Ausfall eines Weitverkehrsnetzes
Werden auf IT-Systemen, die über Weitverkehrsnetze verbunden sind, zeitkritische IT-Anwendungen betrieben, sind die durch einen Netzausfall möglichen Schäden und Folgeschäden entsprechend hoch, wenn keine Ausweichmöglichkeiten (z. B. Anbindung an ein zweites Kommunikationsnetz) vorgesehen sind.
Im Rahmen der Liberalisierung des Telekommunikationsmarktes bietet nicht nur die Deutsche Telekom AG ihre Dienste für die Bereitstellung von Kommunikationsverbindungen zum Daten- und Sprachtransfer an. Viele, teilweise sehr kleine Netzbetreiber, konkurrieren mit günstigen Kommunikationsentgelten untereinander und mit der Deutschen Telekom AG. Daher sollte ein Kunde sich informieren, mit welcher Güte dieser Dienst tatsächlich erbracht werden kann, indem er den Netzbetreiber um detaillierte Auskünfte über Backup-Strategien oder Notfallplanungen bittet.

G.2 Gefährdungskatalog Organisatorische Mängel

G 2.1 Fehlende oder unzureichende Regelungen
Die Bedeutung übergreifender organisatorischer Regelungen und Vorgaben für das Ziel IT-Sicherheit nimmt mit dem Umfang der Informationsverarbeitung, aber auch mit dem Schutzbedarf der zu verarbeitenden Informationen zu.
Von der Frage der Zuständigkeiten angefangen bis hin zur Verteilung von Kontrollaufgaben kann das Spektrum der Regelungen sehr umfangreich sein. Auswirkungen von fehlenden oder unzureichenden Regelungen werden beispielhaft in den Gefährdungen G 2.2 ff. beschrieben.

G 2.2 Unzureichende Kenntnis über Regelungen
Die Festlegung von Regelungen allein sichert den störungsfreien IT-Einsatz noch nicht. Die für einen Funktionsträger geltenden Regelungen müssen diesem auch bekannt sein. Der Schaden, der sich aus einer unzureichenden Kenntnis über bestehende Regelungen ergeben kann, darf sich nicht mit den Aussagen entschuldigen lassen: „Ich habe nicht gewußt, daß ich dafür zuständig bin.“ oder „Ich habe nicht gewußt, wie ich zu verfahren hatte.“

G 2.3 Fehlende, ungeeignete, inkompatible Betriebsmittel
Eine nicht ausreichende Bereitstellung von Betriebsmitteln kann einen IT-Betrieb erheblich beeinträchtigen. Störungen können sich aus einer nicht ausreichenden Menge benötigter Betriebs-

mittel oder deren nicht termingerechter Bereitstellung ergeben. Ebenso kann es vorkommen, daß ungeeignete oder sogar inkompatible Betriebsmittel beschafft werden, die infolgedessen nicht eingesetzt werden können.

G 2.4 Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
Nach der Einführung von IT-Sicherheitsmaßnahmen (z. B. Datensicherung) obliegt es vielfach den Benutzern, sie konsequent umzusetzen. Finden keine oder nur unzureichende Kontrollen der IT-Sicherheitsmaßnahmen statt, wird weder deren Mißachtung noch ihre effektive Wirksamkeit festgestellt. Eine rechtzeitige Reaktion wird dadurch verhindert.
Darüber hinaus gibt es IT-Sicherheitsmaßnahmen, die nur mit der Durchführung entsprechender Kontrollen ihre Wirkung entfalten. Hierzu zählen beispielsweise Protokollierungsfunktionen, deren Sicherheitseigenschaften erst mit der Auswertung der Protokolldaten zum Tragen kommen.

G 2.5 Fehlende oder unzureichende Wartung
Die Funktionsfähigkeit der eingesetzten Technik muß gewährleistet bleiben. Durch regelmäßige Wartung kann die Funktionsfähigkeit der eingesetzten Technik gefördert werden. Werden Wartungsarbeiten nicht oder nur unzureichend durchgeführt, können daraus unabsehbar hohe Schäden oder Folgeschäden entstehen.

G 2.6 Unbefugter Zutritt zu schutzbedürftigen Räumen
Gelangen Unbefugte in schutzbedürftige Räume, können sich Gefährdungen nicht nur durch vorsätzliche Handlungen, sondern auch durch unbeabsichtigtes Fehlverhalten ergeben. Eine Störung des Betriebsablaufs tritt allein schon dadurch ein, daß aufgrund des unbefugten Zutritts eine Feststellung möglicher Schäden erforderlich wird. Dabei ist zu beachten, daß auch dienstlich genutzte Räume im häuslichen Umfeld zu diesen schutzbedürftigen Räumen zu zählen sind.

G 2.7 Unerlaubte Ausübung von Rechten
Rechte wie Zutritts-, Zugangs- und Zugriffsberechtigungen werden als organisatorische Maßnahmen eingesetzt, um eine sichere und ordnungsgemäße IT-Nutzung zu gewährleisten. Werden solche Rechte an die falsche Person vergeben oder wird ein Recht unautorisiert ausgeübt, können sich eine Vielzahl von Gefährdungen ergeben, die die Vertraulichkeit und Integrität von Daten oder die Verfügbarkeit von Rechnerleistung beeinträchtigen.

G 2.8 Unkontrollierter Einsatz von Betriebsmitteln
Betriebsmittel - gleich welcher Art - dürfen nur entsprechend dem Verwendungszweck eingesetzt werden. Die für die Beschaffung und den Einsatz der Betriebsmittel verantwortlichen Personen müssen sowohl den unkontrollierten Einsatz verhindern als auch den korrekten Einsatz überwachen. Wird jedoch der Einsatz von Betriebsmitteln nicht ausreichend kontrolliert, können als Folge vielfältige Gefährdungen auftreten.

G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
Die speziell für den Einsatz von Informationstechnik geschaffenen organisatorischen Regelungen, aber auch das gesamte Umfeld einer Behörde bzw. eines Unternehmens unterliegen stän-

digen Veränderungen. Sei es nur, daß Mitarbeiter ausscheiden oder hinzukommen, Mitarbeiter das Büro wechseln, neue Hardware oder Software beschafft wird, der Zulieferbetrieb für die Betriebsmittel Konkurs anmeldet.

G 2.10 Nicht fristgerecht verfügbare Datenträger
Die korrekte Verwendung von Datenträgern ist für ein IT-Verfahren von besonderer Bedeutung. Bereits geringfügige Fehler - z. B. mangelhafte Kennzeichnung, falscher Aufbewahrungsort, fehlende Ein- oder Ausgabebestätigungen im Datenträgerarchiv - können dazu führen, daß ein Datenträger nicht in der erforderlichen Zeit aufgefunden werden kann. Die resultierenden Verzögerungen können zu erheblichen Schäden führen.

G 2.11 Unzureichende Trassendimensionierung
Bei der Planung von Netzen wird oft der Fehler begangen, die Kapazitätsauslegung ausschließlich am aktuellen Stand zu orientieren. Dabei wird übersehen

- Erweiterungen eines Netzes nicht auszuschließen sind,
- die Kapazität eines Netzes aufgrund steigenden Datenvolumens erweitert werden muß,
- neue Forderungen an das Netz die Verlegung anderer Kabel erforderlich machen.

Eine Erweiterung des Netzes ist nur in dem Umfang möglich, wie es die vorhandenen, verlegten Kabel zulassen oder der zur Verfügung stehende Platz für zusätzliche Kabel erlaubt. Gerade in geschlossenen Trassen (Rohre, estrichüberdeckte Fußbodenkanäle etc.) ist es trotz noch vorhandenen Platzes oft nicht möglich, zusätzliche Kabel einzuziehen, ohne neue und alte Kabel zu beschädigen. Als Ausweg bleibt dann nur, die vorhandenen Kabel aus der Trasse herauszuziehen und alle Kabel, die alten und die neuen, gleichzeitig neu einzuziehen. Die dadurch entstehenden Betriebsbeeinträchtigungen und Kosten sind beträchtlich.

G 2.12 Unzureichende Dokumentation der Verkabelung
Ist aufgrund unzureichender Dokumention die genaue Lage von Leitungen nicht bekannt, so kann es bei Bauarbeiten außerhalb oder innerhalb eines Gebäudes zu Beschädigungen von Leitungen kommen. Dabei kann es zu längeren Ausfallzeiten oder unter Umständen sogar zu lebensbedrohenden Gefahren, z.B. durch Stromschlag, kommen.
Eine unzureichende Dokumentation erschwert zudem Prüfung, Wartung und Reparatur von Leitungen sowie Rangierungen, wie sie z. B. bei Änderungen im Endgeräte-Bereich (Umzug, Neuzugang) erforderlich werden.

G 2.13 Unzureichend geschützte Verteiler
Verteiler des Stromversorgungsnetzes sind vielfach frei zugänglich und unverschlossen in Fluren oder Treppenhäusern untergebracht. Somit ist es jedermann möglich, diese Verteiler zu öffnen, Manipulationen vorzunehmen und ggf. einen Stromausfall herbeizuführen.

G 2.14 Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen
Ein nicht nach ergonomischen Gesichtspunkten eingerichteter Arbeitsplatz oder das Arbeitsumfeld (z. B. Störungen durch Lärm oder Staub) können dazu führen, daß die zur Verfügung stehende IT nicht oder nicht optimal genutzt werden kann.
Die meisten der denkbaren Störungen wirken sich nicht direkt auf die IT aus. Vielmehr wird der Mitarbeiter in der Form beeinflußt, daß er seiner Aufgabe nicht mit entsprechender Konzentration nachgehen kann. Die Störungen reichen von Lärm oder starkem, unorganisiertem Kundenverkehr bis zu ungünstiger Beleuchtung, schlechter Belüftung u.ä.. Erste Anzeichen solcher Störungen sind die Verlangsamung der Aufgabenerledigung und die Zunahme kleiner Fehler (Zeichendreher, Schreibfehler). Dadurch wird nicht nur das direkte Arbeitsergebnis beeinträchtigt. Auch die gespeicherten Daten enthalten evtl. Fehler, die Integrität der Daten wird vermindert.

G 2.15 Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
Durch verschiedene Unix-Programme ist es möglich, Daten abzufragen, die das IT-System über die Benutzer speichert. Hiervon sind auch solche Daten betroffen, die Auskunft über das Leistungsprofil eines Benutzers geben können. Datenschutzrechtliche Gesichtspunkte müssen deshalb genauso beachtet werden wie die Gefahr, daß solche Informationen Mißbrauchsmöglichkeiten erleichtern.

G 2.16 Ungeordneter Benutzerwechsel bei tragbaren PCs
Der Benutzerwechsel bei tragbaren PCs wie Laptops oder Notebooks wird oftmals durch die einfache Übergabe des Gerätes vorgenommen. Dies hat zur Folge, daß meist nicht sichergestellt wird, daß auf dem Gerät keine schutzbedürftigen Daten mehr gespeichert sind und daß das Gerät nicht mit einem Computer-Virus verseucht ist. Zudem ist nach einiger Zeit nicht mehr nachvollziehbar, wer den tragbaren PC wann genutzt hat oder wer ihn zur Zeit benutzt. Der ungeordnete Benutzerwechsel ohne Speicherkontrollen und ohne entsprechende Dokumentation kann damit zur Einschränkung der Verfügbarkeit des Geräts und zum Vertraulichkeitsverlust von Restdaten der Festplatte führen.

G 2.17 Mangelhafte Kennzeichnung der Datenträger
Unterbleibt eine ordnungsgemäße Kennzeichnung der ausgetauschten Datenträger, so ist für den Empfänger oft nicht nachvollziehbar, wer den Datenträger übersandt hat, welche Informationen darauf gespeichert sind oder welchem Zweck sie dienen. Wenn mehrere Datenträger ein- und desselben Absenders eingehen, kann bei fehlender Kennzeichnung die Reihenfolge verwechselt werden.

G 2.18 Ungeordnete Zustellung der Datenträger
Bei ungeordneter Zustellung von Datenträgern besteht die Gefahr, daß vertrauliche, auf dem Datenträger gespeicherte Daten in unbefugte Hände gelangen oder das gewünschte Ziel nicht rechtzeitig erreichen.

G 2.19 Unzureichendes Schlüsselmanagement bei Verschlüsselung

Werden zum Schutz der Vertraulichkeit zu übermittelnder Daten Verschlüsselungssysteme eingesetzt, so kann aufgrund eines unzureichenden Schlüsselmanagements der gewünschte Schutz unterlaufen werden, wenn

- die Schlüssel in einer ungesicherten Umgebung erzeugt oder aufbewahrt werden,
- ungeeignete oder leicht erratbare Schlüssel eingesetzt werden,
- die zur Verschlüsselung bzw. Entschlüsselung eingesetzten Schlüssel nicht auf einem sicheren und von der Datenübertragung getrennten Weg den Kommunikationspartner erreichen.

Einfachstes Negativ-Beispiel ist der Versand der verschlüsselten Informationen und des benutzten Schlüssels auf ein- und derselben Diskette, vorausgesetzt, daß das bei der Verschlüsselung eingesetzte Verfahren bekannt ist.

G 2.20 Unzureichende Versorgung mit Druck-Verbrauchsgütern für Fax-Geräte
Fax-Geräte benötigen für ihren Betrieb einige Verbrauchsgüter. In der Regel sind dies Papier und Druckermaterial (Toner oder Tinte, Druck-Zwischenträgerfolie). Fehlt eines dieser Verbrauchsgüter, können eingehende Faksimiles nicht mehr ausgedruckt werden, obwohl sie ordnungsgemäß empfangen wurden. Ein Puffer-Speicher kann aufgrund seiner begrenzten Speicherkapazität die Abweisung oder den Verlust von Fax-Sendungen nur herauszögern, aber nicht langfristig verhindern.

G 2.21 Mangelhafte Organisation des Wechsels zwischen den Benutzern
Arbeiten mehrere Benutzer zeitlich versetzt an einem Einzelplatz-IT-System, so findet zwangsläufig ein Wechsel zwischen den Benutzern statt. Ist dieser nicht ausreichend organisiert und geregelt, wird er unter Umständen nicht sicherheitsgerecht durchgeführt. Hierdurch können Mißbrauchsmöglichkeiten entstehen, wenn z. B.

- laufende Anwendungen nicht korrekt abgeschlossen werden,
- aktuelle Daten nicht gespeichert werden,
- Restdaten im Hauptspeicher oder in temporären Dateien verbleiben,
- der vorhergehende Benutzer sich nicht am IT-System abmeldet und
- der neue Benutzer sich nicht ordnungsgemäß am IT-System anmeldet.

G 2.22 Fehlende Auswertung von Protokolldaten
Protokolldaten dienen dem Zweck, nachträglich feststellen zu können, ob Sicherheitsverletzungen im IT-System stattgefunden haben oder ob ein solcher Versuch unternommen wurde. Daher können Protokolldaten für die Täterermittlung im Schadensfall genutzt werden. Eine weitere wichtige Funktion der Protokolldaten ist die Abschreckung. Werden Protokolldaten regelmäßig

ausgewertet, können vorsätzliche Angriffe auf ein IT-System frühzeitig erkannt werden. Findet die Auswertung der Protokolldaten jedoch nicht oder nur unzureichend statt und wird dies bekannt, verliert sich die Abschreckungswirkung vollständig.

G 2.23 Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Netz

Durch die Einbindung von DOS-PCs in ein servergestütztes Netz können in einem ansonsten sicheren Netz Schwachstellen hinzukommen.
Werden beispielsweise DOS-PCs in ein Unix-Netz eingebunden, ist den Benutzern der Einsatz von Unix-Diensten wie telnet, ftp, NFS, RPCs, X-Windows möglich. Die hierdurch entstehenden Sicherheitsprobleme sind grundsätzlich nicht verschieden von denen in einem reinen Unix-Netz.
Jedoch werden durch die Einbindung von DOS-PCs in ein servergestütztes Netz zusätzliche unkontrollierte Netzzugänge geschaffen. Jeder Netzanschluß kann zum Abhören des Netzes mißbraucht werden. Dies ist mit geeigneter Software (Sniffer) auch durch einen am Netz angeschlossenen PC möglich. Damit ist es ein Leichtes, alle Informationen, d.h. alle Paßwörter und auch Dateiinhalte, die über das Netz verschickt werden mitzulesen und zu mißbrauchen.
Ein PC-Benutzer kann zudem i.allg. den PC selbständig administrieren. Indem er den PC so konfiguriert, daß hiermit eine falsche Identität vorgespiegelt wird, kann er zugelassene Dienste wie z.B. NFS oder RPCs nutzen, um Zugriff auf Verzeichnisse und Dateien anderer Benutzer auf dem Server zu erlangen. Er kann diese Informationen dann unbemerkt lesen, kopieren, verfälschen oder löschen.
DOS-PCs, die in ein Windows NT Netz eingebunden sind, stellen ebenfalls eine potentielle Bedrohung der Sicherheit dieses Netzes dar. So können durch Kopieren von Dateien von einem Server auf die Festplatte eines PCs sicherheitsrelevante Informationen auf einem physisch nur unzureichend geschützten Medium abgelegt werden, oder durch Kopieren auf ein lokales Diskettenlaufwerk können solche Informationen an externe Stellen abgegeben werden, ohne daß dies von den Protokollierungsfunktionen des Servers erfaßt wird. Umgekehrt besteht die Gefahr des Imports von Computer-Viren über ungenügend abgesicherte Diskettenlaufwerke.

G 2.24 Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes

Bei einem nicht durch eine Firewall geschützten Netz, das mit einem externen Netz wie dem Internet gekoppelt ist, können aus dem externen Netz verschiedene Daten des internen Netzes wie z.B. Mail-Adressen, IP-Nummern, Rechnernamen und Benutzernamen abgerufen werden. Dadurch lassen sich Rückschlüsse auf die interne Netzstruktur und dessen Anwender ziehen. Je mehr Informationen ein Angreifer über potentielle Angriffsziele hat, desto mehr Angriffsmöglichkeiten hat er. Wenn ein Angreifer z.B. Benutzernamen eines IT-Systems kennt, kann er versuchen, die zugehörigen Paßwörter zu erraten oder über Wörterbuchattacken herauszufinden (siehe auch G 5.18 - Systematisches Ausprobieren von Paßwörtern).

G 2.25 Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäten

Wird eines der Betriebssysteme WfW, Windows 95 oder Windows NT in einem servergestütz-

ten PC-Netz als Benutzeroberfläche eingesetzt, können einzelne Peer-to-Peer-Funktionalitäten die Übertragungsbandbreite im servergestützten Netz einschränken, da dasselbe physikalische Medium beansprucht wird. Beispielsweise erfolgen Zugriffe auf Dateien des Servers mit erheblichen Verzögerungen, wenn gleichzeitig über die Peer-to-Peer-Funktionen große Dateien von PC zu PC kopiert werden. Ein PC kann in einem Peer-to-Peer-Netz als „Server", d.h. als Applikations- oder Dateianbieter für andere Rechner, eingesetzt werden. Dabei wird er durch die zu verwaltenden Peer-to-Peer-Funktionalitäten erheblich belastet, wodurch die lokale Bearbeitungsgeschwindigkeit deutlich abnimmt.

G 2.26 Fehlendes oder unzureichendes Software-Test- und Freigabeverfahren
Wird neue Software nicht oder nur unzureichend getestet und ohne Installationsvorschriften freigegeben, kann es passieren, daß Fehler in der Software nicht erkannt werden oder daß die notwendigerweise einzuhaltenden Installationsparameter nicht erkannt bzw. nicht beachtet werden. Diese Software- oder Installationsfehler, die aus einem fehlenden oder unzureichenden Software-Test- und Freigabeverfahren resultieren, stellen eine erhebliche Gefährdung für den IT-Betrieb dar.
Im Vertrauen auf eine problemlose Installation neuer Software wird oftmals übersehen, daß mögliche Schäden in keinem Verhältnis zu dem Aufwand stehen, den ein geordnetes Test- und Freigabeverfahren erfordert. Programme werden unzureichend getestet und mit Fehlern in eine Produktionsumgebung eingebracht. Die Fehler wirken sich in der Folge störend auf den bis zu diesem Zeitpunkt problemlosen Betrieb aus.

G 2.27 Fehlende oder unzureichende Dokumentation
Verschiedene Formen der Dokumentation können betrachtet werden: die Produktbeschreibung, die Administrator- und Benutzerdokumentation zur Anwendung des Produktes und die Systemdokumentation.
Eine fehlende oder unzureichende Dokumentation der eingesetzten IT-Komponenten kann sowohl im Auswahl- und Entscheidungsprozeß für ein Produkt, als auch bei einem Schadensfall im Wirkbetrieb erhebliche Auswirkungen haben.
Bei einer unzureichenden Dokumentation kann sich im Schadensfall, beispielsweise durch den Ausfall von Hardware bzw. Fehlfunktionen von Programmen, die Fehlerdiagnose und -behebung erheblich verzögern oder völlig undurchführbar sein.

G 2.28 Verstöße gegen das Urheberrecht
Der Einsatz nichtlizenzierter Software kann einen Verstoß gegen das Urheberrecht darstellen und sowohl zu zivil- als auch strafrechtlichen Konsequenzen führen.
Behörden und Unternehmen, in denen Raubkopien zum Einsatz kommen, können im Rahmen des Organisationsverschuldens, unabhängig von der Schuldform (Vorsatz oder Fahrlässigkeit) vom Urheberrechtseigentümer schadensersatzpflichtig gemacht werden.

G 2.29 Softwaretest mit Produktionsdaten
Vielfach ist zu beobachten, daß Softwaretests mit Produktionsdaten vollzogen werden. Als wesentliche Gründe werden hierfür angeführt, daß nur im direkten Vergleich mit vorhande-

nen Arbeitsergebnissen eine abschließende Beurteilung über die Funktion und Performance des Produktes möglich ist. Darüber hinaus sind mangelndes Sicherheitsbewußtsein, überzogenes Vertrauen in die zu testende Software und Unkenntnis über mögliche schädliche Auswirkungen ursächlich für diese Vorgehensweise.
Beim Test mit Produktionsdaten kann es zu folgenden Problemen kommen:

- Software wird mit Kopien von Produktionsdaten in isolierter Testumgebung getestet: Wenn neue Software mit nicht anonymisierten Daten getestet wird, erhalten evtl. nicht befugte Mitarbeiter, bzw. Dritte, die mit dem Softwaretest beauftragt worden sind, hierbei Einblick in Dateien mit evtl. vertraulichen Informationen.

- Software wird mit Produktionsdaten im Wirkbetrieb getestet: Fehlfunktionen von Software während des Testens können über den oben geschilderten Fall hinaus beispielsweise dazu führen, daß neben der Vertraulichkeit der Produktionsdaten auch deren Integrität und Verfügbarkeit beeinträchtigt werden.
  Aufgrund der Inkompatibilität unterschiedlicher Programme können Seiteneffekte auftreten, die bei anderen Systemkomponenten zu nachhaltigen Beeinträchtigungen führen können. Bei vernetzten Systemen kann das von Performanceverlusten bis hin zum Systemabsturz des Netzes reichen.
  Durch fehlerhaftes Verhalten der zu testenden Software oder Bedienfehler können Produktionsdaten ungewollt verändert werden. Möglicherweise wird diese Veränderung nicht festgestellt. Da Datenbestände, um unnötige Redundanz zu vermeiden, zunehmend durch unterschiedliche Programme gemeinsam genutzt werden, können sich diese Fehler auch auf andere IT-Anwendungen auswirken. Im Schadensfall ist nicht nur der Aufwand für die Rekonstruktion der Daten notwendig, darüber hinaus müssen bereits erstellte Arbeitsergebnisse auf ihre Integrität überprüft werden.

G 2.30 Unzureichende Domänenplanung

Eine unzureichende Planung der Domänen und ihrer Vertrauensbeziehungen in einem Windows NT Netz kann dazu führen, daß Vertrauensbeziehungen zu Domänen bestehen, die nicht als vertrauenswürdig zu betrachten sind. Damit ist es Benutzern der betreffenden Domänen unter Umständen möglich, auf Ressourcen der vertrauenden Domäne zuzugreifen, ohne daß dies dort beabsichtigt ist oder auch nur erkannt wird. Dies kann insbesondere dann geschehen, wenn die Zugriffsrechte der vertrauenden Domäne in der Annahme, daß keine andere Domäne auf die lokalen Ressourcen zugreift, relativ weitgehend festgesetzt wurden.
Umgekehrt können fehlende Vertrauensbeziehungen zwischen Domänen dazu führen, daß sich Benutzer unnötigerweise explizit bei fremden Domänen authentisieren müssen, was bei mangelnder Koordination der Paßwörter zwischen diesen Domänen zu Verwirrung führt. Der Benutzer muß sich dann eine Vielzahl von Paßwörtern merken, was zu einer Beeinträchtigung der Sicherheit führen kann, wenn er sich die Paßwörter aufschreibt.

G 2.31 Unzureichender Schutz des Windows NT Systems

Windows NT wird mit sehr weitgehenden Zugriffsrechten auf das Dateisystem und auf die

Registrierung ausgeliefert. Wenn diese Zugriffsrechte nicht nach der Installation entsprechend den lokalen Sicherheitsanforderungen strikter eingestellt werden, besitzt effektiv jeder Benutzer Zugriff auf alle Dateien und auf die gesamte Registrierung, d.h. der Zugriffsschutz ist de facto ausgeschaltet. Weiterhin ist Windows NT nicht in der Lage, den Zugriff auf Disketten- und CD-ROM-Laufwerke sowie auf Bänder zu kontrollieren, so daß hier eine Möglichkeit zu unzulässigem Datenimport und -export besteht, wenn nicht durch zusätzliche Maßnahmen der Zugriff auf diese Datenträger eingeschränkt oder zumindest auf organisatorischer Ebene kontrolliert wird.

G 2.32 Unzureichende Leitungskapazitäten
Bei der Planung von Netzen wird oft der Fehler begangen, die Kapazitätsauslegung ausschließlich am aktuellen Bedarf vorzunehmen. Dabei wird übersehen, daß die Kapazitätsanforderungen an das Netz stetig steigen, z. B. wenn neue IT-Systeme in das Netz integriert werden oder das übertragene Datenvolumen zunimmt.
Wenn die Kapazität des Netzes nicht mehr ausreicht, wird die Übertragungsgeschwindigkeit und ggf. auch die Erreichbarkeit im Netz für alle Benutzer stark eingeschränkt. Beispielsweise werden Dateizugriffe auf entfernten IT-Systemen erheblich verzögert, wenn gleichzeitig das Netz von anderen Benutzern stark in Anspruch genommen wird, wie durch das Verschieben von großen Dateien von einem IT-System zum anderen.

G 2.35 Fehlende Protokollierung unter Windows 95
Auf einem nicht vernetzten Windows 95-Rechner gibt es keine Möglichkeit, die Aktivitäten eines oder mehrerer Benutzer benutzerspezifisch zu protokollieren. Es ist daher nicht festzustellen, ob Sicherheitsverletzungen im IT-System stattgefunden haben oder ob ein solcher Versuch unternommen wurde.

G 2.36 Ungeeignete Einschränkung der Benutzerumgebung
Verschiedene Betriebssysteme (z. B. Windows 95, Windows NT) und PC-Sicherheitsprodukte bieten die Möglichkeit, die Benutzerumgebung individuell für jeden Benutzer einzuschränken. Dabei bestehen prinzipiell zwei Möglichkeiten:
1. Bestimmte Funktionalitäten werden erlaubt, alle anderen sind verboten.
2. Bestimmte Funktionalitäten werden verboten, alle anderen sind erlaubt.
In beiden Fällen besteht die Möglichkeit, den Benutzer derart einzuschränken, daß dieser wesentliche Funktionen nicht mehr ausführen kann oder daß sogar ein sinnvolles und effizientes Arbeiten mit dem PC nicht mehr möglich ist.

G 2.37 Unkontrollierter Aufbau von Kommunikationsverbindungen
Beim Einsatz von Kommunikationskarten innerhalb eines IT-Systems (Fax-, Modem- oder ISDN-Karten) ist für den Benutzer nicht immer offensichtlich, was außer seinen Nutz- und Protokollinformationen zusätzlich übertragen wird. Nach Aktivierung einer Kommunikationskarte ist es grundsätzlich möglich, daß diese, ohne Initiierung durch den Benutzer, Verbindungen zu einer nicht gewünschten Gegenstelle aufbaut oder durch Dritte über dem Benutzer nicht bekannte Remote-Funktionalitäten angesprochen wird.

G 2.38 Fehlende oder unzureichende Aktivierung von Datenbank-Sicherheitsmechanismen

Jede Datenbank-Standardsoftware stellt in der Regel eine Reihe von Sicherheitsmechanismen bereit, mittels derer die Daten vor unberechtigtem Zugriff o. ä. geschützt werden können. Sie sind jedoch nicht unbedingt automatisch aktiv, sondern müssen vom Datenbank-Administrator meistens manuell eingeschaltet werden. Wird davon kein Gebrauch gemacht, so kann weder die Vertraulichkeit noch die Integrität der Daten gewährleistet werden. In diesem Fall ist es dann meistens nicht möglich, solche Schutzverletzungen zu erkennen und zu protokollieren. Der Verlust bzw. die Manipulation von Daten bis hin zur Zerstörung der Datenbank selbst kann die Folge sein.

G 2.39 Komplexität eines DBMS

Die Auswahl und der Einsatz einer Datenbank-Standardsoftware erfordert sorgfältige Planung, Installation und Konfiguration des Datenbank-Managementsystems (DBMS), um einen störungsfreien Einsatz zu gewährleisten. Die Vielzahl möglicher Gefährdungen sollen durch die nachfolgenden Beispiele verdeutlicht werden.
Auswahl einer ungeeigneten Datenbank-Standardsoftware

- Es wird ein DBMS ausgewählt, welches in der geplanten Einsatzumgebung nicht lauffähig ist. Dies kann daraus resultieren, daß das DBMS an ein bestimmtes Betriebssystem gebunden ist oder die Mindestanforderungen an die Hardware nicht erfüllt werden.

- Das ausgewählte DBMS stellt ein Sicherheitsrisiko dar, weil die vom Hersteller zur Verfügung gestellten Sicherheitsmechanismen nicht ausreichen, um die geforderte Verfügbarkeit, Integrität und Vertraulichkeit der Daten zu gewährleisten.

Fehlerhafte Installation bzw. Konfiguration der Datenbank-Standardsoftware

- Es können sich weitere Gefährdungen ergeben, wenn die vom Hersteller empfohlenen Sicherheitsmaßnahmen falsch oder gar nicht durchgeführt werden.
  Beispiel: Die Kontrolldateien eines Datenbanksystems werden nicht gespiegelt bzw. die gespiegelte Kontrolldatei wird nicht auf einer anderen Festplatte abgelegt. Ein Plattencrash führt dabei unweigerlich zur Zerstörung der Datenbank.

- Die physischeVerteilung der Daten ist unzureichend (falls das DBMS eine physikalische Verteilung vorsieht).
  Beispiel: In einer Oracle-Datenbank gibt es eine maximal zulässige Anzahl Dateien pro Tablespace. Werden nun alle Daten im System-Tablespace verwaltet, so können keine Dateien mehr hinzugefügt werden, wenn diese maximale Anzahl erreicht ist. Da im System-Tablespace auch das Data Dictionary abgelegt ist, kann dieses Problem nur über eine komplette Neu-Installation der Datenbank behoben werden.

- Durch falsche Parametereinstellungen kann der Zugriff auf bestimmte Daten verhindert werden.

G 2.40 Komplexität des Datenbankzugangs/-zugriffs
Die Benutzer greifen über ein Datenbankmanagementsystem (DBMS) auf eine oder mehrere Datenbanken zu. Dabei können sie dies direkt tun oder aber von einer Anwendung aus. Um die Integrität einer Datenbank zu gewährleisten, müssen alle Datenbankzugriffe von einer zentralen Stelle aus kontrolliert werden. Aufgrund der Komplexität solcher Zugriffe können die folgenden Probleme entstehen.
Fehlerhafte Konzeption der Benutzerumgebung

- Ist der Berechtigungsumfang für die Benutzer zu restriktiv definiert, kann dies dazu führen, daß sie bestimmte Arbeiten nicht durchführen können.
- Ist der Berechtigungsumfang für die Benutzer dagegen zu umfangreich, kann dies dazu führen, daß Daten unberechtigt manipuliert bzw. eingesehen werden können. Dadurch werden die Integrität und Vertraulichkeit der Datenbank verletzt.
- Wird es den Benutzern erlaubt, direkt auf die Datenbank zuzugreifen (im Gegensatz zum Zugriff aus einer Anwendung heraus), so besteht das Risiko des Integritätsverlustes der Datenbank durch Datenmanipulationen, deren Auswirkungen die Benutzer nicht abschätzen können.
- Werden Datenbankobjekte von den darauf zugreifenden Anwendungen nicht explizit durch ein entsprechendes Berechtigungs- und Zugriffskonzept geschützt, so besteht das Risiko, daß die Datenbankobjekte selbst manipuliert werden (Manipulation von Feldern einer Tabelle, Manipulation von Tabellen-Indizes etc.). Dies kann zur Zerstörung der Datenbank führen.

Remote-Zugriff auf Datenbanken

- Wird die Datenbank in einem Netz zur Verfügung gestellt, so können durch mangelnde Sicherheitsvorkehrungen im Bereich des Remote-Zugriffs auf die Datenbank sowohl Daten manipuliert als auch unberechtigt eingesehen werden. Auch dies verletzt die Integrität und Vertraulichkeit der Datenbank. Datenbankabfragen
- Die Menge aller möglichen Datenbankabfragen muß für jeden Benutzer eingeschränkt sein bzw. bestimmte Abfragen müssen explizit verboten werden. Ist dies nicht der Fall, kann dies (insbesondere bei statistischen Datenbanken) zum Verlust der Vertraulichkeit schutzbedürftiger Daten führen.
- Werden Datenbankabfragen innerhalb einer Anwendung nicht gemäß des SQL-Standards formuliert, so kann dies dazu führen, daß sie vom DBMS nicht bearbeitet werden können und zurückgewiesen werden (insbesondere beim Einsatz von DBMS'en verschiedener Hersteller).
- Bei der Verwendung von nicht exakt formulierten Datenbankabfragen kann dies dazu führen, daß durch eine Änderung der Datenbankobjekte die Datenbankabfrage plötzlich falsche oder unerwartete Ergebnisse liefert.

G 2.41 Mangelhafte Organisation des Wechsels von Datenbank-Benutzern
Teilen sich mehrere Benutzer einer Datenbank den gleichen Arbeitsplatz, so besteht die Gefahr von ungewollten oder gezielten Datenmanipulationen, wenn der Wechsel zwischen den Benutzern nicht organisiert ist bzw. der Wechsel nicht ordnungsgemäß durchgeführt wird. Auch ist dann die Vertraulichkeit der Daten nicht mehr gewährleistet.

G 2.47 Ungesicherter Akten- und Datenträgertransport
Werden Dokumente, Datenträger oder Akten zwischen der Institution und anderen Stellen, zum Beispiel dem häuslichen Arbeitsplatz, transportiert, besteht die Gefahr, daß sie

- auf dem Transportweg verloren gehen,
- auf dem Transportweg entwendet werden,
- auf dem Transportweg gelesen oder manipuliert werden und
- an einen falschen Empfänger übergeben werden.

Insbesondere wenn es sich um Unikate handelt, können Zerstörung, Vertraulichkeitsverlust oder Manipulation größere Schäden verursachen.

G 2.48 Ungeeignete Entsorgung der Datenträger und Dokumente am häuslichen Arbeitsplatz
Sind am häuslichen Arbeitsplatz keine geeigneten Möglichkeiten vorhanden, um Datenträger und Dokumente geeignet zu entsorgen, können bei unsachgemäßer Entsorgung Informationen oder Restinformationen auf den Datenträgern von Dritten ausgelesen oder aus den Dokumenten extrahiert werden. Der entstehende Schaden richtet sich nach dem Wert der Informationen.

G 2.54 Vertraulichkeitsverlust durch Restinformationen
Bei elektronischer Datenübermittlung oder Datenträgerweitergabe passiert es immer wieder, daß dabei auch Informationen weitergegeben werden, die die Institution nicht verlassen sollten.

G 2.55 Ungeordnete E-Mail-Nutzung
Bei ungeordneter Nutzung von E-Mails besteht die Gefahr, daß sensitive Daten Unbefugten zur Kenntnis gelangen oder das gewünschte Ziel nicht rechtzeitig erreichen.

G 2.56 Mangelhafte Beschreibung von Dateien
Werden beim elektronischen Dateiaustausch die übertragenen Dateien nicht gut genug beschrieben, so ist für den Empfänger oft nicht nachvollziehbar, wer diese übersandt hat, welche Informationen sie enthalten oder welchem Zweck sie dienen. Wenn mehrere E-Mails ein- und desselben Absenders eingehen, kann bei fehlender oder schlechter Kennzeichnung die Reihenfolge verwechselt werden.

G 2.57 Nicht ausreichende Speichermedien für den Notfall
Wenn Daten nach ihrer Zerstörung wiederhergestellt werden müssen, ist es vielen Fällen notwendig, die gesicherten Daten zunächst auf getrennten Speichermedien wiedereinzuspielen. Dies

ist insbesondere bei komplexeren Datenstrukturen wie z.B. bei Datenbanken notwendig, da die Wiederherstellung nicht immer reibungslos und fehlerfrei funktioniert. Wird die hierfür benötigte Speicherkapazität nicht für den Notfall vorgehalten, kann es durch übereiltes Handeln während des Notfalls zu weiteren Datenverlusten kommen.

G.3 Gefährdungskatalog Menschliche Fehlhandlungen

G 3.1 Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
Durch Fehlverhalten können IT-Benutzer den Vertraulichkeits-/Integritätsverlust von Daten herbeiführen bzw. ermöglichen. Die Folgeschäden ergeben sich aus der Schutzbedürftigkeit der Daten.

G 3.2 Fahrlässige Zerstörung von Gerät oder Daten
Durch Fahrlässigkeit, aber auch durch ungeschulten Umgang kann es zu Zerstörungen an Geräten und Daten kommen, die den Betrieb des IT-Systems empfindlich stören können. Dies ist auch durch die unsachgemäße Verwendung von IT-Anwendungen möglich, wodurch fehlerhafte Ergebnisse entstehen oder Daten unabsichtlich verändert oder zerstört werden.

G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
Aufgrund von Nachlässigkeit und fehlenden Kontrollen kommt es immer wieder vor, daß Personen die ihnen empfohlenen oder angeordneten IT-Sicherheitsmaßnahmen nicht oder nicht im vollen Umfang durchführen. Es können Schäden entstehen, die sonst verhindert oder zumindest vermindert worden wären. Je nach der Funktion der Person und der Bedeutung der mißachteten Maßnahme können sogar gravierende Schäden eintreten. Vielfach werden IT-Sicherheitsmaßnahmen aus einem mangelnden Sicherheitsbewußtsein heraus nicht beachtet. Ein typisches Indiz dafür ist, daß wiederkehrende Fehlermeldungen nach einer gewissen Gewöhnungszeit ignoriert werden.

G 3.4 Unzulässige Kabelverbindungen
Hauptursache unzulässiger Verbindungen ist neben technischen Defekten die fehlerhafte Verkabelung, z.B. bei der Belegung von Rangier- und Spleißverteilern. Ungenaue Dokumentation und unzureichende Kabelkennzeichnung führen häufig zu versehentlichen Fehlbelegungen und erschweren das Erkennen von absichtlichen Fehlbelegungen. Durch unzulässige Verbindungen können Informationen zusätzlich oder ausschließlich zu falschen Empfängern übertragen werden. Die normale Verbindung kann gestört werden.

G 3.5 Unbeabsichtigte Leitungsbeschädigung
Je ungeschützter ein Kabel verlegt ist, desto größer ist die Gefahr einer unbeabsichtigten Beschädigung. Die Beschädigung führt nicht unbedingt sofort zu einem Ausfall von Verbindungen. Auch die zufällige Entstehung unzulässiger Verbindungen ist möglich.

G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal
Die Gefährdung durch Reinigungs- und Fremdpersonal erstreckt sich von der unsachgemäßen Behandlung der technischen Einrichtungen, über den Versuch des „Spielens“ am IT-System ggf. bis zum Diebstahl von IT-Komponenten.

G 3.7 Ausfall der TK-Anlage durch Fehlbedienung
Neben dem technischen Versagen durch Defekt von Bauteilen, Stromausfall oder Sabotage gibt es eine Reihe weiterer Umstände, die zum Ausfall einer TK-Anlage führen können. So können z.B. durch unzureichend ausgebildetes Wartungspersonal Änderungen an der Anlagenkonfiguration vorgenommen werden, die solche Ausfälle zur Folge haben. Das nicht rechtzeitige Erkennen von Alarmsignalen oder abnormem Betriebsverhalten kann dieselbe Folge haben, ferner unsachgemäßes oder unüberlegtes Handeln bei eigentlich einfachen Routinereparaturen.

G 3.8 Fehlerhafte Nutzung des IT-Systems
Eine fehlerhafte Nutzung des IT-Systems beeinträchtigt die Sicherheit eines IT-Systems, wenn dadurch IT-Sicherheitsmaßnahmen mißachtet oder umgangen werden. Dies kann vermieden werden, wenn der Benutzer über die ordnungsgemäße Funktion und den Betrieb eines IT-Systems ausreichend informiert ist.

G 3.9 Fehlerhafte Administration des IT-Systems
Eine fehlerhafte Administration beeinträchtigt die Sicherheit eines IT-Systems, wenn dadurch IT-Sicherheitsmaßnahmen mißachtet oder umgangen werden. Eine fehlerhafte Administration liegt z.B. vor, wenn Netzzugangsmöglichkeiten (Daemon-Prozesse) geschaffen oder nicht verhindert werden, die für den ordnungsgemäßen Betrieb des IT-Systems nicht notwendig sind oder auf Grund ihrer Fehleranfälligkeit eine besonders große Bedrohung darstellen.

G 3.10 Falsches Exportieren von Dateisystemen unter Unix
Exportierte Platten können von jedem Rechner, der sich mit dem in der /etc/exports angegebenen Namen meldet, gemountet werden. Der Benutzer dieses Rechners kann jede UID und GID annehmen, d. h., es lassen sich nur Dateien schützen, die root gehören. Die Dateien von allen anderen Benutzern sind völlig ungeschützt, insbesondere also auch Dateien, die privilegierten Benutzern wie bin oder daemon gehören.

G 3.11 Fehlerhafte Konfiguration von sendmail
Fehler in der Konfiguration oder Software von sendmail haben in der Vergangenheit schon mehrmals zu Sicherheitslücken auf den betroffenen IT-Systemen geführt (Stichwort Internet-Wurm).

G 3.12 Verlust der Datenträger beim Versand
Werden Datenträger in nicht sonderlich stabilen Behältnissen (Briefumschlägen oder sonstigen Verpackungen) versandt, besteht die Gefahr, daß der Datenträger (insbesondere Disketten) bei Beschädigung der Verpackung verloren geht. Auch besteht die Gefahr des Verlustes auf dem Postweg oder durch Unachtsamkeit eines Boten. Falls beispielsweise eine Diskette zusammen

mit einem Anschreiben in einem Umschlag verschickt wird, der wesentlich größer als die Diskette ist, so kann beim Empfang des Umschlages die innenliegende Diskette übersehen und zusammen mit dem scheinbar leeren Umschlag entsorgt werden.

G 3.13 Übertragung falscher oder nicht gewünschter Datensätze
Es ist denkbar, daß der für den Versand vorgesehene Datenträger bereits Daten früherer Arbeitsgänge enthält, die dem Empfänger nicht zur Kenntnis gelangen sollen. Werden diese Daten nicht gezielt physikalisch gelöscht, können diese vom Empfänger gelesen werden. Befinden sich darüber hinaus die zu übertragenden Daten in einem Verzeichnis mit weiteren Daten, die ebenfalls schutzbedürftig sind, besteht die Gefahr, daß diese versehentlich mit auf den Datenträger übertragen werden (z.B. copy *.*) und dem Empfänger unnötig (unberechtigt) zur Kenntnis gelangen.
Sollen Datensätze nicht über das Medium „Datenträger", sondern über Datennetze direkt versandt werden (E-Mail im Internet, Modemverbindungen, interne Firmennetze, X.400-Dienst), bieten Kommunikationsprogramme die Möglichkeit der Verwendung von Kurzbezeichnungen für komplexe Adreßstrukturen und Verteilerlisten für die Mehrfachversendung. Werden solche Verteilerlisten nicht zentral geführt oder nicht in regelmäßigen Abständen aktualisiert, können Datensätze an Adressen versendet werden, die zu nicht mehr autorisierten Personen gehören.

G 3.14 Fehleinschätzung der Rechtsverbindlichkeit eines Fax
Häufig wird versucht, bei eiligen Entscheidungen den Postweg einzusparen, indem wichtige Unterlagen oder Informationen an den Geschäftspartner per Fax übermittelt werden. Dabei wird oft außer acht gelassen, daß so übermittelte Unterlagen in einem Streitfall nicht immer als rechtsverbindlich angesehen werden. Bestellungen müssen dann nicht vom Kunden angenommen, Zusagen nicht eingehalten werden. Eine Rechtsmittelfrist kann trotz rechtzeitigen Absendens eines Fax ablaufen.

G 3.16 Fehlerhafte Administration von Zugangs- und Zugriffsrechten
Zugangsrechte zu einem IT-System und Zugriffsrechte auf gespeicherte Daten und IT-Anwendungen dürfen nur in dem Umfang eingeräumt werden, wie sie für die Wahrnehmung der Aufgaben erforderlich sind. Werden diese Rechte fehlerhaft administriert, so kommt es zu Betriebsstörungen, falls erforderliche Rechte nicht zugewiesen wurden, bzw. zu Sicherheitslücken, falls über die notwendigen Rechte hinaus weitere vergeben werden.

G 3.17 Kein ordnungsgemäßer PC-Benutzerwechsel
Arbeiten mehrere Benutzer an einem PC, so kann es aufgrund von Nachlässigkeit oder Bequemlichkeit dazu kommen, daß sich bei einem Wechsel der vorhergehende Benutzer nicht abmeldet und der neue sich nicht ordnungsgemäß anmeldet. Dies wird von den Betroffenen meist damit begründet, daß die Zeit, die das IT-System zum Neustarten benötigt, sehr lang ist und als nicht akzeptabel empfunden wird.
Dieses Fehlverhalten führt jedoch dazu, daß die Protokollierung von An- und Abmeldevorgängen und damit ein Teil der Beweissicherung unwirksam wird. Es läßt sich anhand der Protokolle nicht mehr zuverlässig feststellen, wer den Rechner zu einem bestimmten Zeitpunkt genutzt hat.

G 3.21 Fehlbedienung von Codeschlössern

Erfahrungsgemäß führen Fehler in der Bedienung von mechanischen Codeschlössern verhältnismäßig oft dazu, daß der Schrank nicht mehr ordnungsgemäß geöffnet werden kann. Die Fehlbedienungen treten bei der Eingabe und besonders häufig bei der Änderung des Codes auf. Um die aufbewahrten Datenträger oder informationstechnischen Geräte wieder zugänglich zu machen, muß dann ein spezialisierter Schlüsseldienst beauftragt werden, so daß neben dem Schaden, der aus der fehlenden Verfügbarkeit der Datenträger oder Geräte entsteht, auch erhebliche Reparaturkosten anfallen können. Im ungünstigsten Falle muß ein neuer Schutzschrank beschafft werden.

G 3.22 Fehlerhafte Änderung der Registrierung

Windows 95 bietet die Möglichkeit, die Benutzerumgebung eines PC fest bzw. benutzerindividuell einzuschränken. Dies geschieht in der Regel unter Verwendung des Systemrichtlinieneditors (POLEDIT.EXE) oder des Registrierungseditors (REGEDIT.EXE). Die Benutzung dieser Programme sollte mit Bedacht und jede Änderung der Registrierung mit äußerster Sorgfalt ausschließlich durch geschultes Personal erfolgen, weil sehr schnell ein Systemzustand eingestellt werden kann, der ein Arbeiten mit dem PC nicht mehr erlaubt. Im ungünstigsten Fall ist dann das Betriebssystem neu zu installieren oder bestimmte Hardwarekomponenten erneut zu initialisieren (durch Laden der entsprechenden Treiber).

G 3.23 Fehlerhafte Administration eines DBMS

Wird ein Datenbankmanagementsystem (DBMS) nachlässig oder fehlerhaft administriert, kann dies folgende Gefährdungen nach sich ziehen:

- Verlust von Daten,
- (gezielte oder unbeabsichtigte) Datenmanipulation,
- unberechtigter Zugang zu vertraulichen Daten,
- Verlust der Datenbankintegrität,
- Crash der Datenbank und
- Zerstörung der Datenbank.

Die oben aufgeführten Gefährdungen können durch zu großzügig vergebene Rechte für die Benutzer, durch eine unregelmäßige oder gar keine Datenbanküberwachung, durch mangelhafte Datensicherungen, durch ungültige, aber noch nicht gesperrte Kennungen usw. hervorgerufen werden.

G 3.24 Unbeabsichtigte Datenmanipulation

Je umfangreichere Zugriffsberechtigungen auf eine Datenbank für die Anwender bestehen, um so größer ist auch das Risiko einer unbeabsichtigten Datenmanipulation. Dies kann prinzipiell

von keiner Anwendung verhindert werden.

G 3.31 Unstrukturierte Datenhaltung
Durch unzureichende Vorgaben und/oder fehlende Schulung der Mitarbeiter kann es zu einer unübersichtlichen Speicherung der Daten auf den benutzten Datenträgern kommen. Dadurch kann es zu verschiedenen Probleme kommen wie:

- Speicherplatzverschwendung durch mehrfache Speicherung von Dateien,
- vorschnelle Löschung oder nicht erfolgte Löschung von Daten, da keiner mehr weiß, was in welchen Dateien gespeichert ist,
- unbefugte Zugriffe, wenn sich Dateien in Verzeichnisse oder auf Datenträgern befinden, die Dritten zugänglich gemacht werden, oder
- nicht konsistente Versionsstände in verschiedenen Verzeichnen und IT-Systemen.

G.4 Gefährdungskatalog Technisches Versagen

G 4.1 Ausfall der Stromversorgung
Trotz hoher Versorgungssicherheit kommt es immer wieder zu Unterbrechungen der Stromversorgung seitens der Energieversorgungsunternehmen (EVU). Die größte Zahl dieser Störungen ist mit Zeiten unter einer Sekunde so kurz, daß der Mensch sie nicht bemerkt. Aber schon Unterbrechungen von mehr als 10 ms sind geeignet, den IT-Betrieb zu stören. Bei einer bundesweiten Messung mit ca. 60 Meßstellen wurden 1983 rund 100 solcher Netzeinbrüche registriert. Davon dauerten fünf Ausfälle bis zu 1 Stunde und einer länger als eine Stunde. Diese Unterbrechungen beruhten einzig auf Störungen im Versorgungsnetz. Dazu kommen Unterbrechungen durch Abschaltungen bei nicht angekündigten Arbeiten oder durch Kabelbeschädigungen bei Tiefbauarbeiten.
Von der Stromversorgung sind nicht nur die offensichtlichen, direkten Stromverbraucher (PC, Beleuchtung usw.) abhängig. Alle Infrastruktureinrichtungen sind heute direkt oder indirekt vom Strom abhängig, z. B. Aufzüge, Rohrpostanlagen, Klimatechnik, Gefahrenmeldeanlagen, Telefonnebenstellenanlagen. Selbst die Wasserversorgung in Hochhäusern ist wegen der zur Druckerzeugung in den oberen Etagen erforderlichen Pumpen stromabhängig.

G 4.2 Ausfall interner Versorgungsnetze
Es gibt in einem Gebäude eine Vielzahl von Netzen, die der Ver- und Entsorgung und somit als Basis für die IT dienen. Der Ausfall von Versorgungsnetzen wie

- Strom,
- Telefon und
- Klima/Lüftung

kann zu einer sofortigen Störung des IT-Betriebs führen. Demgegenüber kann es bei Ausfall in den Bereichen:

- Heizung,
- Wasser,
- Löschwasserspeisungen,
- Abwasser,
- Rohrpost,
- Gas,
- Melde- und Steueranlagen (Einbruch, Brand, Hausleittechnik) und
- Sprechanlagen

unter Umständen zu zeitverzögerten Störungen kommen.
Die Netze sind in unterschiedlich starker Weise voneinander abhängig, so daß sich Betriebsstörungen in jedem einzelnen Netz auch auf andere auswirken können.

G 4.3 Ausfall vorhandener Sicherungseinrichtungen
Durch technische Defekte oder äußere Einflüsse (z. B. aufgrund von Alterung, Fehlbedienung, mangelhafter Wartung, Manipulation, Stromausfall) kann es zum Ausfall von Sicherungseinrichtungen kommen, so daß ihre Schutzwirkung stark herabgesetzt ist oder gänzlich ausfällt.

G 4.4 Leitungsbeeinträchtigung durch Umfeldfaktoren
Die Übertragungseigenschaften von Kabeln mit elektrischer Signalübertragung können durch elektrische und magnetische Felder negativ beeinflußt werden. Ob dies zu einer tatsächlichen Störung der Signalübertragung führt, hängt im wesentlichen von drei Faktoren ab:

- Frequenzbereich, Stärke und Dauer der Einwirkung,
- Abschirmung des Kabels und
- Schutzmaßnahmen bei der Datenübertragung (Redundanz, Fehlerkorrektur).

Viele Beeinträchtigungen lassen sich im Vorfeld erkennen:

- Entlang von Starkstromtrassen und im Bereich großer Motoren entstehen starke induktive Felder (Eisenbahn, Produktionsbetrieb, Aufzug),
- Im Bereich von Sendeeinrichtungen existieren elektromagnetische Felder (Rundfunk, Polizei/Feuerwehr, Betriebsfunk, Personensuchanlagen, Funknetze),
- Mobiltelefone ("Handys") überschreiten durch ihre Sendeleistung (2 bis 4 Watt) die Störempfindlichkeit vieler IT-Systeme,

- Kabel beeinflussen sich gegenseitig durch wechselseitige Induktion.

Unabhängig von den rein elektrischen oder magnetischen Einflüssen können weitere Umfeldfaktoren auf ein Kabel wirken:

- hohe Temperaturen (in der Prozesssteuerung),
- aggressive Gase und
- hohe mechanische Belastungen (z.B. bei provisorischer Verlegung auf dem Fußboden oder Leitungen zu beweglichen Geräten).

G 4.5 Übersprechen
Übersprechen ist eine spezielle Form der Leitungsbeeinträchtigung. Dabei wird die Störung nicht allgemein im Umfeld, sondern durch Ströme und Spannungen von Signalen erzeugt, die auf eine benachbarte Leitung übertragen werden. Die Stärke dieses Effektes ist vom Kabelaufbau (Abschirmung, Kabelkapazität, Isolationsgüte) und von den elektrischen Parametern bei der Informationsübertragung (Strom, Spannung, Frequenz) abhängig. Nicht jede Leitung, die durch Übersprechen beeinflußt wird, muß ihrerseits auch andere beeinflussen. Bekannt ist dies aus dem Telefonnetz. Dort sind Gespräche anderer Netzteilnehmer zu hören. Diese reagieren aber auf die Aufforderung äus der Leitung zu gehenöft deswegen nicht, weil das Übersprechen nur in eine Richtung geschieht. Das Prüfen eigener Leitungen auf eingekoppelte Fremdsignale gibt keine Auskunft darüber, ob die eigenen Signale auf andere Leitungen übersprechen und somit dort abhörbar sind. Der wesentliche Unterschied zu anderen Leitungsstörungen ist der, daß neben der Störung der Signalübertragung auf benachbarten Leitungen durch Übersprechen auswertbare Informationen auf fremden Leitungen zur Verfügung stehen können.

G 4.6 Spannungsschwankungen/Überspannung/Unterspannung
Durch Schwankungen der Versorgungsspannung kann es zu Funktionsstörungen und Beschädigungen der IT kommen. Die Schwankungen reichen von extrem kurzen und kleinen Ereignissen, die sich kaum oder gar nicht auf die IT auswirken, bis zu Totalausfällen oder zerstörerischen Überspannungen. Die Ursache dafür kann in allen Bereichen des Stromversorgungsnetzes entstehen, vom Netz des Energieversorgungsunternehmens bis zum Stromkreis, an dem die jeweiligen Geräte angeschlossen sind.

G 4.7 Defekte Datenträger
Der Ausfall bzw. der Defekt einzelner Datenträger durch technische Mängel oder Beschädigung ist kein Einzelfall. Betroffen sind Massenspeicher wie Festplatten, Bänder oder Kassettensysteme. Festplatten können durch den „Headcrash“ des Schreib-/Lesekopfes, Bänder oder Kassetten durch direkte mechanische Einwirkung zerstört werden. Auch CD-ROMs können durch Verkratzen der Oberfläche unbrauchbar werden. Vor allem aber Disketten sind von Ausfällen betroffen. Häufig stellt man fest, daß diese nicht mehr beschreibbar oder lesbar sind.

G 4.8 Bekanntwerden von Softwareschwachstellen
Unter Softwareschwachstellen sollen unbeabsichtigte Programmfehler verstanden werden, die dem Anwender nicht oder noch nicht bekannt sind und ein Sicherheitsrisiko für das IT-System darstellen. Es werden ständig neue Sicherheitslücken in vorhandener, auch in weit verbreiteter oder ganz neuer Software gefunden.

G 4.9 Ausfall der internen Stromversorgung
Der Einsatz eines mobilen IT-Systems, z.B. eines Laptop, setzt voraus, daß das System über eine vom Versorgungsnetz unabhängige Stromversorgung verfügt. Diese meist mit wiederaufladbaren Batterien konzipierte Stromversorgung reicht üblicherweise für eine mehrstündige Betriebsdauer. Nach dieser Zeit ist die ausreichende Stromversorgung nicht mehr gesichert, so daß das IT-System außer Betrieb genommen bzw. an das Stromnetz angeschlossen werden muß. Die überwiegende Zahl der mobilen Systeme überprüft kontinuierlich die Versorgungsspannung und zeigt einen kritischen Spannungsabfall an. Wird diese Anzeige ignoriert, kann es passieren, daß das System plötzlich seinen Dienst versagt und die letzten Arbeitsergebnisse im Hauptspeicher verloren gehen.

G 4.10 Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
Im Gegensatz zu Stand-alone-Systemen, bei denen im wesentlichen der Login-Prozeß für die Zugangskontrolle verantwortlich ist und die somit nur durch schlechte oder fehlende Paßwörter korrumpiert werden können, gibt es auf Netzrechnern sehr viele komplexe Prozesse, die die verschiedensten Arten von Zugängen erlauben. So ermöglicht z. B. unter Unix der sendmail-Daemon das Einbringen von Texten (Mails) in den Netzrechner, der FTP-Daemon einen, wenn auch etwas eingeschränkten, Login, der u. U. (anonymous FTP) nicht einmal durch ein Paßwort geschützt ist, der telnet-Daemon einen kompletten Login.
Server-Systeme wie Windows NT oder Novell Netware vermeiden aus Sicherheitsgründen die Übertragung von Klartext-Paßwörtern. Dieser Schutzmechanismus wird jedoch durch den Einsatz von Diensten wie FTP oder Telnet unterlaufen, da hier wieder Klartext-Paßwörter Verwendung finden.
Abgesehen davon, daß alle diese Prozesse durch eine falsche oder fehlerhafte Konfiguration eine Sicherheitslücke darstellen können, ist auf Grund ihres Umfanges natürlich auch die Wahrscheinlichkeit, daß in einem dieser Prozesse ein sicherheitsrelevanten Programmierfehler ist, wesentlich größer.

G 4.11 Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Client
Kennt man den NIS-Domain-Namen, läßt sich jeder Rechner als Client anmelden, und es lassen sich alle NIS-Maps, insbesondere also auch die passwd Map, abrufen.
Ist es möglich, Administrationsrechte auf einem Rechner zu bekommen, läßt sich auf diesem ein NIS-Server-Prozeß (ypserv) an einem privilegierten Port starten. Startet man nun den Client-Prozeß ypbind auf dem zu infiltrierenden Rechner neu und sorgt dafür, daß der eigene Server-Prozeß vor dem korrekten NIS-Server antwortet, läßt sich jede beliebige Information an den Client überspielen.

G 4.12 Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Client
Für das X-Window-System gilt im besonderen Maße, daß es nur in einer vertrauenswürdigen Umgebung eingesetzt werden sollte, da es allen beteiligten Benutzern die Möglichkeit bietet, sowohl den X-Client als auch den X-Server zu korrumpieren. Den X-Server-Prozeß, der auf einem Rechner für die Ein- und Ausgabe zuständig ist, interessiert nicht, wem der X-Client-Prozeß, der mit ihm kommuniziert, gehört. Alle X-Clients können also auf alle Daten, die auf einem X-Server eingegeben werden, zugreifen, und der X-Server hat keine Möglichkeit festzustellen, von welchem X-Client er Daten erhält. So simuliert z.B. das Programm meltdown das optische „Schmelzen" des Bildschirms eines beliebigen X-Servers. Genauso ist es möglich, Daten von einem xterm-Client zu lesen oder ihm eigene Daten zu schicken, also z.B. Bildschirmabzüge von einem anderen, mit X-Windows arbeitenden Rechner zu machen.

G 4.13 Verlust gespeicherter Daten
Der Verlust gespeicherter Daten kann erhebliche Auswirkungen auf den IT-Einsatz haben. Sind die Anwendungsdaten oder die Kundenstammdaten verloren oder verfälscht, so können privatwirtschaftliche Betriebe in ihrer Existenz bedroht sein. Der Verlust oder die Verfälschung wichtiger Dateien kann in Behörden Verwaltungs- und Fachaufgaben verzögern oder sogar ausschließen.
Dabei können die Gründe für den Verlust gespeicherter Daten vielfältiger Art sein:

- Entmagnetisierung von magnetischen Datenträgern durch Alterung oder durch ungeeignete Umfeldbedingungen (Temperatur, Luftfeuchte),
- Störung magnetischer Datenträger durch äußere Magnetfelder,
- Zerstörung von Datenträgern durch höhere Gewalt wie Feuer oder Wasser,
- versehentliches Löschen oder Überschreiben von Dateien,
- technisches Versagen von Peripheriespeichern (Headcrash),
- fehlerhafte Datenträger,
- unkontrollierte Veränderungen gespeicherter Daten (Integritätsverlust) und
- vorsätzliche Datenzerstörung durch Computer-Viren usw.

G 4.14 Verblassen spezieller Fax-Papiere
Bei Fax-Geräten, die im Thermodruckverfahren arbeiten, muß Spezialpapier eingesetzt werden, auf dem oft bereits nach relativ kurzer Zeit die Schrift bis zur Unlesbarkeit verblaßt oder durch Schwärzung des Papieres unlesbar wird. Außerdem können sich diese Papiere bei Kontakt mit Textmarkern oder Klebstoffen so verfärben, daß der Text nicht mehr lesbar ist.

G 4.15 Absenden eines Fax an einen falschen Empfänger durch Fehlverbindung
Durch Fehlschaltungen im öffentlichen Fernsprechnetz oder durch simples Verwählen kann ein

Fax an einen falschen Empfänger übermittelt werden. Dadurch können u. U. vertrauliche Informationen unbefugten Personen bekannt werden. Der mögliche Schaden richtet sich nach der Vertraulichkeit der Informationen. Darüber hinaus wird der Absender im Glauben bleiben, daß das Fax ordnungsgemäß an den gewünschten Adressaten übermittelt wurde. Hierdurch auftretende Zeitverzögerungen können zu Schäden führen.

G 4.16 Übertragungsfehler bei Fax-Versand
Durch Störungen auf dem Übertragungsweg oder bei den beteiligten Geräten können Informationen unvollständig oder unlesbar beim Empfänger ankommen. Entscheidungen, die auf diesen Informationen beruhen, können daher zu Schäden führen.

G 4.17 Technischer Defekt des Fax-Gerätes
Bei technischen Fehlern kann ein Fax-Gerät ausfallen oder die Informationen nicht oder nur unvollständig wiedergeben. Damit sind Verfügbarkeit und Integrität der gespeicherten oder übertragenen Informationen gefährdet. Besonders kritisch ist dies dort, wo der Defekt nicht offensichtlich ist und die Unvollständigkeit von Informationen nicht erkannt wird.

G 4.18 Entladene oder überalterte Notstromversorgung im Anrufbeantworter
Bei Anrufbeantwortern mit einem digitalen Speicher wird der Ausfall der Netzenergieversorgung durch Batterie oder Akkumulator überbrückt, um so den Speicherinhalt zu erhalten. Ist die Kapazität von Batterie oder Akkumulator vor Ende der Netzunterbrechung erschöpft, werden in der Regel der Ansagetext und zusätzlich bei digitaler Anrufaufzeichnung auch die bereits aufgesprochenen Nachrichten gelöscht.

G 4.19 Informationsverlust bei erschöpftem Speichermedium
Ist das Speichermedium (digitaler Speicher oder Audiokassette) des Anrufbeantworters mit aufgezeichneten Anrufen erschöpft, so ist eine weitere Aufzeichnung entweder nicht mehr möglich oder vorher aufgesprochene Nachrichten werden durch neue Anrufe überschrieben. In beiden Fällen entsteht ein Informationsverlust.

G 4.20 Datenverlust bei erschöpftem Speichermedium
Jedes Speichermedium kann nur begrenzt viele Daten aufnehmen. Wenn diese Grenze erreicht ist, kann das zu Datenverlusten führen, aber auch dazu, daß Dienste nicht mehr verfügbar sind, wie z.B. daß

- Benutzer keine Daten mehr abspeichern können,
- eingehende E-Mail abgewiesen wird, oder
- keine Protokollierung mehr möglich ist bzw. daß noch nicht ausgewertete Protokolldaten überschrieben werden.

Die Kapazität des Speichermediums kann aus verschiedenen Gründen plötzlich erschöpft sein, z.B. durch Fehler in Anwendungsprogrammen, erhöhten Speicherbedarf der Benutzer oder auch

durch einen gezielten Angriff, bei dem vorsätzlich der vorhandene Speicherplatz reduziert wird, um eine Protokollierung zu verhindern.

G 4.21 Ausgleichsströme auf Schirmungen
Werden IT-Geräte, die über ein TN-C-Netz elektrisch versorgt werden, durch Datenleitungen mit beidseitig aufgelegtem Schirm miteinander verbunden, kann es zu Ausgleichsströmen auf dem Schirm kommen (eine erläuternde Zeichnung findet man in M 1.39 Verhinderung von Ausgleichsströmen auf Schirmungen).
Ursache dafür ist die Eigenart des TN-C-Netzes, daß bei ihm Schutz- (PE-) und Neutral- (N-) Leiter bis zu den einzelnen Verteilungen gemeinsam als PEN-Leiter geführt werden. Erst in der Verteilung erfolgt die Aufteilung in N-Leiter und PE-Leiter. Diese Installation ist gemäß VDE 0100 zulässig! Werden die mit PE verbundenen Schnittstellen-Schirmungen von Geräten, die an verschiedenen Verteilungen angeschlossen sind, durch geschirmte Datenleitungen miteinander verbunden, kommt es zu einer Parallelschaltung des PEN-Leiters zwischen den Verteilungen und der Schirmung zwischen den Schnittstellen. Der dadurch über die Schirmung fließende Ausgleichsstrom kann zu Schäden an den Schnittstellen und zu Personengefährdungen bei Arbeiten an den Datenleitungen führen.
Zwischen Geräten, die in einem TN-C-Netz an der gleichen Verteilung oder zwischen Geräten, die in einem TN-S-Netz - auch an verschiedenen Verteilungen - angeschlossen sind, fließen keine Ausgleichsströme über die Schirmung von Datenleitungen.
Bei TN-CS-Netzen sind einige Teilbereiche als TN-C-Netz, andere als TN-S-Netz ausgeführt. Solange Datenleitungen mit beidseitig aufgelegtem Schirm nur jeweils innerhalb gleichartiger Teilbereiche geführt werden, gelten dort die gleichen Verhältnisse wie in den jeweiligen Netzen. Werden jedoch IT-Geräte aus unterschiedlichen Bereichen über Datenleitungen mit beidseitig aufgelegter Schirmung verbunden, können auch im TN-S-Bereich Ausgleichsströme fließen!

G 4.22 Schwachstellen oder Fehler in Standardsoftware
Wie für jede Software gilt auch für Standardsoftware: je komplexer sie ist, desto häufiger treten Programmierfehler auf. Es ist zu beobachten, daß hohe Erwartungen der Anwender und zeitlich zu knapp bemessene Erscheinungstermine bei Standardsoftwareprodukten auch dazu führen, daß die Hersteller ihre Produkte teilweise unausgereift oder nicht fehlerfrei anbieten. Werden diese Softwarefehler nicht erkannt, können die bei der Anwendung entstehenden Fehler zu weitreichenden Folgen führen.

G 4.23 Automatische CD-ROM-Erkennung
Bei eingeschalteter CD-ROM-Erkennung unter Windows 95 oder Windows NT werden CD-ROMs automatisch erkannt und die Datei AUTORUN.INF automatisch ausgeführt, wenn diese sich im Wurzelverzeichnis der CD-ROM befindet. Diese Datei kann beliebige auf der CD-ROM gespeicherte Programme (z.B. mit Schadfunktion) automatisch ausführen.
Ob diese Option eingeschaltet ist, erkennt man zum Beispiel unter Windows 95 daran, daß der Explorer vor dem CD-ROM-Laufwerksbuchstaben den Namen der CD-ROM automatisch einblendet. Ein Nebeneffekt hierbei ist, daß Energiespar-Funktionen in der Regel nicht mehr aktiviert werden.

G 4.24 Dateinamenkonvertierung bei Datensicherungen unter Windows 95
Werden zur Datensicherung unter Windows 95 Programme benutzt, die lange Dateinamen nicht unterstützen, so sind alle langen Dateinamen vor der Datensicherung mit dem zum Lieferumfang von Windows 95 gehörenden Programm LFNBK.EXE und der Option /B in die 8.3er-Konvention zu konvertieren. Anschließend ist das Datensicherungsprogramm aufzurufen. Schließlich sind die ursprünglichen Dateinamen mit LFNBK.EXE /R wieder herzustellen.
Dieses Verfahren ist jedoch mit Vorsicht anzuwenden, da zum einen bei der Namenskonvertierung Informationen verloren gehen können, zum anderen sich Dateien nicht mehr herstellen lassen, sobald sich die Verzeichnisstruktur nach der Datensicherung auf diesem PC geändert hat. Dies kann dann einen Datenverlust zur Folge haben.

G 4.25 Nicht getrennte Verbindungen
Bei der Verwendung von ISDN-Kommunikationskarten kann es vorkommen, daß eine über die Kommunikations-Software ausgelöste Verbindung nicht tatsächlich durch die ISDN-Karte getrennt wird. Besteht der Verdacht eines solchen Defekts, läßt sich dieser durch einen Anrufversuch bei der betreffenden ISDN-Rufnummer leicht verifizieren.

G 4.26 Ausfall einer Datenbank
Steht eine Datenbank, z.B. aufgrund von Hardware- oder Software-Problemen bzw. durch Sabotage, nicht mehr zur Verfügung, so kann dies je nach Einsatzzweck und Bedeutung der Datenbank weitreichende Folgen haben. Sämtliche Anwendungen, die auf die Daten der Datenbank angewiesen sind, können nicht mehr benutzt werden und fallen ebenfalls aus. Die Benutzer solcher Anwendungen können ihre Aufgaben nur noch teilweise oder gar nicht mehr wahrnehmen, falls sie diese nicht mit manuellen Mitteln erfüllen können. Je nach Art der Aufgaben, die nur mittels IT-Unterstützung unter Benutzung der Datenbank ausgeführt werden können, sind folgende Konsequenzen möglich:

- wirtschaftlicher Schaden,
- Sicherheitsrisiken, die bis hin zu Beeinträchtigungen im persönlichen Bereich führen können (z.B. bei medizinischen Datenbanken),
- bedingte oder komplette Handlungsunfähigkeit.

G 4.27 Unterlaufen von Zugriffskontrollen über ODBC
Existierende Zugangs- oder Zugriffskontrollen einer Datenbank können unterlaufen werden, wenn auf die Datenbank außerhalb einer Anwendung über ODBC (Open Database Connectivity) zugegriffen wird und bei der Installation der ODBC-Treiber Fehler gemacht wurden. In diesem Fall kann ein Schutz vertraulicher Daten nicht mehr gewährleistet werden, ebenso ist auch die Manipulation von Daten ohne weiteres möglich.

G 4.28 Verlust von Daten einer Datenbank
Ein Verlust von Daten einer Datenbank kann auf vielfältige Art und Weise verursacht werden.

Dies kann sich von ungewollten Datenmanipulationen (z.B. durch das unbeabsichtigte Löschen von Daten) über einen Verlust durch einen Crash der Datenbank bis hin zu gezielten Angriffen erstrecken. Dadurch ist die Verfügbarkeit und die Vollständigkeit der Daten nicht mehr gewährleistet, und es kann zu folgenden Konsequenzen kommen:

- Bestimmte Anwendungen, die auf die Daten der Datenbank angewiesen sind, können ggf. nicht mehr oder nicht mehr in vollem Umfang ausgeführt werden.
- Der Informationsgehalt der Daten in ihrer Gesamtheit geht verloren.
- Es entsteht ein hoher Aufwand, um die zerstörten Daten wiederzubeschaffen.

Je nach Ursache des Datenverlustes kann es schwer bis unmöglich sein festzustellen, welche Daten nicht mehr vorhanden sind. Dies kann weitere wirtschaftliche Schäden oder Sicherheitsrisiken nach sich ziehen.

G 4.29 Datenverlust einer Datenbank bei erschöpftem Speichermedium
Jedes Speichermedium kann nur begrenzt viele Daten aufnehmen. Dies gilt auch für eine Datenbank, die für die dauerhafte Speicherung ihrer Daten auf ein physikalisches Speichermedium zurückgreifen muß. Ist dieses erschöpft, kann es zu einem Crash der Datenbank und einem Verlust von Daten kommen. Die sich daraus ergebenden Konsequenzen werden in G 4.28 Verlust von Daten einer Datenbank beschrieben.
Die Kapazität des Speichermediums kann aus verschiedenen Gründen plötzlich erschöpft sein, z.B. durch Fehler in Anwendungsprogrammen, erhöhtem Speicherbedarf der Benutzer oder auch durch einen gezielten Angriff, bei dem vorsätzlich der vorhandene Speicherplatz reduziert wird, um z.B. eine Protokollierung zu verhindern.

G 4.30 Verlust der Datenbankintegrität/-konsistenz
Ein Verlust der Datenbankintegrität/-konsistenz bedeutet, daß die Daten in der Datenbank zwar noch vorhanden sind, aber einen fehlerhaften oder sinnlosen Wert angenommen haben. Dadurch können die Daten nicht mehr korrekt verarbeitet werden. Dies kann auf vielfältige Art und Weise verursacht werden, von ungewollten Datenmanipulationen (z.B. durch das unbeabsichtigte Ändern von Daten) über eine fehlerhafte Synchronisationskontrolle der Transaktionen bis hin zu gezielten Angriffen.
Dadurch kann es zu folgenden Konsequenzen kommen:

- Bestimmte Aufgaben, die auf die korrekten Daten der Datenbank angewiesen sind, können ggf. nicht mehr oder nicht mehr in vollem Umfang durchgeführt werden.
- Der Informationsgehalt der Daten in ihrer Gesamtheit wird verfälscht.
- Es entsteht ein hoher Aufwand, um die Datenintegrität und Datenkonsistenz der Datenbank wiederherzustellen.

Je nach Ursache der Verletzung der Datenbankintegrität/-konsistenz kann es schwer bis unmöglich sein festzustellen, welche Daten verändert wurden. Dies kann weitere wirtschaftliche

Schäden oder Sicherheitsrisiken nach sich ziehen.

G 4.32 Nichtzustellung einer Nachricht
Der Datenaustausch über E-Mail ist schnell und komfortabel, aber nicht immer sehr zuverlässig. Aufgrund von Hardware- oder Softwarefehlern bei den beteiligten IT-Systemen oder durch Störungen auf dem Übertragungsweg kommt es immer wieder zum Nachrichtenverlust. Die technischen Probleme können vielfältige Ursachen haben, z.B. können Leitungen beschädigt sein, Netzkopplungselemente ausfallen oder die Kommunikationssoftware falsch konfiguriert sein. E-Mails können auch verloren gehen, weil die Empfängeradresse nicht korrekt angegeben war. Dabei ist das größte Problem, daß die Benutzer häufig nicht über die unterbliebene Zustellung der E-Mail informiert werden. Auf eine automatisierte Unterrichtung bei einer unterbliebenen Zustellung kann nicht vertraut werden.
Viele E-Mail-Programme bieten Optionen wie „Zustellung bestätigen“ oder „Empfang bestätigen“. Entsprechende Rückmeldungen sollten aber nicht überbewertet werden. Zum einen werden die Zustellbestätigungen häufig nicht durch die Ankunft einer E-Mail am Bildschirmarbeitsplatz des Empfängers ausgelöst wird, sondern durch die Ankunft bei einem Mailserver. Ob der Mailserver die E-Mail erfolgreich an den Adressaten weitergeleitet hat, wird dann nicht mehr mitgeteilt. Zum anderen erfolgt auch häufig keine Zustellbestätigung, obwohl die E-Mail korrekt übertragen wurde, wenn diese Option durch die Empfängerseite nicht unterstützt wird.

G.5 Gefährdungskatalog Vorsätzliche Handlungen

G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
Außentäter, aber auch Innentäter, können aus unterschiedlichen Beweggründen (Rache, Böswilligkeit, Frust) heraus versuchen, IT-Geräte, Zubehör, Schriftstücke oder ähnliches zu manipulieren oder zu zerstören. Die Manipulationen können dabei umso wirkungsvoller sein, je später sie entdeckt werden, je umfassender die Kenntnisse des Täters sind und je tiefgreifender die Auswirkungen auf einen Arbeitsvorgang sind. Die Auswirkungen reichen von der unerlaubten Einsichtnahme in schützenswerte Daten bis hin zur Zerstörung von Datenträgern oder IT-Systemen, die erhebliche Ausfallzeiten nach sich ziehen können.

G 5.2 Manipulation an Daten oder Software
Daten oder Software können auf vielfältige Weise manipuliert werden: durch falsches Erfassen von Daten, Änderungen von Zugriffsrechten, inhaltliche Änderung von Abrechnungsdaten oder von Schriftverkehr, Änderungen in der Betriebssystemsoftware und vieles mehr. Ein Täter kann allerdings nur die Daten und Software manipulieren, auf die er Zugriff hat. Je mehr Zugriffsrechte eine Person besitzt, desto schwerwiegendere Manipulationen kann sie vornehmen. Falls die Manipulationen nicht frühzeitig erkannt werden, kann der reibungslose IT-Einsatz empfindlich gestört werden.
Manipulationen an Daten oder Software können aus Rachegefühlen, um einen Schaden mutwillig zu erzeugen, zur Verschaffung persönlicher Vorteile oder zur Bereicherung vorgenommen werden.

G 5.3 Unbefugtes Eindringen in ein Gebäude

Das unbefugte Eindringen in ein Gebäude geht verschiedenen Gefährdungen der IT wie Diebstahl oder Manipulation voraus. Maßnahmen, die dagegen gerichtet sind, wirken dadurch auch gegen die entsprechenden Folgegefährdungen. Schon durch das unbefugte Eindringen können Sachschäden entstehen. Fenster und Türen werden gewaltsam geöffnet und dabei beschädigt, sie müssen repariert oder ersetzt werden.

G 5.4 Diebstahl

Durch den Diebstahl von IT-Geräten, Zubehör, Software oder Daten entstehen einerseits Kosten für die Wiederbeschaffung sowie für die Wiederherstellung eines arbeitsfähigen Zustandes, andererseits Verluste aufgrund mangelnder Verfügbarkeit. Darüber hinaus können Schäden durch einen Vertraulichkeitsverlust und daraus resultierenden Konsequenzen entstehen.

G 5.5 Vandalismus

Vandalismus ist dem Anschlag sehr verwandt, nur daß er nicht wie dieser gezielt eingesetzt wird, sondern meist Ausdruck blinder Zerstörungswut ist.
Sowohl Außentäter (z.B. enttäuschte Einbrecher, außer Kontrolle geratene Demonstrationen) als auch Innentäter (z.B. frustrierte oder alkoholisierte Mitarbeiter) kommen in Betracht. Die tatsächliche Gefährdung durch Vandalismus ist schwerer abschätzbar als die eines Anschlages, da ihm in der Regel keine zielgerichtete Motivation zugrunde liegt. Persönliche Probleme oder ein schlechtes Betriebsklima können dabei Ursachen sein.

G 5.6 Anschlag

Die technischen Möglichkeiten, einen Anschlag zu verüben, sind vielfältig: geworfene Ziegelsteine, Explosion durch Sprengstoff, Schußwaffengebrauch, Brandstiftung. Ob und in welchem Umfang ein IT-Betreiber der Gefahr eines Anschlages ausgesetzt ist, hängt neben der Lage und dem Umfeld des Gebäudes stark von seinen Aufgaben und vom politisch-sozialen Klima ab. IT-Betreiber in politisch kontrovers diskutierten Bereichen sind stärker bedroht als andere. IT-Betreiber in der Nähe üblicher Demonstrationsaufmarschgebiete sind stärker gefährdet als solche in abgelegenen Randbereichen. Für die Einschätzung der Gefährdung durch politisch motivierte Anschläge können die Landeskriminalämter oder das Bundeskriminalamt beratend hinzugezogen werden.

G 5.7 Abhören von Leitungen

Wegen des geringen Entdeckungsrisikos ist das Abhören von Leitungen eine nicht zu vernachlässigende Gefährdung der IT-Sicherheit. Grundsätzlich gibt es keine abhörsicheren Kabel. Lediglich der erforderliche Aufwand zum Abhören unterscheidet die Kabel. Ob eine Leitung tatsächlich abgehört wird, ist nur mit hohem meßtechnischen Aufwand feststellbar.
Der Entschluß, eine Leitung abzuhören, wird im wesentlichen durch die Frage bestimmt, ob die Informationen den technischen (kostenmäßigen) Aufwand und das Risiko der Entdeckung wert sind. Die Beantwortung dieser Frage ist sehr von den individuellen Möglichkeiten und Interessen des Angreifers abhängig. Somit ist eine sichere Festlegung, welche Informationen

und damit Leitungen ggf. abgehört werden, nicht möglich.

G 5.8 Manipulation an Leitungen
Neben dem Abhören von Leitungen (siehe G 5.7 - Abhören von Leitungen) kann eine Manipulation an Leitungen noch andere Ziele haben:

- Frustrierte Mitarbeiter manipulieren Leitungen so, daß es zu unzulässigen Verbindungen innerhalb und außerhalb der eigenen IT kommt. Dabei geht es oft nur darum, den IT-Betrieb zu stören.
- Leitungen können so manipuliert werden, daß eine private Nutzung zu Lasten des Netzbetreibers erfolgen kann. Neben den dadurch entstehenden Kosten bei der Nutzung gebührenpflichtiger Verbindungen werden Leitungen und Ressourcen durch die private Nutzung blockiert.
- Durch die Manipulation von Leitungen kann es möglich werden, darauf übertragene Daten zum Vorteil des Täters zu verändern. Insbesondere bei kassenwirksamen Verfahren, in der Lohnbuchhaltung und bei allen IT-Anwendungen, die sich direkt oder indirekt mit der Verwaltung von Sachwerten befassen, können sich durch Manipulationen hohe Schäden ergeben.

G 5.9 Unberechtigte IT-Nutzung
Ohne Mechanismen zur Identifikation und Authentisierung von Benutzern ist die Kontrolle über unberechtigte IT-Nutzung praktisch nicht möglich. Selbst bei IT-Systemen mit einer Identifikations- und Authentisierungsfunktion in Form von Benutzer-ID- und Paßwort-Prüfung ist eine unberechtigte Nutzung denkbar, wenn Paßwort und zugehörige Benutzer-ID ausgespäht werden.
Um das geheimgehaltene Paßwort zu erraten, können Unbefugte innerhalb der Login-Funktion ein mögliches Paßwort eingeben. Die Reaktion des IT-Systems gibt anschließend Aufschluß darüber, ob das Paßwort korrekt war oder nicht. Auf diese Weise können Paßwörter durch Ausprobieren erraten werden.
Viel erfolgversprechender ist jedoch die Attacke, ein sinnvolles Wort als Paßwort anzunehmen und alle Benutzereinträge durchzuprobieren. Bei entsprechend großer Benutzeranzahl wird damit oft eine gültige Kombination gefunden.
Falls die Identifikations- und Authentisierungsfunktion mißbräuchlich nutzbar ist, so können sogar automatisch Versuche gestartet werden, indem ein Programm erstellt wird, das systematisch alle möglichen Paßwörter testet.

G 5.10 Mißbrauch von Fernwartungszugängen
Bei unzureichend gesicherten Fernwartungszugängen ist es denkbar, daß Hacker Zugang zum Administrierungsport des IT-Systems erlangen. Sie können somit nach Überwindung des Anlagenpaßwortes ggf. alle Administrationstätigkeiten ausüben. Der entstehende Schaden kann sich vom vollständigen Anlagenausfall, über schwerste Betriebsstörungen, den Verlust der Vertraulichkeit aller auf der Anlage vorhandenen Daten bis hin zum großen direkten finanziellen

Schaden erstrecken.

G 5.11 Vertraulichkeitsverlust in TK-Anlagen gespeicherter Daten
In TK-Anlagen werden personenbezogene und firmen-/behördeninterne Daten für längere Zeit auf Festplatten gespeichert. Personenbezogene Daten sind hierbei Gebührendaten, Konfigurationsdaten, Berechtigungen und ggf. Daten für die elektronischen Telefonbücher, Paßworte und Verrechnungsnummern.
Diese Daten können durch das Administrationspersonal eingesehen und verändert werden. Art und Umfang dieser Eingriffe sind vom Anlagentyp und, falls vorgesehen, von der Rechtevergabe abhängig. Das Administrationspersonal hat diese Möglichkeit sowohl vor Ort als auch über Fernwartung. Bei einer externen Fernwartung hat der damit Beauftragte (im Regelfall der Hersteller) jederzeit diese Möglichkeit!
Bei einer Aktualisierung der Anlagensoftware werden die Festplatten oft zu den TK-Anlagen-Herstellern gebracht. Personenbezogene Daten können dann vom Hersteller ausgelesen werden.

G 5.12 Abhören von Telefongesprächen und Datenübertragungen
Durch mißbräuchliche Verwendung von Leistungsmerkmalen können Gespräche unter Umständen im Kollegenkreis mitgehört werden. Als Beispiel hierfür kann die Dreierkonferenz genannt werden. Erhält der Teilnehmer A einen Anruf für den Teilnehmer B, so könnte er, anstatt den Anruf zu übergeben, versuchen, heimlich eine Dreierkonferenz herzustellen. Besitzt Teilnehmer B ein Telefon ohne Display, würde er diese Tatsache nicht bemerken.
Desweiteren könnten Gespräche durch das Aktivieren von gesperrten, in Deutschland zum Teil unzulässigen Leistungsmerkmalen von Dritten mitgehört werden. Als ein Beispiel sei hier nur die Zeugenschaltung erwähnt. Eine derartige Aktivierung erfordert genauere Systemkenntnisse.

G 5.13 Abhören von Räumen
Grundsätzlich müssen zwei Varianten des unbefugten Abhörens von Räumen unterschieden werden. Bei der ersten Variante geht die Bedrohung ausschließlich vom Endgerät aus. Hier sind intelligente Endgeräte mit eingebauten Mikrofonen wie Anrufbeantworter oder ISDN-Karten bzw. Multimedia-PCs zu nennen. Solche Endgeräte können, wenn entsprechende Funktionalitäten implementiert sind, aus der Ferne, d.h. aus dem öffentlichen Netz, dazu veranlaßt werden, die eingebauten Mikrofone freizuschalten. Ein bekanntes Beispiel hierfür ist die sogenannte „Baby-Watch-Funktion“ von Anrufbeantwortern (vgl. Kapitel 8.3 - Anrufbeantworter).
Die zweite Variante ist die Ausnutzung der Funktionalität der TK-Anlage selbst in Verbindung mit entsprechend ausgerüsteten Endgeräten. Diese Gefährdung entsteht durch die mißbräuchliche Verwendung des Leistungsmerkmals „direktes Ansprechen“ in Kombination mit der Option „Freisprechen“. Die auf diese Weise realisierbare Funktion einer Wechselsprechanlage kann unter gewissen Umständen auch zum Abhören eines Raumes ausgenutzt werden.

G 5.14 Gebührenbetrug
In letzter Zeit waren vermehrt Meldungen über Gebührenbetrug an TK-Anlagen durch Hacker in der Presse zu lesen. Solche Manipulationen sind auf verschiedene Weisen durchführbar. Zum einen kann versucht werden, vorhandene Leistungsmerkmale einer TK-Anlage für diese Zwecke

zu mißbrauchen. Geeignet hierfür sind beispielsweise aus der Ferne umprogrammierbare Rufumleitungen oder Dial-In-Optionen. Zum anderen können die Berechtigungen so vergeben werden, daß kommende „Amtsleitungen“ abgehende „Amtsleitungen“ belegen können. Auf diese Weise kann bei Anwahl einer bestimmten Rufnummer von außen der Anrufer automatisch wieder mit dem „Amt“ verbunden werden, wobei dies allerdings auf Kosten des TK-Anlagenbetreibers geschieht.
Eine weitere Art des Gebührenbetruges ist der durch den Benutzer selbst. Auf unterschiedliche Arten, wie z.B. durch das Telefonieren von fremden Apparaten, Auslesen fremder Berechtigungscodes (Paßwort) oder Verändern der persönlichen Berechtigungen kann versucht werden, auf Kosten des Arbeitgebers oder der anderen Beschäftigten zu telefonieren.

G 5.15 „Neugierige“ Mitarbeiter
„Neugierige“ Mitarbeiter könnten durch Mißbrauch von Leistungsmerkmalen der TK-Anlage versuchen:

- Anrufe für Kollegen auf ihren eigenen Telefonapparat umzuleiten,
- die Anrufe für andere anzunehmen,
- fremde Anruf- und Wahlwiederholspeicher auszulesen und
- Telefongespräche Dritter mitzuhören.

G 5.16 Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Personal
Zum eigenen Vorteil oder aus Gefälligkeit für Kollegen könnte bei Wartungs- oder Administrationsarbeiten durch internes Personal versucht werden, Berechtigungen (z.B. Auslandsberechtigung) zu ändern oder Leistungsmerkmale zu aktivieren. Durch Unkenntnis können Systemabstürze verursacht werden. Ferner können durch unsachgemäße Handhabung der Hardwarekomponenten diese u.U. zerstört werden. Zusätzlich hat das Wartungspersonal vollen oder eingeschränkten Zugriff auf die gespeicherten Daten (lesend und schreibend).

G 5.17 Gefährdung bei Wartungsarbeiten durch externes Personal
Ein IT-System kann bei Wartungsarbeiten auf jedwede Weise manipuliert werden. Die Gefahr besteht in erster Linie darin, daß der Eigentümer oft nicht in der Lage ist, die vorgenommenen Modifikationen nachzuvollziehen. Darüber hinaus hat der externe Wartungstechniker genau wie der interne auch üblicherweise Zugriff auf alle auf der Anlage gespeicherten Daten.

G 5.18 Systematisches Ausprobieren von Paßwörtern
Zu einfache Paßwörter lassen sich durch systematisches Ausprobieren herausfinden. Beispiel: Eine Untersuchung von Klein (Klein, Daniel V. 1990, USENIX Security Workshop Proceedings, Portland August 1990) an 15000 Accounts ergab eine Erfolgsquote von 24,2 % , wobei folgende Möglichkeiten für ein Paßwort ausprobiert wurden:
ca. 130 Variationen des Login Namens (Vor- und Zuname) und anderer persönlicher Daten

aus dem /etc/passwd File, häufige Namen, Namen von bekannten Personen, Namen und Orte aus Filmen, von Sportereignissen und aus der Bibel, gebräuchliche Schimpfwörter und Wörter aus Fremdsprachen, verschiedene Variationen dieser Wörter, wie z.B. Umwandlung Groß-Kleinschreibung, Einfügen von Sonder- und Kontrollzeichen, Umkehrung der Buchstabenreihenfolge, wiederholte Buchstaben (z.B. aaabbb) oder häufige Abkürzungen (z.B. rggbv für die Farben des Regenbogens) und Paare aus zwei kurzen Wörtern.
Alle diese Kombinationen und mehr lassen sich mit Hilfe des Public Domain Programms crack von jedem Benutzer eines Unix-Systems, auf dem die Paßwortdatei frei zugänglich ist, ausprobieren. Darüber hinaus ist die Wahrscheinlichkeit, ein Paßwort durch systematisches Probieren aller Kombinationen zu finden, bei zu kurzen Paßwörtern groß.

G 5.19 Mißbrauch von Benutzerrechten
Eine mißbräuchliche Nutzung liegt vor, wenn man vorsätzlich recht- oder unrechtmäßig erworbene Möglichkeiten ausnutzt, um dem System oder dessen Benutzern zu schaden.

G 5.20 Mißbrauch von Administratorrechten
Eine mißbräuchliche Administration liegt vor, wenn man vorsätzlich recht- oder unrechtmäßig erworbene Super-User- (root-) Privilegien ausnutzt, um dem System oder dessen Benutzern zu schaden.
Beispiel: Da root auf Unix-Anlagen keinerlei Beschränkungen unterliegt, kann der Administrator unabhängig von Zugriffsrechten jede Datei lesen, verändern oder löschen. Außerdem kann er die Identität jedes Benutzers seines Systems annehmen, ohne daß dies von einem anderen Benutzer bemerkt wird, es ist ihm also z. B. möglich unter fremden Namen Mails zu verschicken oder fremde Mails zu lesen und zu löschen.
Es gibt verschiedene Möglichkeiten, mißbräuchlich Super-User-Privilegien auszunutzen. Dazu gehören der Mißbrauch von falsch administrierten Super-User-Dateien (Dateien mit Eigentümer root und gesetztem s-Bit) und des Befehls su.
Die Gefährdung kann auch durch automatisches Mounten von austauschbaren Datenträgern entstehen: Sobald das Medium in das Laufwerk gelegt wird, wird es gemountet. Dann hat jeder Zugriff auf die dortigen Dateien. Mit sich auf dem gemounteten Laufwerk befindenden s-Bit-Programmen kann jeder Benutzer Super-User-Rechte erlangen.
In Abhängigkeit von der Unix-Variante und der zugrundeliegenden Hardware kann bei Zugangsmöglichkeit zur Konsole der Monitor-Modus aktiviert oder in den Single-User-Modus gebootet werden. Das ermöglicht die Manipulation der Konfiguration.

G 5.21 Trojanische Pferde
Ein Trojanisches Pferd ist ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung. Der Anwender kann daher auf die Ausführung dieser Funktion keinen Einfluß nehmen, insoweit besteht eine gewisse Verwandtschaft mit Computer-Viren. Es ist jedoch keine Selbstreproduktion vorhanden. Als Träger für Trojanische Pferde lassen sich alle möglichen Anwenderprogramme benutzen. Aber auch Scriptsprachen, wie Batch-Dateien, Ansi-Steuersequenzen, Postscript u.ä., die vom jeweiligen Betriebssystem oder Anwenderprogramm interpretiert werden, können für Trojanische Pferde mißbraucht werden.

Die Schadwirkung eines Trojanischen Pferdes ist um so wirkungsvoller, je mehr Rechte sein Trägerprogramm besitzt.

G 5.22 Diebstahl bei mobiler Nutzung des IT-Systems
Wird ein IT-System mobil genutzt, so ergeben sich aus der Mobilität heraus neue Gefährdungen, die stationäre IT-Systeme in dem Maße nicht berühren. Mobile Systeme wie Laptops werden üblicherweise nicht in einem durch Schutzvorkehrungen gesicherten Raum eingesetzt. Sie werden in Kraftfahrzeugen oder öffentlichen Verkehrsmitteln transportiert, in fremden Büroräumen in Pausen hinterlassen oder in Hotelzimmern unbewacht aufgestellt.
Aufgrund dieser Umfeldbedingungen sind solche mobil eingesetzten IT-Systeme naturgemäß einem höheren Diebstahlrisiko ausgesetzt. Der im Kofferraum eines PKW eingeschlossene Laptop kann gestohlen werden, ohne daß dies das originäre Ziel des Diebstahl ist, denn mit dem gestohlenen Wagen würde auch der Laptop in die falschen Hände geraten.

G 5.23 Computer-Viren
Computer-Viren gehören zu den Programmen mit Schadensfunktionen. Als Schaden ist hier insbesondere der Verlust oder die Verfälschung von Daten oder Programmen sicherlich von größter Tragweite. Solche Funktionen von Programmen können sowohl unbeabsichtigt als auch bewußt gesteuert auftreten.
Die Definition eines Computer-Virus bezieht sich nicht unmittelbar auf eine möglicherweise programmierte Schadensfunktion: Ein Computer-Virus ist eine nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. (Zusätzlich können programmierte Schadensfunktionen des Virus vorhanden sein.)
Es werden drei Grundtypen von Computer-Viren unterschieden:

- Boot-Viren
- Datei-Viren
- Makro-Viren

Es sind auch Misch- und Sonderformen dieser drei Typen bekannt. Weitere Unterteilungsmerkmale sind die Tarnmechanismen, mit denen die Viren oft gegen die Erkennung durch Anwender und Suchprogramme geschützt sind.

Boot-Viren
Als „Booten“ bezeichnet man das Laden des Betriebssystems. Hierbei werden u.a. Programmteile ausgeführt, die zwar eigenständig sind, sich aber in sonst nicht zugänglichen und im Inhaltsverzeichnis der Disketten und Festplatten nicht sichtbaren Sektoren befinden. Boot-Viren überschreiben diese mit ihrem Programm. Der originale Inhalt wird an eine andere Stelle auf dem Datenträger verlagert und dann beim Start des Computers anschließend an den Virus-Code ausgeführt. Dadurch startet der Computer scheinbar wie gewohnt. Der Boot-Virus gelangt jedoch bereits vor dem Laden des Betriebssystems in den Arbeitsspeicher des Computers und verbleibt dort während der gesamten Betriebszeit. Er kann deshalb den Boot-Sektor jeder nicht

schreibgeschützten Diskette infizieren, die während des Rechnerbetriebs benutzt wird. Boot-Viren können sich nur durch Booten oder einen Bootversuch mit einer infizierten Diskette auf andere Computer übertragen.

Datei-Viren
Die meisten Datei-Viren lagern sich an Programmdateien an. Auch hier wird beim Aufruf der Virus-Code i.allg. ausgeführt und erst anschließend das originale Programm unverändert. Datei-Viren verbreiten sich durch Aufruf eines infizierten Programms. Bei den Mischformen von Boot- und Datei-Viren haben sogenannte multipartite Viren eine größere Bedeutung erlangt, die sich sowohl durch Aufruf eines infizierten Programms als auch durch Booten (oder einen Boot-Versuch) von einer infizierten Diskette verbreiten können.

Makro-Viren
Auch Makro-Viren sind in Dateien enthalten, diese infizieren jedoch nicht die Anwendungsprogramme, sondern die damit erzeugten Dateien. Betroffen sind alle Anwendungsprogramme, bei denen in die erzeugten Dateien nicht nur einzelne Steuerzeichen, sondern auch Programme und andere Objekte eingebettet werden können. Davon sind insbesondere Microsoft Word- und Excel-Dateien betroffen. Bei diesen steht eine leistungsfähige Programmiersprache für Makros zur Verfügung, die auch von weniger geschulten Anwendern leicht zur Programmierung von Viren mißbraucht werden kann (siehe auch G 5.43 - Makro-Viren).
Die Gefährdung durch Makro-Viren ist inzwischen größer als die durch Boot- und Datei-Viren.

G 5.24 Wiedereinspielen von Nachrichten
Angreifer zeichnen bei diesem Angriff eine Nachricht auf und spielen diese Information zu einem späteren Zeitpunkt unverändert wieder ein.

G 5.25 Maskerade
Die Maskerade benutzt ein Angreifer um eine falsche Identität vorzutäuschen. Eine falsche Identität erlangt er z.B. durch das Ausspähen von Benutzer-ID und Paßwort (siehe G 5.9 - Unberechtigte IT-Nutzung), die Manipulation des Absenderfeldes einer Nachricht, durch die Manipulation einer Kartenadresse im Netz oder durch die Manipulation der Rufnummernanzeige (Calling Line Identification Presentation) im ISDN.
Ein Benutzer, der über die Identität seines Kommunikationspartners getäuscht wurde, kann leicht dazu gebracht werden, schutzbedürftige Informationen zu offenbaren.
Ein Angreifer kann durch eine Maskerade auch versuchen, sich in eine bereits bestehende Verbindung einzuhängen, ohne sich selber authentisieren zu müssen, da dieser Schritt bereits von den originären Kommunikationsteilnehmern durchlaufen wurde.

G 5.26 Analyse des Nachrichtenflusses
Über eine Verkehrsflußanalyse versucht ein Angreifer Auskunft darüber zu erhalten, wer wann welche Datenmengen an wen gesendet hat und wie oft. Sogar wenn der Lauscher die Nachrichteninhalte nicht lesen kann, können hierdurch Rückschlüsse auf das Benutzerverhalten gezogen werden. Die Informationen über Datum und Uhrzeit der Erstellung einer Nachricht können

zu einem Persönlichkeitsprofil des Absenders ausgewertet werden. Daneben forschen Adreßsammler für Adreßverlage nach E-Mail- und Post-Adressen, um unaufgefordert Werbung zuzuschicken.
Innerhalb des ISDN (Integrated Services Digital Network) wäre der D-Kanal einer Kommunikationsverbindung, welcher der Signalisierung zwischen Endgerät und Vermittlungsstelle dient, ein geeigneter Angriffspunkt. Die Analyse der dort übertragenen Signalisierung mittels eines Protokollanalysators läßt nicht nur die o.a. Rückschlüsse auf das Benutzerverhalten zu (z.B. wer telefoniert wann mit wem wie lange?), sondern kann auch der Vorbereitung komplexerer Angriffe über den D-Kanal dienen.

G 5.27 Nichtanerkennung einer Nachricht
Ein Kommunikationsteilnehmer kann den Nachrichtenempfang ableugnen (Non-Repudiation of Receipt). Dies ist insbesondere bei finanziellen Transaktionen von Bedeutung.

G 5.28 Verhinderung von Diensten
Ein solcher Angriff zielt darauf ab, die IT-Benutzer daran zu hindern, Funktionen oder Geräte zu benutzen, die ihnen normalerweise zur Verfügung stehen. Dieser Angriff steht häufig im Zusammenhang mit verteilten Ressourcen, indem ein Angreifer diese Ressourcen so stark in Anspruch nimmt, daß andere Benutzer an der Arbeit gehindert werden. Es können z. B. die folgenden Ressourcen künstlich verknappt werden: Prozesse, CPU-Zeit, Plattenplatz, Inodes, Verzeichnisse.
Dies kann z.B. geschehen durch

- das Starten von beliebig vielen Programmen gleichzeitig,
- das mehrfache Starten von Programmen, die viel CPU-Zeit verbrauchen,
- das Belegen aller freien Inodes in einem Unix-System, so daß keine neuen Dateien mehr angelegt werden können,
- das Anlegen sehr vieler kleiner Dateien in einem Verzeichnis auf einem DOS-PC, so daß in diesem Verzeichnis keine neuen Dateien mehr angelegt werden können,
- die gezielte Überlastung des Netzes,
- das Kappen von Netzverbindungen.

G 5.29 Unberechtigtes Kopieren der Datenträger
Werden Datenträger ausgetauscht oder transportiert, so bedeutet dies unter Umständen, daß die zu übermittelnden Informationen aus einer gesicherten Umgebung heraus über einen unsicheren Transportweg in eine ggf. unsichere Umgebung beim Empfänger übertragen werden. Unbefugte können sich in solchen Fällen diese Informationen dort durch Kopieren einfacher beschaffen, als es in der ursprünglichen Umgebung der Fall war.

G 5.30 Unbefugte Nutzung eines Fax-Gerätes
Der unberechtigte Zugang zu einem Fax-Gerät kann für manipulative Zwecke ausgenutzt werden. Dabei können neben den Kosten für die Fax-Übertragung (Gebühren und Material) auch Schäden dadurch entstehen, daß ein Unbefugter vorgibt, das Gerät als Berechtigter zu nutzen (Schreiben mit Firmenkopf vom entsprechenden Fax-Anschluß).

G 5.31 Unbefugtes Lesen eingegangener Fax-Sendungen
Werden Fax-Geräte in frei zugänglichen Bereichen aufgestellt, können eingehende Fax-Sendungen von jedem gelesen werden. Vertrauliche Informationen können so bekannt werden, ihren Wert verlieren oder zum Schaden des Empfängers genutzt werden.

G 5.32 Auswertung von Restinformationen in Fax-Geräten
Abhängig vom technischen Verfahren, mit denen Fax-Geräte Informationen speichern, weiterverarbeiten oder drucken, können sich nach dem Fax-Empfang Restinformationen unterschiedlichen Umfanges im Fax-Gerät befinden. Sie können wiederhergestellt werden, wenn man in den Besitz des Gerätes oder der entsprechenden Bauteile kommt.
Bei Fax-Geräten, die mittels des Thermotransferverfahrens drucken, werden eingehende Fax-Sendungen zunächst auf eine Zwischenträgerfolie geschrieben, mit deren Hilfe sie dann ausgedruckt werden. Diese Folie ist Verbrauchsmaterial und muß regelmäßig ausgetauscht werden, das Entfernen der Folie ist daher leicht möglich. Gelangt ein Unbefugter in den Besitz dieser Folie (durch Diebstahl oder bei der Entsorgung), kann er den Inhalt mit einfachen technischen Mitteln reproduzieren. Dabei können ihm die Informationen von mehreren hundert Fax-Seiten bekannt werden. Die meisten Fax-Geräte verfügen über einen Zwischenspeicher (Puffer), der mehrere Fax-Seiten enthalten kann, und der u. U. von jedem, der Zugang zum Fax-Gerät hat, ausgedruckt werden kann.

G 5.33 Vortäuschen eines falschen Absenders bei Fax-Geräten
So wie man einen Brief unter falschem Namen und mit falschem Briefkopf schreiben kann, kann man auch ein entsprechend gefälschtes Fax versenden. Dadurch können Schäden entstehen, wenn der Empfänger die darin enthaltenen Informationen als authentisch und ggf. als rechtsverbindlich ansieht (vgl. G 3.14 - Fehleinschätzung der Rechtsverbindlichkeit eines Fax).

G 5.34 Absichtliches Umprogrammieren der Zieltasten eines Fax-Gerätes
Um häufig wiederkehrende Fax-Empfängernummern nicht ständig neu eingeben zu müssen, bieten einige Fax-Geräte programmierbare Zielnummerntasten an. Häufig werden die Empfängernummern beim Versenden des Fax nicht einmal mehr kontrolliert. Kann ein Unbefugter die Programmierung der Zieltasten ändern und veranlaßt er dann noch, daß die bei der neuen Zieladresse eingehenden Fax-Sendungen möglichst unverzüglich zum berechtigten Empfänger weitergeleitet werden, kann er bequem den Fax-Verkehr zu diesem Empfänger mitverfolgen, ggf. ohne jemals entdeckt zu werden.

G 5.35 Überlastung durch eingehende Fax-Sendungen
Eine Überlastung durch eingehende Fax-Sendungen kann entstehen, wenn nicht genügend Fax-

Anschlüsse vorhanden sind. Darüber hinaus kann ein Fax-Anschluß absichtlich blockiert werden, indem

- andauernd umfangreiche Faxe (ggf. mit sinnlosem Inhalt) zugesandt werden oder
- absichtlich solange Faxe zugesandt werden, bis der Papiervorrat des Fax-Gerätes und der Pufferspeicher aufgebraucht sind.

G 5.39 Eindringen in Rechnersysteme über Kommunikationskarten
Eine Kommunikationskarte (z.B. eine ISDN-Karte oder ein internes Modem, aber auch ein externes Modem) kann eingehende Anrufe automatisch entgegennehmen. Abhängig von der eingesetzten Kommunikationssoftware und deren Konfiguration besteht dann die Möglichkeit, daß ein Anrufer unbemerkt Zugriff auf das angeschlossene IT-System nehmen kann.
Über eine Kommunikationskarte kann ein externer Rechner als Terminal an einen Server angeschlossen werden. Falls der Benutzer sich nach einer Terminalsitzung abmeldet, aber die Leitung ansonsten bestehen bleibt, ist vom externen Rechner ein Zugang wie über ein lokales Terminal möglich. Damit haben Dritte, die Zugang zu diesem Rechner haben, die Möglichkeit, Benutzerkennungen und Paßwörter zu testen. Wesentlich gefährlicher ist der Fall, daß die Verbindung unterbrochen wird, aber der Benutzer nicht automatisch am entfernten System ausgeloggt wird. Dann kann der nächste Anrufer unter dieser Benutzerkennung weiterarbeiten, ohne sich anmelden zu müssen. Er hat somit vollen Zugriff auf das IT-System, ohne sich identifiziert und authentisiert zu haben.

G 5.40 Abhören von Räumen mittels Rechner mit Mikrofon
Viele IT-Systeme werden mittlerweile mit Mikrofon ausgeliefert. Das Mikrofon eines vernetzten Rechners kann von denjenigen benutzt werden, die über Zugriffsrechte auf die entsprechende Gerätedateien verfügen (unter Unix ist das zum Beispiel /dev/audio, unter Windows NT ist es ein Eintrag in der Registrierung). Wenn diese Rechte nicht sorgfältig vergeben sind und dadurch auch andere als die vorgesehenen Benutzer Zugriff haben, kann das Mikrofon zum Abhören mißbraucht werden.

G 5.41 Mißbräuchliche Nutzung eines Unix-Systems mit Hilfe von uucp
Das Programmpaket UUCP (Unix-to-Unix Copy) erlaubt den Austausch von ASCII- und Binärdateien zwischen IT-Systemen und die Ausführung von Kommandos auf entfernten IT-Systemen. UUCP war ursprünglich auf Unix-Systeme beschränkt, ist aber mittlerweile auch für viele andere Betriebssysteme verfügbar. Bei der Kommunikation über UUCP werden IT-Benutzern auf entfernten Rechnern Rechte auf dem lokalen Rechner eingeräumt. Wenn diese Rechte nicht sorgfältig und auf das Notwendige beschränkt vergeben werden, besteht die Gefahr der mißbräuchlichen Nutzung des lokalen Systems. Denkbar ist auch eine Maskerade über UUCP, indem z.B. ein Host - bei Kenntnis des Paßworts - vorgetäuscht wird.

G 5.42 Social Engineering
Social Engineering ist eine Methode, um nicht allgemein zugängliche Informationen durch „Aushorchen“ zu erlangen. Oft gibt sich ein Angreifer bei Gesprächen durch die Kenntnisse der

richtigen Schlagworte als Insider zu erkennen und erhält so zusätzliche Informationen, die an anderer Stelle ausgenutzt werden können.
Das „Aushorchen“ kann z. B. per Telefonanruf erfolgen, bei dem sich jemand ausgibt:

- als Vorzimmerkraft, deren Vorgesetzter schnell noch etwas erledigen will, aber sein Paßwort vergessen hat und es jetzt dringend braucht,
- als Administrator, der wegen eines Systemfehlers anruft, da er zur Fehlerbehebung noch das Paßwort des Benutzers benötigt,
- als Telefonentstörer, der einige technische Details wissen will, z.B. unter welcher Rufnummer ein Modem angeschlossen ist und welche Einstellungen es hat,
- als Externer, der gerne Herrn X sprechen möchte, der aber nicht erreichbar ist. Die Information, daß Herr X drei Tage abwesend ist, sagt ihm auch gleichzeitig, daß der Account von Herrn X in dieser Zeit nicht benutzt wird, also unbeobachtet ist.

Wenn kritische Rückfragen kommen, ist der Neugierige angeblich „nur eine Aushilfe“ oder eine „wichtige“ Persönlichkeit.

G 5.43 Makro-Viren
Mit dem Austausch von Dateien (z.B. per Datenträger oder E-Mail) besteht die Gefahr, daß neben der eigentlichen Datei (Textdatei, Tabelle etc.) weitere, mit dem Dokument verbundene Makros bzw. eingebettete Editorkommandos übersandt werden. Diese Makros laufen erst mit dem jeweiligen Anwendungsprogramm (Winword, Excel etc.) bei der Bearbeitung des Dokuments ab, indem der Anwender das Makro aktiviert bzw. das Makro automatisch gestartet wird. Wird ein Dokument über einen WWW-Browser empfangen, der das Dokument automatisch öffnet, kann hierdurch ein (Auto-) Makro aktiviert werden.
Da die Makrosprachen über einen sehr umfangreichen Befehlssatz verfügen, besteht auch die Gefahr, daß einem Dokument ein Makro beigefügt wird, das eine Schadfunktion enthält (z.B. einen Virus).
In der Praxis hat diese Gefährdung insbesondere bei den Dateien der Programme Word für Windows und Excel der Firma Microsoft im Jahr 1996 weltweit beträchtlich zugenommen. Für den Anwender ist dabei nicht transparent, daß Dateien für Word-Vorlagen (*.DOT), in denen Makros enthalten sein können, durch Umbenennen in *.DOC-Dateien scheinbar zu Datendateien werden, die keine Makros enthalten. Von Word werden solche Dateien jedoch ohne Hinweis auf diese Tatsache in nahezu gleicher Weise verarbeitet (Ausnahme: Winword ab Version 7.0a). Die Word-Makro-Viren haben inzwischen die Spitzenstellung bei gemeldeten Infektionen eingenommen. Hervorzuheben ist, daß die Makro-Viren auf verschiedenen Betriebssystem-Plattformen auftreten können, nämlich auf allen, auf denen WINWORD läuft (Windows Versionen 3.1 und 3.11, Windows 95, Windows NT, Apple-Computer).

G 5.44 Mißbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlagen
TK-Anlagen verfügen über Remote-Zugänge für Managementfunktionen. Über diese Zugänge

können alle Administrations- und Wartungstätigkeiten sowie sonstige Managementfunktionalitäten wie z. B. Alarmsignalisierung und -bearbeitung abgewickelt werden.
Solche Remote-Zugänge sind besonders in TK-Anlagen-Verbünden (Corporate Networks) nützlich und teilweise unverzichtbar. Bei der Art des Remote Zuganges läßt sich zwischen

- ModemZugang über dedizierte Managementports und
- direkte Einwahl über DISA (Direct Inward System Access)

unterscheiden. Desweiteren sind in neueren Protokollierungsverfahren wie QSig und einigen anderen proprietären Protokollen Managementfunktionen bereits im Signalisierungsspektrum enthalten. Hieraus ergeben sich potentielle Mißbrauchsmöglichkeiten.
Bei unzureichend gesicherten Fernwartungszugängen ist es denkbar, daß Hacker Zugang zu den Managementprogrammen des TK-Systems erlangen. Sie können somit nach Überwindung des Anlagenpaßwortes ggf. alle Administrationstätigkeiten ausüben. Der entstehende Schaden kann sich vom vollständigen Anlagenausfall, über schwerste Betriebsstörungen, den Verlust der Vertraulichkeit aller auf der Anlage vorhandenen Daten bis hin zum großen direkten finanziellen Schaden z. B. durch Gebührenbetrug erstrecken.

G 5.48 IP-Spoofing

IP-Spoofing ist eine Angriffsmethode, bei der falsche IP-Nummern verwendet werden, um dem angegriffenen IT-System eine falsche Identität vorzuspielen.
Bei vielen Protokollen der TCP/IP-Familie erfolgt die Authentisierung der kommunizierenden IT-Systeme nur über die IP-Adresse, die aber leicht gefälscht werden kann. Nutzt man darüber hinaus noch aus, daß die von den Rechnern zur Synchronisation beim Aufbau einer TCP/IP-Verbindung benutzten Sequenznummern leicht zu erraten sind, ist es möglich, Pakete mit jeder beliebigen Absenderadresse zu verschicken. Damit können entsprechend konfigurierte Dienste wie rlogin benutzt werden. Allerdings muß ein Angreifer dabei u.U. in Kauf nehmen, daß er kein Antwortpaket von dem mißbräuchlich benutzten Rechner erhält.
Weitere Dienste, die durch IP-Spoofing bedroht werden, sind rsh, rexec, X-Windows, RPC-basierende Dienste wie NFS und der TCP-Wrapper, der ansonsten ein sehr sinnvoller Dienst zur Einrichtung einer Zugangskontrolle für TCP/IP-vernetzte Systeme ist. Leider sind auch die in Schicht 2 des OSI-Modells eingesetzten Adressen wie Ethernet- oder Hardware-Adressen leicht zu fälschen und bieten somit für eine Authentisierung keine zuverlässige Grundlage.
In LANs, in denen das Address Resolution Protocol (ARP) eingesetzt wird, sind sehr viel wirkungsvollere Spoofing-Angriffe möglich. ARP dient dazu, zu einer 32-Bit großen IP-Adresse die zugehörige 48-Bit große Hardware- oder Ethernet-Adresse zu finden. Falls in einer internen Tabelle des Rechners kein entsprechender Eintrag gefunden wird, wird ein ARP-Broadcast-Paket mit der unbekannten IP-Nummer ausgesandt. Der Rechner mit dieser IP-Nummer sendet dann ein ARP-Antwort-Paket mit seiner Hardware-Adresse zurück. Da die ARP-Antwort-Pakete nicht manipulationssicher sind, reicht es dann meist schon, die Kontrolle über einen der Rechner im LAN zu bekommen, um das gesamte Netz zu kompromittieren.

G 5.49 Mißbrauch des Source-Routing

Der Mißbrauch des Routing-Mechanismus und -Protokolls ist eine sehr einfache protokoll-

basierte Angriffsmöglichkeit. In einem IP-Paket läßt sich der Weg, auf dem das Paket sein Ziel erreichen soll oder den die Antwortpakete nehmen sollen, vorschreiben. Die Wegbeschreibung kann aber während der Übertragung manipuliert werden, so daß nicht die durch die Routing Einträge vorgesehenen sicheren Wege benutzt werden (z.B. über die Firewall), sondern andere unkontrollierte Wege.

G 5.50 Mißbrauch des ICMP-Protokolls
Das Internet Control Message Protocol (ICMP) hat als Protokoll der Transportschicht die Aufgabe, Fehler- und Diagnoseinformationen zu transportieren. Es läßt sich in mehrfacher Weise mißbrauchen. Zum einem können über Redirect Pakete die Routingtabellen eines Rechners geändert und z.B. unerwünschte Routen konfiguriert werden. Zum anderen kann ein Angreifer gefälschte Destination Unreachable Pakete in die Verbindung einschleusen, so daß die bestehende Verbindung unterbrochen wird und somit die Verfügbarkeit der Netzverbindung nicht mehr gewährleistet ist.

G 5.51 Mißbrauch der Routingprotokolle
Routing Protokolle wie RIP (Routing Information Protocol) oder OSPF (Open Shortest Path First) dienen dazu, Veränderungen der Routen zwischen zwei vernetzten Systemen an die beteiligten Systeme weiterzuleiten und so eine dynamische Änderung der Routingtabellen zu ermöglichen. Es ist leicht möglich, falsche RIP-Pakete zu erzeugen und somit unerwünschte Routen zu konfigurieren.
Der Einsatz von dynamischem Routing ermöglicht es, Routing-Informationen an einen Rechner zu schicken, die dieser in der Regel ungeprüft zum Aufbau seiner Routingtabellen benutzt. Dies kann ein Angreifer ausnutzen, um gezielt den Übertragungsweg zu verändern.

G 5.52 Mißbrauch von Administratorrechten im Windows NT System
Eine mißbräuchliche Administration liegt vor, wenn man vorsätzlich recht- oder unrechtmäßig erworbene Administrator-Berechtigungen und -Rechte ausnutzt, um dem System oder dessen Benutzern zu schaden.

G 5.53 Bewußte Fehlbedienung von Schutzschränken aus Bequemlichkeit
Eine häufig festzustellende Form der absichtlichen Fehlbedienung von Schutzschränken mit mechanischen Codeschlössern besteht darin, nach Schließen eines Schutzschrankes den Code nicht zu verwerfen, um den Code beim Öffnen nicht wieder eingeben zu müssen. Dieses Fehlverhalten reduziert den Schutzwert des Schrankes gegen unbefugten Zugriff, da hierdurch einem Dritten das Öffnen des Schutzschrankes ohne Kenntnis des Codes ermöglicht wird.
Ebenso häufig anzutreffen ist der Umstand, daß Schutzschränke bei kurzfristigem Verlassen des Raumes nicht verschlossen werden, um sich das Öffnen des Schrankes nach Rückkehr zu ersparen. Dies reduziert ebenfalls den Schutzwert gegen unbefugten Zugriff.

G 5.52 Mißbrauch von Administratorrechten im Windows NT System
Eine mißbräuchliche Administration liegt vor, wenn man vorsätzlich recht- oder unrechtmäßig erworbene Administrator-Berechtigungen und -Rechte ausnutzt, um dem System oder dessen

Benutzern zu schaden.
Beispiel: Durch mißbräuchliche Nutzung des Rechtes zur Besitzübernahme beliebiger Dateien kann sich ein Administrator unter Windows NT Zugriff auf beliebige Dateien verschaffen, obwohl deren Eigentümer ihm diesen Zugriff explizit durch entsprechende Zugriffskontrollen verwehrt hat. Eine Zugriffsübernahme kann allerdings vom ursprünglichen Eigentümer der Dateien erkannt werden, da der Administrator sich hierbei zum Besitzer der betreffenden Dateien machen muß und unter Windows NT keine Funktion verfügbar ist, um diese Änderung wieder rückgängig zu machen. Trotzdem kann der Administrator unbemerkt auf Benutzerdateien zugreifen, in dem er sich z.B. in die Gruppe Sicherungs-Operatoren einträgt und ein Backup der Dateien durchführt, die er lesen will.
Es gibt verschiedene Möglichkeiten, mißbräuchlich Administrator-Rechte auszunutzen. Dazu gehören unzulässige Zugriffe auf Dateien, Veränderungen der Protokollierungs-Einstellungen und der Vorgaben für Benutzerkonten. Andere Möglichkeiten des Mißbrauchs bestehen in der Fälschung von Protokollinformationen durch Verstellen der Systemzeit oder in der detaillierten Verfolgung der Tätigkeiten einzelner Benutzer.
In Abhängigkeit von der zugrundeliegenden Hardware kann bei Zugangsmöglichkeit zur Konsole bzw. zum Systemgehäuse das System gebootet werden. Das ermöglicht ggf. die Manipulation der Konfiguration, wenn hierbei von einem Fremdmedium gebootet oder ein anderes Betriebssystem ausgewählt werden kann.

G 5.60 Umgehen der Systemrichtlinien
Besteht lokaler Zugang zu einem nicht vernetzten PC unter Windows 95, ist es möglich, die Paßwortdatei (name.PWL), die zu einer bestimmten Benutzerkennung gehört, zu löschen. Der Zugang mit dieser Benutzerkennung ist dann ohne Kenntnis des Benutzerpaßwortes möglich. Dies ist insbesondere dann kritisch, wenn ein nicht vernetzter Windows 95-Rechner durch Systemrichtlinien für bestimmte Benutzer eingeschränkt ist, aber eine Administrator-Kennung (z. B. ADMIN) existiert, die alle Rechte besitzt. Durch löschen der ADMIN.PWL durch einen auf diesem PC eingeschränkten, aber dennoch berechtigten Benutzer kann dieser sich anschließend als Administrator anmelden. Die für den Benutzer eingestellten Einschränkungen bzw. Systemrichtlinien werden somit umgangen.

G 5.61 Mißbrauch von Remote-Zugängen für Managementfunktionen von Routern
Router verfügen über Remote-Zugänge für Managementfunktionen. Über diese Zugänge können alle Administrations- und Wartungstätigkeiten sowie Signalisierungsfunktionalitäten abgewickelt werden. Solche Remote-Zugänge sind besonders in größeren Netzen mit mehreren Routern bzw. bei der LAN-Kopplung über Weitverkehrsnetze nützlich und teilweise unverzichtbar.
Bei der Art des Remote-Zugangs läßt sich unterscheiden zwischen:

- ModemZugang über dedizierte Schnittstelle (z. B. V.24) und
- direkter Zugang über reservierte Bandbreiten.

Wird für das Netzmanagement das Protokollverfahren SNMP (Simple Network Management Protocol) eingesetzt, ergeben sich aufgrund fehlender bzw. noch nicht umgesetzter Sicherheits-

funktionalitäten weitere Gefährdungen, die über den direkten Mißbrauch der ungeschützten Remote-Schnittstellen hinausgehen:

- Ein nicht autorisierter Benutzer fängt Datenpakete einer SNMP-Management-Station ab und verändert die darin enthaltenen Parameterwerte für seine Zwecke. Nach dieser Manipulation werden die manipulierten Datenpakete zur eigentlichen Zielstation gesendet. Das Empfängergerät hat keine Möglichkeit, diese Datenmanipulation zu erkennen und reagiert deshalb auf die im Paket enthaltenen Informationen so, als ob diese von der Management-Station direkt abgesandt worden wären.
- Erhält der Besitzer einer Netzmanagement-Station Zugang zum mittels SNMP verwalteten Netz, ist das Vorspiegeln einer Community (Verwaltungsbereich innerhalb von SNMP) möglich. Durch diese Maskerade täuscht ein nicht autorisierter Benutzer eine autorisierte Identität vor und kann alle Informationen der Agents (im Netz zu verwaltende Objekte, bspw. Router) auslesen sowie sämtliche Managementoperationen durchführen. Der Agent hat keine Möglichkeit zwischen der richtigen und der falschen Identität zu unterscheiden.

G 5.62 Mißbrauch von Ressourcen über abgesetzte IT-Systeme
Abgesetzte IT-Systeme (z.B. Telearbeitsplätze) können meist auf vielfältige Ressourcen eines unternehmensweiten Netzes zugreifen. Grundsätzlich besteht deshalb immer die Gefahr des Daten- und Programmdiebstahls.
Bestehen zu einem Unternehmensnetz auch Zugriffsmöglichkeiten von abgesetzten IT-Systemen (z.B. Telearbeitsplätzen), besteht grundsätzlich die Gefahr, daß in dem Unternehmensnetz angebotenen Dienstleistungen mißbraucht werden können. Die Bereitstellung von Kommunikationsservern im Netz (z.B. Fax-Gateway, Internetanbindungen usw.) kann bei einer nicht erlaubten privaten Nutzung zu einem Gebührenbetrug führen.

G 5.63 Manipulationen über den ISDN-D-Kanal
Die Summe aller physikalischen Verbindungen der Kommunikationsteilnehmer zu einer ihnen zugeordneten digitalen Vermittlungsstelle bezeichnet man als Anschlußnetz. Innerhalb des Anschlußnetzes existieren zahlreiche Verteiler und Übergabepunkte, die teilweise frei zugänglich und nicht aufwendig gesichert sind (z.B. Kabelverzweiger). Die Kommunikation auf dem Anschlußnetz kann im einfachsten Fall durch das mechanische Beschädigen einer Anschlußleitung unterbrochen werden. Weiterhin ist es mit Hilfe eines ISDN-Protokollanalysators möglich, Kommunikationsinhalte aufzuzeichnen und auszuwerten. Mittels Einschleifen eines Protokollanalysators ist ebenfalls das Manipulieren von Steuerungsinformationen im D-Kanal des ISDN möglich. Die Kommunikationskomponenten des angegriffenen Kommunikationsteilnehmers (also ISDN-Karten, ISDN-Router, TK-Anlagen etc.) können so zu Reaktionen veranlaßt werden, die ihren ordnungsgemäßen Betrieb beeinträchtigen oder zur Kompromittierung gespeicherter Daten führen.

G 5.64 Manipulation an Daten oder Software bei Datenbanksystemen
Durch ein gezieltes Manipulieren von Daten werden diese vorsätzlich verfälscht oder unbrauchbar gemacht. Die entsprechenden Folgen sind in G 4.28 (Verlust von Daten einer Datenbank)

und G 4.30 (Verlust der Datenbankintegrität/-konsistenz) beschrieben. Werden die Dateien einer Datenbank oder der Datenbankstandardsoftware gezielt gelöscht oder verändert, so führt dies zur vorsätzlichen Zerstörung des gesamten Datenbanksystems (siehe G 4.26 - Ausfall einer Datenbank). Es ist prinzipiell nicht verhinderbar, daß Benutzer mit den entsprechenden Zugangs- und Zugriffsberechtigungen gezielt Datenmanipulationen durchführen oder eine Datenbank zerstören können. Ist es außerdem möglich, die Zugangs- und Zugriffsberechtigungen zu umgehen (z.B. durch eine fehlerhafte Administration des DBMS), so können sich auch unberechtigte Benutzer Zugang zur Datenbank verschaffen und dort Manipulationen vornehmen.

G 5.65 Verhinderung der Dienste eines Datenbanksystems
Ein solcher Angriff zielt darauf ab, die IT-Benutzer daran zu hindern, die Funktionen und Dienste eines Datenbanksystems benutzen zu können, die ihnen normalerweise zur Verfügung stehen. Neben den in G 5.28 (Verhinderung von Diensten) aufgeführten Beispielen, kann dies im Bereich Datenbanken zusätzlich z.B. dadurch erreicht werden, daß große Datenmengen selektiert werden, deren Auswertung das gesamte Datenbanksystem lahmlegt, oder daß die Datensätze durch Sperren blockiert werden.

G 5.69 Erhöhte Diebstahlgefahr am häuslichen Arbeitsplatz
Der häusliche Arbeitsplatz ist in der Regel nicht so abgesichert wie der Arbeitsplatz in einem Unternehmen oder einer Behörde. Dort ist, bedingt durch aufwendigere Vorkehrungen (Verwendung von Sicherheitstüren, Einbruchschutz, Pförtnerdienst usw.) die Gefahr, daß jemand in das Gebäude unbefugt eindringt, weit geringer als bei einem Privathaus.
Einbruch und Diebstahl im Privathaus dienen meist der Bereicherung. Dabei gestohlene dienstliche IT wird mit dem Ziel der Veräußerung gestohlen. Die mitentwendeten Daten können ggf. auch einen Wert darstellen, der zum Beispiel durch Erpressung oder Informationsweitergabe an Konkurrenzunternehmen realisiert werden kann.

G 5.70 Manipulation durch Familienangehörige und Besucher
Am häuslichen Arbeitsplatz ist mit Angehörigen und Besuchern der Familie zu rechnen, so daß die Gefahr besteht, daß bei unzureichender Sicherung die dienstliche IT durch diese manipuliert werden kann. So sollte auch betrachtet werden, daß durch Familienangehörige private Software (z.B. Computerspiele) aufgespielt werden könnte, daß durch Kinder die IT zerstört werden kann oder daß dienstliche Datenträger zweckentfremdet weitergegeben werden können. Diese teils fahrlässigen oder auch absichtlichen Manipulationen können sowohl die Vertraulichkeit und Integrität der dienstlichen Daten betreffen als auch die Verfügbarkeit von Daten und IT beeinträchtigen.

G 5.71 Vertraulichkeitsverlust schützenswerter Informationen
Für Informationen, die einen Schutzbedarf bezüglich Vertraulichkeit besitzen (wie Paßwörter, personenbezogene Daten, firmen- oder amtsvertrauliche Informationen, Entwicklungsdaten), besteht die inhärente Gefahr, daß die Vertraulichkeit durch Unachtsamkeit oder auch durch vorsätzliche Handlungen beeinträchtigt wird. Dabei kann auf diese vertraulichen Informationen an unterschiedlichen Stellen zugegriffen werden, beispielsweise

- auf Speichermedien innerhalb von Rechnern (Festplatten),
- auf austauschbaren Speichermedien (Disketten, Magnetbänder),
- in gedruckter Form auf Papier (Ausdrucke, Akten) und
- auf Übertragungswegen während der Datenübertragung.

Auch die Art und Weise, wie die vertraulichen Informationen gewonnen werden, kann sehr unterschiedlich sein:

- Auslesen von Dateien,
- Kopieren von Dateien,
- Wiedereinspielen von Datensicherungsbeständen,
- Diebstahl des Datenträgers und anschließendes Auswerten,
- Abhören von Übertragungsleitungen und
- Mitlesen am Bildschirm.

Je höher der Vertraulichkeitsbedarf der Informationen ist, umso größer ist auch der Anreiz für Dritte, diese Informationen zu erlangen und zu mißbrauchen.

G 5.72 Mißbräuchliche E-Mail-Nutzung
Der Mißbrauch von E-Mail-Systemen kann an verschiedenen Punkten aufsetzen, beim Benutzer, im internen Netz, bei einem der übertragenden Mailserver oder beim Empfänger.
Wenn der Zugang zum E-Mail-Programm eines Benutzers oder zum E-Mail-System einer Organisation nicht gut genug geschützt ist, kann ein Unbefugter sich unberechtigt Zugang für manipulative Zwecke verschaffen. Dabei können neben den Übertragungskosten auch Schäden dadurch entstehen, daß ein Unbefugter sich als Berechtigter ausgibt.
Ebenso muß verhindert werden, daß E-Mails von Unbefugten gelesen werden können. Vertrauliche Informationen können so bekannt werden, ihren Wert verlieren oder zum Schaden des Empfängers genutzt werden.

G 5.73 Vortäuschen eines falschen Absenders
Es ist relativ einfach, beim Versand von E-Mail einen falschen Absender anzugeben. Dadurch können Schäden entstehen, wenn der Empfänger die darin enthaltenen Informationen als authentisch und verbindlich ansieht.
Beispiel: Mit dem verbreiteten Mailprogramm Eudora ist es ohne Probleme möglich, eine Mail mit gefälschten Absenderangaben ohne Paßwortüberprüfung auf den Mailserver weiterzuleiten. Die so versandte Mail wird bei nicht erfolgter Benutzer-Authentisierung nur im Feld „X-Sender“ mit „Unverified“ gekennzeichnet. Dies wird aber erfahrungsgemäß von kaum einem Empfänger

bemerkt, ohnehin wird dieses Feld von den meisten Mailprogramme in der Standardkonfiguration nicht angezeigt.

G 5.74 Manipulation von Alias-Dateien oder Verteilerlisten
Um häufig wiederkehrende E-Mail-Adressen nicht ständig neu eingeben zu müssen, kann über die Vergabe von Alias-Namen eine „sprechende" Schreibweise für E-Mail-Adressen gewählt werden oder es kann über die Erstellung von Verteilerlisten ein größerer Empfängerkreis komfortabel angewählt werden. Werden solche Alias-Namen oder Verteilerlisten unbefugt geändert, kann auf diese Weise die Weiterleitung einer E-Mail an einen gewünschten Empfänger unterbunden oder die Weiterleitung zu einem unerwünschten Empfänger erfolgen. Besonders gefährdert sind hier Alias-Dateien oder Adreßbücher, die zentral geführt werden.

G 5.75 Überlastung durch eingehende E-Mails
Eine E-Mail-Adresse kann absichtlich blockiert werden, indem andauernd umfangreiche E-Mails (ggf. mit sinnlosem Inhalt) zugesandt werden. Dies kann beispielsweise passieren, weil der Benutzer die Netiquette nicht beachtet hat und sich dadurch in Newsgruppen unbeliebt gemacht hat. Als Netiquette (die Netz-Etiquette) werden die Höflichkeitsregeln bezeichnet, die sich mit der Zeit bei der Nutzung des Internet, insbesondere in den Newsgruppen, eingebürgert haben und deren Einhaltung gewährleisten soll, daß jeder das Internet effizient und zu aller Zufriedenheit benutzen kann.
Durch vorsätzlich erzeugtes hohes Verkehrsaufkommen kann das lokale Mailsystems überlastet werden, so daß es funktionsuntüchtig wird. Dies kann sogar solche Ausmaße annehmen, daß der Provider den Benutzer bzw. dessen ganze Organisation vom Netz nimmt.
Ein Mailsystem kann auch überlastet werden, wenn die Mitarbeiter an E-Mail-Kettenbrief-Aktionen teilnehmen. So hat schon Mitte der achtziger Jahre eine Kettenmail-Aktion zu Weihnachten weltweit viele IT-Systeme lahmgelegt. Hierbei erhielten Benutzer eine E-Mail mit Weihnachtsgrüßen und einer ansprechenden Graphik und wurden aufgefordert, diese E-Mail zu kopieren und zehn andere Benutzer weiterleiten.

G 5.76 Mailbomben
Unter dem Begriff Mailbomben werden E-Mails verstanden, die absichtlich eingebaute Schadfunktionen enthalten. Diese sind üblicherweise in den Anlagen der E-Mail enthalten. Eine solche Anlage erzeugt z.B. beim Aktivieren zum Lesen oder nach dem Auspacken Unmengen von Unterverzeichnissen oder beansprucht sehr viel Festplattenplatz. Vielfach wird auch die gezielte Überlastung von E-Mail-Adressen durch eingehende E-Mails mit meist sinnlosem Inhalt (siehe G 5.75 - Überlastung durch eingehende E-Mails) als Mailbombing bezeichnet.

G 5.77 Mitlesen von E-Mails
Elektronische Post (E-Mail) wird im Normalfall im Klartext übertragen. Auf allen IT-Systemen, über die die Daten übertragen werden, können diese mitgelesen oder unbemerkt verändert werden, wenn sie kryptographisch ungesichert sind. Bei E-Mail über das Internet können das sehr viele IT-Systeme sein, ohne daß der genaue Übertragungsweg vorher bekannt ist. Der Übertragungsweg hängt von der Auslastung und Verfügbarkeit der Gateways und Teilen des Netzes

ab. Eine E-Mail von einem Stadtteil in den anderen kann sogar über das Ausland weitergeleitet werden.
Der Zugriff auf eingehende E-Mails kann auch über die beim Mailserver des Empfängers geführte Mailbox erfolgen. Sie enthält alle empfangenen E-Mails, je nach Konfiguration nicht nur die ungelesenen, sondern ein Archiv aller in den letzten Monaten eingegangenen Nachrichten. Hierauf hat mindestens der Systemadministrator des Mailservers Zugriff. In manchen Fällen werden auch Kopien ausgehender E-Mails auf dem Mail-Server gespeichert, häufiger jedoch legt das Benutzer-Mailprogramm diese auf dem Rechner des Absenders ab.

G 5.78 DNS-Spoofing
Um im Internet mit einem anderen Rechner kommunizieren zu können, benötigt man dessen IP-Adresse. Diese Adresse setzt sich aus vier Zahlen zwischen 0 und 255 zusammen, also zum Beispiel 194.95.176.226. Da solche Nummern nicht sehr einprägsam sind, wird einer solchen IP-Adresse fast immer ein Name zugeordnet. Das Verfahren hierzu nennt sich DNS (Domain Name System). So kann der WWW-Server des BSI sowohl unter http://www.bsi.bund.de als auch unter http://194.95.176.226 angesprochen werden, da der Name bei der Abfrage in die IP-Adresse umgewandelt wird.
Die Datenbanken, in denen den Rechner-Namen die zugehörigen IP-Adressen zugeordnet sind und den IP-Adressen entsprechende Rechnernamen, befinden sich auf sogenannten Nameservern. Für die Zuordnung zwischen Namen und IP-Adressen gibt es zwei Datenbanken: In der einen wird einem Namen seine IP-Adresse zugewiesen und in der anderen einer IP-Adresse der zugehörige Name. Diese Datenbanken müssen miteinander nicht konsistent sein! Von DNS-Spoofing ist die Rede, wenn es einem Angreifer gelingt, die Zuordnung zwischen einem Rechner-Namen und der zugehörigen IP-Adresse zu fälschen, d.h. daß ein Name in eine falsche IP-Adresse bzw. umgekehrt umgewandelt wird.
Dadurch sind unter anderem die folgenden Angriffe möglich:

- r-Dienste (rsh, rlogin, rsh) Diese Dienste erlauben eine Authentisierung anhand des Namens des Clients. Der Server weiß die IP-Adresse des Clients und fragt über DNS nach dessen Namen.

- Web-Spoofing Ein Angreifer könnte die Adresse www.bsi.bund.de einem falschen Rechner zuweisen, und bei Eingabe von http://www.bsi.bund.de würde dieser falsche Rechner angesprochen werden.

Wie leicht es ist, DNS-Spoofing durchzuführen, hängt davon ab, wie das Netz des Angegriffenen konfiguriert ist. Da kein Rechner alle DNS-Informationen der Welt besitzen kann, ist er immer auf Informationen anderer Rechner angewiesen. Um die Häufigkeit von DNS-Abfragen zu verringern, speichern die meisten Nameserver Informationen, die sie von anderen Nameservern erhalten haben, für eine gewisse Zeit zwischen.
Ist ein Angreifer in einen Nameserver eingebrochen, kann er auch die zur Verfügung gestellten Informationen abändern. Der Fall eines direkten Einbruchs auf einen Nameserver soll hier nicht weiter betrachtet werden. Vielmehr geht es darum, prinzipielle Schwächen im DNS aufzuzeigen.

G 5.79 Unberechtigtes Erlangen von Administratorrechten unter Windows NT
Bei jeder Standardinstallation von Windows NT (betrifft sowohl die Versionen Workstation, Server als auch Domänenkontroller) wird ein Administratorkonto angelegt. Im Gegensatz zu selbst angelegten Konten kann dieses vordefinierte Administratorkonto weder gelöscht noch gesperrt werden, um zu verhindern, daß der Administrator vorsätzlich oder versehentlich ausgesperrt wird und somit die Verwaltung unmöglich wird. Problematisch in diesem Zusammenhang ist, daß das vordefinierte Administratorkonto selbst dann nicht gesperrt wird, wenn die in der Kontorichtlinie für eine Sperre eingetragene Anzahl ungültiger Kennworteingaben überschritten wird. Dies ermöglicht das planmäßige Ausprobieren von Paßwörtern unter Einsatz von Crack-Programmen.
Es gibt aber noch weitere Möglichkeiten, um in den Besitz eines zu einem Administratorkonto gehörenden Paßwortes zu kommen, um damit Administratorrechte zu erlangen: Wird ein Rechner unter dem Betriebssystem Windows NT fernadministriert, so besteht die Gefahr, daß beim Authentisierungsvorgang das Anmeldepaßwort im Klartext übertragen und damit von einem Angreifer aufgezeichnet werden kann. Selbst wenn durch Eingriffe in das System sichergestellt ist, daß die Anmeldepaßwörter nur verschlüsselt übertragen werden, ist es möglich, daß ein Angreifer das verschlüsselte Paßword aufzeichnet und mit Hilfe entsprechender Software entschlüsselt. Weiterhin wird jedes Paßwort in der Registrierung und in einer Datei, die sich im Verzeichnis %Systemroot%\System32\Repair bzw. auf den Notfalldisketten und ggf. auf Bandsicherungen befindet, verschlüsselt gespeichert. Gelangt ein Angreifer in den Besitz der entsprechenden Datei, so kann er mit Hilfe entsprechender Software versuchen, das benötigte Paßwort zu entschlüsseln.
Schließlich ist es mit einer speziellen Schadsoftware möglich, daß ein Angreifer auf dem Windows NT Rechner, an dem er lokal angemeldet ist, ein beliebiges Benutzerkonto der Gruppe Administratoren hinzufügt und dem Kontoinhaber damit Administratorrechte verschafft.

Anhang H

Maßnahmenkatalog nach dem BSI-Grundschutzhandbuch

Quellenangabe:
Auszug aus dem BSI - IT-Grundschutzhandbuch 1998 [BSI1998].
Im IT-Grundschutzhandbuch sind zu den Beschreibungen der Gefährdungen oftmals Beispiele angegeben; diese sind aus Platzgründen hier weggelassen worden. Für eine vertiefte Betrachtung wird auf die Quelle verwiesen.

H.1 Maßnahmenkatalog Infrastruktur

M 1.1 Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften
Für nahezu alle Bereiche der Technik gibt es Normen bzw. Vorschriften, z. B. DIN, VDE, VDMA, Richtlinien des VdS. Diese Regelwerke tragen dazu bei, daß technische Einrichtungen ein ausreichendes Maß an Schutz für den Benutzer und Sicherheit für den Betrieb gewährleisten.
Bei der Planung und Errichtung von Gebäuden, bei deren Umbau, beim Einbau technischer Gebäudeausrüstungen (z. B. interne Versorgungsnetze wie Telefon- oder Datennetze) und bei Beschaffung und Betrieb von Geräten sind entsprechende Normen und Vorschriften unbedingt zu beachten.

M 1.2 Regelungen für Zutritt zu Verteilern
Die Verteiler (z.B. für Energieversorgung, Datennetze, Telefonie) sind nach Möglichkeit in Räumen für technische Infrastruktur (Teil 1, Kapitel 4.3.4) unterzubringen. Die dort geforderten Maßnahmen sind zu berücksichtigen.
Der Zutritt zu den Verteilern aller Versorgungseinrichtungen (Strom, Wasser, Gas, Telefon, Gefahrenmeldung, Rohrpost etc.) im Gebäude muß möglich und geordnet sein.
Mit möglich ist gemeint,

- daß Verteiler nicht bei Malerarbeiten mit Farbe oder Tapeten so verklebt werden, daß sie nur noch mit Werkzeug zu öffnen oder unauffindbar sind,
- daß Verteiler nicht mit Möbeln, Geräten, Paletten etc. zugestellt werden,

- daß für verschlossene Verteiler die Schlüssel verfügbar sind und die Schlösser funktionieren.

Mit geordnet ist gemeint, daß festgelegt ist, wer welchen Verteiler öffnen darf. Verteiler sollten verschlossen sein und dürfen nur von den für die jeweilige Versorgungseinrichtung zuständigen Personen geöffnet werden. Die Zugriffsmöglichkeiten können durch unterschiedliche Schließungen und eine entsprechende Schlüsselverwaltung geregelt werden (siehe dazu M 2.14 - Schlüsselverwaltung).
Sind in Verteilern des Stromversorgungsnetzes Schmelzsicherungen eingebaut, sollten entsprechende Ersatzsicherungen (im Verteiler) bereit liegen. Eine Dokumentation der Verteiler ist entsprechend M 2.19 - Neutrale Dokumentation - in den Verteilern auszuführen.
Alle im Verteiler eingebauten Einrichtungen sind exakt und verständlich zu beschriften.

M 1.3 Angepaßte Aufteilung der Stromkreise
Die Raumbelegung und die Anschlußwerte, für die eine Elektroinstallation ausgelegt wurde, stimmen erfahrungsgemäß nach einiger Zeit nicht mehr mit den tatsächlichen Gegebenheiten überein. Es ist also unerläßlich, bei Änderungen der Raumnutzung und bei Änderungen und Ergänzungen der technischen Ausrüstung (IT, Klimatruhe, Beleuchtung etc.) die Elektroinstallation zu prüfen und ggf. anzupassen. Das kann durch Umrangierung von Leitungen geschehen. Andernfalls kann die Neuinstallation von Einspeisung, Leitungen, Verteilern etc. erforderlich werden.

M 1.4 Blitzschutzeinrichtungen
Die direkten Auswirkungen eines Blitzeinschlages auf ein Gebäude (Beschädigung der Bausubstanz, Dachstuhlbrand u.ä.) lassen sich durch die Installation einer Blitzschutzanlage gemäß DIN/VDE 0185 verhindern. Über diesen „Äußeren Blitzschutz“ hinaus ist fast zwingend der „Innere Blitzschutz“, der Überspannungsschutz, erforderlich. Denn der äußere Blitzschutz schützt die elektrischen Betriebsmittel im Gebäude nicht. Dies ist nur durch einen Überspannungsschutz möglich (siehe dazu M 1.25 - Überspannungsschutz), dessen hohe Kosten dem Schutzgut gegenüber gerechtfertigt sein müssen.

M 1.5 Galvanische Trennung von Außenleitungen
Viele hausinterne Netze stehen in direkter galvanischer Verbindung mit Außenleitungen.
Telefon-, Strom- und Datennetze mit DFÜ-Anschlüssen sind davon betroffen, aber auch Gas- und Wasserleitungen.
Über diese Netzanschlüsse können Fremd- und Überspannungen in das Gebäude verschleppt werden. Es gibt eine Reihe von elektrischen, elektronischen oder softwaregestützten Maßnahmen, Netze gegen Einflüsse von außen zu schützen. Ein absolut sicherer Schutz läßt sich aber nicht in allen Fällen garantieren. Hier bleibt nur noch die konsequente galvanische Trennung der Netzübergänge ins Gebäude. Dies kann z.B. durch den Einbau eines Schalters geschehen, der die Leitung nur bei Bedarf durchschaltet (Fernwartung).
Zum Schutz nicht trennbarer Leitungen (Telefon, Daten, Strom, Gas, Wasser) gegen Überspannungen ist die Einrichtung eines Überspannungsschutzes (M 1.25 Überspannungsschutz)

in Erwägung zu ziehen.

M 1.6 Einhaltung von Brandschutzvorschriften und Auflagen der örtlichen Feuerwehr
Die bestehenden Brandschutzvorschriften (z.B. DIN 4102) und die Auflagen der örtlichen Feuerwehr für Gebäude sind unbedingt einzuhalten. Die örtliche Feuerwehr kann bei der Brandschutzplanung hinzugezogen werden. Es ist empfehlenswert, weitere Hinweise zum Brandschutz zu beachten, wie sie zum Beispiel im Merkblatt Räume für EDV-Anlagen"des Verbands der Schadensversicherer (VdS) zu finden sind.

M 1.7 Handfeuerlöscher
Die meisten Brände entstehen aus kleinen, anfangs noch gut beherrschbaren Brandherden. Besonders in Büros findet das Feuer reichlich Nahrung und kann sich sehr schnell ausbreiten. Der Sofortbekämpfung von Bränden kommt also ein sehr hoher Stellenwert zu.
Diese Sofortbekämpfung ist nur möglich, wenn Handfeuerlöscher in der jeweils geeigneten Brandklasse (DIN EN 3) in ausreichender Zahl und Größe (Beratung durch die örtliche Feuerwehr) im Gebäude zur Verfügung stehen. Dabei ist die räumliche Nähe zu schützenswerten Bereichen und Räumen wie Serverraum, Raum mit technischer Infrastruktur, Belegarchiv anzustreben. Pulverlöscher mit Eignung für Brandklasse E bis 1000 V sind für elektrisch betriebene Peripheriegeräte geeignet, für elektronisch gesteuerte Geräte, z.B. Rechner, sollten Kohlendioxyd-Löscher (Brandklasse B) zur Verfügung stehen.
Die Feuerlöscher müssen regelmäßig geprüft und gewartet werden. Die Beschäftigten sollten sich die Standorte des nächsten Feuerlöschers einprägen. Bei entsprechenden Brandschutzübungen sind die Mitarbeiter in die Benutzung der Handfeuerlöscher einzuweisen.

M 1.8 Raumbelegung unter Berücksichtigung von Brandlasten
Eine Brandlast entsteht durch alle brennbaren Stoffe, die ins Gebäude eingebracht werden. Sie ist von der Menge und vom Heizwert der Stoffe abhängig. IT-Geräte und Leitungen stellen ebenso eine Brandlast dar wie Möbel, Fußbodenbeläge und Gardinen. Maximale Brandlasten, standardisierte Heizwerte, weitere Informationen und Bestimmungen sind in der DIN 4102 zusammengestellt.
Bei der Unterbringung von IT-Geräten, Datenträgern etc. sollte eine vorherige Beachtung der vorhandenen Brandlasten im gleichen Raum und in den benachbarten Räumen erfolgen. Z.B. sollte das Datenträgerarchiv nicht in der Nähe von oder über einem Papierlager untergebracht sein.

M 1.9 Brandabschottung von Trassen
Bei Gebäuden mit mehreren Brandabschnitten läßt es sich kaum vermeiden, daß Trassen durch Brandwände und Decken führen. Die Durchbrüche sind nach Verlegung der Leitungen entsprechend dem Brandwiderstandswert der Wand bzw. Decke zu schotten. Um die Nachinstallation zu erleichtern, können geeignete Materialien (z.B. Brandschutzkissen) verwendet werden. Entsprechende VdS-Richtlinien sind zu beachten.

M 1.10 Verwendung von Sicherheitstüren

Sicherheitstüren wie z.B. Stahlblechtüren, bieten gegenüber normalen Bürotüren Vorteile:

- Sie bieten aufgrund ihrer Stabilität (DIN 18 103) einen höheren Schutz gegen Einbruch (z.B. bei Keller- und Lieferanteneingängen) und
- sie verzögern in der Ausführung als selbstschließende feuerhemmende Tür (FH-Tür T30, DIN 18 082) die Ausbreitung eines Brandes.

Der Einsatz von Sicherheitstüren ist über den von der Feuerwehr vorgeschriebenen Bereich hinaus (vgl. M 1.6 - Einhaltung von Brandschutzvorschriften der und Auflagen der örtlichen Feuerwehr) besonders bei schutzbedürftigen Räumen wie Serverraum, Beleg- oder Datenträgerarchiv sinnvoll.

M 1.11 Lagepläne der Versorgungsleitungen

Es sind genaue Lagepläne aller Versorgungsleitungen (Strom, Wasser, Gas, Telefon, Gefahrenmeldung, Rohrpost etc.) im Gebäude und auf dem dazugehörenden Grundstück zu führen und alle die Leitungen betreffenden Sachverhalte aufzunehmen:

- genaue Führung der Leitungen (Einzeichnung in bemaßte Grundriß- und Lagepläne),
- genaue technische Daten (Typ und Abmessung),
- evtl. vorhandene Kennzeichnung,
- Nutzung der Leitungen, Nennung der daran angeschlossenen Netzteilnehmer,
- Gefahrenpunkte und
- vorhandene und zu prüfende Schutzmaßnahmen.

Es muß möglich sein, sich anhand der Pläne einfach und schnell ein genaues Bild der Situation zu machen. Nur so kann das Risiko, daß Leitungen bei Arbeiten versehentlich beschädigt werden, auf ein Mindestmaß reduziert werden. Eine Schadstelle ist schneller zu lokalisieren, die Störung schneller zu beheben.
Es ist sicherzustellen, daß alle Arbeiten an Leitungen rechtzeitig und vollständig dokumentiert werden. Die Pläne sind gesichert aufzubewahren und der Zugriff ist zu regeln, da sie schützenswerte Informationen beinhalten.

M 1.12 Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile

Schützenswerte Gebäudeteile sind z.B. Serverraum, Rechenzentrum, Datenträgerarchiv, Klimazentrale, Verteilungen der Stromversorgung, Schalt- und Rangierräume, Ersatzteillager.
Solche Bereiche sollten keinen Hinweis auf ihre Nutzung tragen. Türschilder wie z.B. RECHENZENTRUM oder EDV-ARCHIV geben einem potentiellen Angreifer, der zum Gebäude Zutritt hat, Hinweise, um seine Aktivitäten gezielter und damit erfolgversprechender vorbereiten zu können.

Ist es unvermeidbar, IT in Räumen oder Gebäudebereichen unterzubringen, die für Fremde leicht von außen einsehbar sind (siehe auch M 1.13 - Anordnung schützenswerter Gebäudeteile), so sind geeignete Maßnahmen zu treffen, um den Einblick zu verhindern oder so zu gestalten, daß die Nutzung nicht offenbar wird. Dabei ist darauf zu achten, daß z.B. nicht nur ein Fenster einer ganzen Etage mit einem Sichtschutz versehen wird.

M 1.13 Anordnung schützenswerter Gebäudeteile
Schützenswerte Räume oder Gebäudeteile sollten nicht in exponierten oder besonders gefährdeten Bereichen untergebracht sein:

- Kellerräume sind durch Wasser gefährdet.
- Räume im Erdgeschoß - zu öffentlichen Verkehrsflächen hin - sind durch Anschlag, Vandalismus und höhere Gewalt (Verkehrsunfälle in Gebäudenähe) gefährdet.
- Räume im Erdgeschoß mit schlecht einsehbaren Höfen sind durch Einbruch und Sabotage gefährdet.
- Räume unterhalb von Flachdächern sind durch eindringendes Regenwasser gefährdet.

Als Faustregel kann man sagen, daß schutzbedürftige Räume oder Bereiche im Zentrum eines Gebäudes besser untergebracht sind als in dessen Außenbereichen.
Optimal ist es, diese Aspekte schon in die Bauplanung für ein neues Gebäude oder in die Raumbelegungsplanung bei Einzug in ein bestehendes einzubeziehen. Bei bereits genutzten Gebäuden wird eine entsprechende Nutzungsanordnung oft mit internen Umzügen verbunden sein. Ersatzweise sollten die sich aus ohnehin erforderlichen Änderungen der Raumbelegung ergebenden Gelegenheiten konsequent genutzt werden.

M 1.14 Selbsttätige Entwässerung
Alle Bereiche, in denen sich Wasser sammeln und stauen kann oder in denen fließendes oder stehendes Wasser nicht oder erst spät entdeckt wird und in denen das Wasser Schäden verursachen kann, sollten mit einer selbsttätigen Entwässerung und ggf. mit Wassermeldern ausgestattet sein. Zu diesen Bereichen gehören u. a.:

- Keller,
- Lufträume unter Doppelböden,
- Lichtschächte,
- Heizungsanlage.

Erfolgt die Entwässerung passiv, also durch Bodengullys direkt in das Abwassersystem des Gebäudes, sind Rückstauklappen unerläßlich. Ohne solche Klappen wird diese Entwässerung zur Wassereintrittsöffnung, wenn das Abwassersystem überlastet wird. Nach extremen Niederschlägen dringt in der Mehrzahl aller Fälle Wasser über diesen Weg in Keller ein. Die

Rückstauklappen müssen regelmäßig auf ihre Funktionstüchtigkeit hin untersucht werden. Ist eine passive Entwässerung nicht möglich, weil das Niveau des Abwassersystems zu hoch ist, können Pumpen eingesetzt werden, die über Schwimmerschalter oder Wassersensoren automatisch eingeschaltet werden. Beim Einsatz dieser Technik sind insbesondere folgende Punkte zu beachten:

- Die Pumpenleistung muß ausreichend bemessen sein.
- Die Druckleitung der Pumpe ist mit einem Rückstauventil auszustatten.
- Es sind Vorkehrungen zu treffen, damit die Pumpe nicht durch mitgeschwämmte Gegenstände blockiert werden kann (Ansaugfilter etc.).
- Das Anlaufen der Pumpe sollte automatisch (z.B. beim Hausmeister oder der Haustechnik) angezeigt werden.
- Die Funktion von Pumpe und Schalter ist regelmäßig zu testen.
- Die Druckleitung der Pumpe darf nicht an eine in unmittelbarer Nähe vorbeigeführte Abwasserleitung angeschlossen werden. Bei einem Leck dieser Leitung würde die Pumpe das Wasser nur ïm Kreis pumpen".

M 1.15 Geschlossene Fenster und Türen
Fenster und nach außen gehende Türen (Balkone, Terrassen) sind in Zeiten, in denen ein Raum nicht besetzt sind, zu schließen. Im Keller- und Erdgeschoß und, je nach Fassadengestaltung, auch in den höheren Etagen bieten sie einem Einbrecher auch während der Betriebszeiten eine ideale Einstiegsmöglichkeit.
Während normaler Arbeitszeiten und sichergestellter kurzer Abwesenheit des Mitarbeiters kann von einer zwingenden Regelung für Büroräume abgesehen werden.

M 1.16 Geeignete Standortauswahl
Bei der Planung des Standortes, an dem ein Gebäude angemietet werden oder entstehen soll, empfiehlt es sich, neben den üblichen Aspekten wie Raumbedarf und Kosten, auch Umfeldgegebenheiten die Einfluß auf die IT-Sicherheit haben zu berücksichtigen:

- In Zusammenhang mit Schwächen in der Bausubstanz kann es durch Erschütterungen naher Verkehrswege (Straße, Eisenbahn, U-Bahn) zu Beeinträchtigungen der IT kommen.
- Gebäude, die direkt an Hauptverkehrstrassen (Bundesbahn, Autobahn, Bundesstraße) liegen, können durch Unfälle beschädigt werden.
- Die Nähe zu optimalen Verkehrs- und somit Fluchtwegen kann die Durchführung eines Anschlages erleichtern.
- In der Nähe von Sendeeinrichtungen kann es zu Störungen der IT kommen.

- In der Nähe von Gewässern und in Niederungen ist mit Hochwasser zu rechnen.
- In der Nähe von Kraftwerken oder Fabriken kann durch Unfälle oder Betriebsstörungen (Explosion, Austritt schädlicher Stoffe) die Verfügbarkeit des Gebäudes (z.B. durch Evakuierung oder großräumige Absperrung) beeinträchtigt werden.

M 1.17 Pförtnerdienst
Die Einrichtung eines Pförtnerdienstes hat weitreichende positive Auswirkungen gegen eine ganze Reihe von Gefährdungen. Voraussetzung ist allerdings, daß bei der Durchführung des Pförtnerdienstes einige Grundprinzipien beachtet werden.

- Der Pförtner beobachtet bzw. kontrolliert alle Personenbewegungen an der Pforte.
- Unbekannte Personen („selbst der neue Chef“) haben sich beim Pförtner zu legitimieren.
- Der Pförtner hält vor Einlaßgewährung eines Besuchers bei dem Besuchten Rückfrage.
- Der Besucher wird zu dem Besuchten begleitet oder an der Pforte abgeholt.
- Dem Pförtner müssen die Mitarbeiter bekannt sein. Scheidet ein Mitarbeiter aus, ist auch der Pförtner zu unterrichten, ab wann diesem Mitarbeiter der Einlaß zu verwehren ist.
- In einem Besucherbuch kann der Zutritt von Fremdpersonen zum Gebäude dokumentiert werden. Die Ausgabe von Besucherausweisen oder Besucherbegleitscheinen ist zu erwägen.

Die Arbeitsbedingungen des Pförtners sind für die Aufgabenwahrnehmung geeignet auszugestalten. Die Aufgabenbeschreibung muß verbindlich festschreiben, welche Aufgaben dem Pförtner im Zusammenspiel mit weiteren Schutzmaßnahmen zukommt (z.B. Gebäudesicherung nach Dienst- oder Geschäftsschluß, Scharfschaltung der Alarmanlage, Kontrolle der Außentüren und Fenster).

M 1.18 Gefahrenmeldeanlage
Ist eine Gefahrenmeldeanlage (GMA) für Einbruch oder Brand vorhanden und läßt sich diese mit vertretbarem Aufwand entsprechend erweitern, ist zu überlegen, ob zumindest die Kernbereiche der IT (Serverräume, Datenträgerarchive, Räume für technische Infrastruktur u.ä.) in die Überwachung durch diese Anlage mit eingebunden werden sollen. So lassen sich Gefährdungen wie Feuer, Einbruch, Diebstahl frühzeitig erkennen und Gegenmaßnahmen einleiten. Um die Schutzwirkung aufrechtzuerhalten, ist eine regelmäßige Wartung und Funktionsprüfung der GMA vorzusehen.
Ist keine GMA vorhanden oder läßt sich die vorhandene nicht nutzen, kommen als Minimallösung lokale Melder in Betracht. Diese arbeiten völlig selbständig, ohne Anschluß an eine Zentrale. Die Alarmierung erfolgt vor Ort oder mittels einer einfachen Zweidrahtleitung (evtl. Telefonleitung) an anderer Stelle.

M 1.19 Einbruchsschutz
Die gängigen Maßnahmen zum Einbruchsschutz sollten den örtlichen Gegebenheiten entsprechend angepaßt werden. Dazu gehören:

- Rolladensicherungen bei einstiegsgefährdeten Türen oder Fenster,
- besondere Schließzylinder, Zusatzschlösser und Riegel,
- Sicherung von Kellerlichtschächten,
- Verschluß von nichtbenutzten Nebeneingängen,
- einbruchgesicherte Notausgänge (soweit seitens der örtlichen Bauaufsicht zugelassen),
- Verschluß von Personen- und Lastenaufzügen außerhalb der Dienstzeit.

Empfehlungen hierzu geben die örtlichen Beratungsstellen der Kriminalpolizei.
Den Mitarbeitern ist durch Regelungen bekanntzugeben, welche Maßnahmen zum Einbruchsschutz beachtet werden müssen.

M 1.20 Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht
Bei der Auswahl von Kabeln ist neben der Berücksichtigung von übertragungstechnischen Notwendigkeiten das Umfeld, in dem die Kabel verlegt werden sollen, zu beachten. Für die meisten Verlegebedingungen gibt es Kabel mit entsprechenden Qualitäten. Die wichtigsten sind hier zusammengestellt:

- Innen- bzw. Außenkabel,
- längswassergeschütztes Kabel für Feucht- oder Naßbereiche,
- zugentlastete Kabel für Freileitungen und extreme Steigungen,
- funktionserhaltende Kabel in feuergefährdeten Bereichen,
- geschirmte Kabel für Bereiche mit starken elektrischen und induktiven Störfeldern,
- gepanzerte Kabel für Fälle, in denen ein ausreichender mechanischer Schutz auf andere Weise nicht realisierbar ist, z.B. bei der provisorischen Verlegung auf Boden und Wänden.

M 1.21 Ausreichende Trassendimensionierung
Kabeltrassen (z.B. Fußbodenkanäle, Fensterbankkanäle, Pritschen, Rohrtrassen im Außenbereich) sind ausreichend zu dimensionieren, d.h., daß einerseits genügend Platz vorhanden ist, um evtl. notwendige Erweiterungen des Netzes vornehmen zu können. Andererseits sind zur Verhinderung des Übersprechens (gegenseitige Beeinflussung von Kabeln) ggf. Mindestabstände zwischen Kabeln einzuhalten.
Ist es aus unterschiedlichen Gründen nicht möglich, Trassen sofort mit ausreichenden Reserven zu errichten, sollte zumindest darauf geachtet werden, daß im Bereich der Trassenführung Platz

ist, um Erweiterungen unterzubringen. Bei der Auslegung von Wand- und Deckendurchbrüchen erspart dies spätere lärm-, schmutz- und kostenintensive Arbeiten.
Diese Maßnahme kann ersetzt werden durch die Auswahl anderer Kabeltypen (M 2.20 - Kontrolle bestehender Verbindungen und M 5.3 - Auswahl geeigneter Kabeltypen unter kommunikationstechnischer Sicht). Durch Verwendung weniger hochadriger Kabel kann gegenüber vielen kleinen Kabeln Platz eingespart werden. Durch den Einsatz von geschirmten Kabeln oder Lichtwellenleitern kann Übersprechen verhindert werden.

M 1.22 Materielle Sicherung von Leitungen und Verteilern
In Räumen mit Publikumsverkehr oder in unübersichtlichen Bereichen eines Gebäudes kann es sinnvoll sein, Leitungen und Verteiler zu sichern. Dies kann auf verschiedene Weise erreicht werden:

- Verlegung der Leitungen unter Putz,
- Verlegung der Leitungen in Stahlpanzerrohr,
- Verlegung der Leitungen in mechanisch festen und abschließbaren Kanälen,
- Verschluß von Verteilern und
- bei Bedarf zusätzlich elektrische Überwachung von Verteilern und Kanälen.

Bei Verschluß sind Regelungen zu treffen, die die Zutrittsrechte, die Verteilung der Schlüssel und die Zugriffsmodalitäten (was muß der Berechtigte ggf. vor dem Zugriff auf Leitungen tun?) festlegen.

M 1.23 Abgeschlossene Türen
Die Türen nicht besetzter Räume sollten abgeschlossen werden. Dadurch wird verhindert, daß Unbefugte Zugriff auf darin befindliche Unterlagen und IT-Einrichtungen erlangen.
In manchen Fällen, z.B. in Großraumbüros, ist der Verschluß des Büros nicht möglich. Dann sollte alternativ jeder Mitarbeiter vor seiner Abwesenheit seine Unterlagen („Clear-Desk-Politik“) und den persönlichen Arbeitsbereich verschließen: Schreibtisch, Schrank und PC (Schloß für Diskettenlaufwerk, Tastaturschloß), Telefon.
Bei laufendem Rechner kann auf das Abschließen der Türen verzichtet werden, wenn eine Sicherungsmaßnahme installiert ist, mit der die Nutzung des Rechners nur unter Eingabe eines Paßwortes weitergeführt werden kann (paßwortunterstützte Bildschirmschoner), der Bildschirm gelöscht wird und wenn das Booten des Rechners die Eingabe eines Paßwortes verlangt.
Bei ausgeschaltetem Rechner kann auf das Verschließen des Büros verzichtet werden, wenn das Booten des Rechners die Eingabe eines Paßwortes verlangt.
Wird in oben genannten Fällen auf das Verschließen der Türen verzichtet, dürfen allerdings keine schutzbedürftigen Gegenstände wie Unterlagen oder Datenträger offen ausliegen.

M 1.24 Vermeidung von wasserführenden Leitungen
In Räumen oder Bereichen, in denen sich IT-Geräte mit zentralen Funktionen (z.B. Server)

befinden, sollten wasserführende Leitungen aller Art vermieden werden. Die einzigen wasserführenden Leitungen sollten, wenn unbedingt erforderlich, Kühlwasserleitungen, Löschwasserleitungen und Heizungsrohre sein. Zuleitungen zu Heizkörpern sollten mit Absperrventilen, möglichst außerhalb des Raumes/Bereiches, versehen werden. Außerhalb der Heizperiode sind diese Ventile zu schließen. Sind Wasserleitungen unvermeidbar, kann als Minimalschutz eine Wasserauffangwanne oder -rinne unter der Leitung angebracht werden, deren Ablauf außerhalb des Raumes führt. Günstig ist es, dazu den Flur zu nutzen, da so ein eventueller Leitungsschaden früher entdeckt wird.
Optional können Wassermelder mit automatisch arbeitenden Magnetventilen eingebaut werden. Diese Magnetventile sind außerhalb des Raumes/Bereiches einzubauen und müssen stromlos geschlossen sein.
Als zusätzliche oder alternative Maßnahme empfiehlt sich ggf. eine selbsttätige Entwässerung (M 1.14 - Selbsttätige Entwässerung).

M 1.25 Überspannungsschutz
Je nach Qualität und Ausbau des Versorgungsnetzes des Energieversorgungsunternehmens und des eigenen Stromleitungsnetzes, abhängig vom Umfeld (andere Stromverbraucher) und von der geographischen Lage, können durch Induktion oder Blitzschlag Überspannungsspitzen im Stromversorgungsnetz entstehen. Überspannungen durch Blitz haben i.d.R. ein recht hohes zerstörerisches Potential, während Überspannungen anderer Ursachen geringer sind, aber trotzdem ausreichen können, um die IT zu stören.
Ein komplettes Überspannungschutzkonzept baut sich in drei Stufen auf:

- der Grobschutz in der Gebäudeeinspeisung,
- der Mittelschutz in den Etagenverteilern und
- der Feinschutz an den jeweiligen Steckdosen und den Steckverbindungen aller anderen Leitungen.

Die Auslegung des Grobschutzes ist von dem Vorhandensein eines äußeren Blitzschutzes abhängig. Die Schutzwirkung jeder Stufe baut auf der vorherigen auf. Der Verzicht auf eine Stufe macht den gesamten Überspannungsschutz nahezu unwirksam.
Ist der gebäudeweite Aufbau eines Überspannungsschutzes nicht möglich, so kann man zumindest wichtige Teile der IT (Server etc.) mit einer entsprechenden Schutzzone umgeben. Netze mit einer Vielzahl angeschlossener Geräte können, um einen möglichen Schaden klein zu halten, durch Optokoppler oder Überspannungsableiter in kleine, gegeneinander geschützte Bereiche aufgeteilt werden.
Zwei Grundvoraussetzungen sind unabhängig von Umfang und Ausbau des Überspannungsschutzes zu beachten:

- Die Leitungslänge zwischen dem Feinschutz und zu schützenden Geräten sollte 20 m nicht überschreiten. Falls doch, ist ein erneuter Feinschutz zwischenzuschalten. Verfügt ein Gerät über einen Feinschutz im Eingang, entfällt die 20 m Begrenzung.

- Für einen funktionierenden Überspannungsschutz ist ein umfassender Potentialausgleich aller in den Überspannungsschutz einbezogenen elektrischen Betriebsmittel erforderlich!

M 1.26 Not-Aus-Schalter
Bei Räumen, in denen elektrische Geräte in der Weise betrieben werden, daß z. B. durch deren Abwärme, durch hohe Gerätedichte oder durch Vorhandensein zusätzlicher Brandlasten ein erhöhtes Brandrisiko besteht, ist die Installation eines Not-Aus-Schalters sinnvoll. Mit Betätigung des Not-Aus-Schalters wird dem Brand eine wesentliche Energiequelle genommen, was bei kleinen Bränden zu deren Verlöschen führen kann. Zumindest ist aber die Gefahr durch elektrische Spannungen beim Löschen des Feuers beseitigt.
Zu beachten ist, daß lokale unterbrechungsfreie Stromversorgungen (USV) nach Ausschalten der externen Stromversorgung die Stromversorgung selbsttätig übernehmen und die angeschlossenen Geräte unter Spannung bleiben. Daher ist bei der Installation eines Not-Aus-Schalters zu beachten, daß auch die USV abgeschaltet und nicht nur von der externen Stromversorgung getrennt wird.
Der Not-Aus-Schalter sollte innerhalb des Raumes neben der Eingangstür (evtl. mit Lagehinweis außen an der Tür) oder außerhalb des Raumes neben der Tür angebracht werden. Dabei ist allerdings zu bedenken, daß dieser Not-Aus-Schalter auch ohne Gefahr versehentlich oder absichtlich betätigt werden kann.

M 1.27 Klimatisierung
Um den zulässigen Betriebstemperaturbereich von IT-Geräten zu gewährleisten, reicht der normale Luft- und Wärmeaustausch eines Raumes manchmal nicht aus, so daß der Einbau einer Klimatisierung erforderlich wird. Deren Aufgabe ist es, die Raumtemperatur durch Kühlung unter dem von der IT vorgegebenen Höchstwert zu halten.
Werden darüber hinaus Forderungen an die Luftfeuchtigkeit gestellt, kann ein Klimagerät durch Be- und Entfeuchtung auch diese erfüllen. Dazu muß das Klimagerät allerdings an eine Wasserleitung angeschlossen werden. M 1.24 - Vermeidung von wasserführenden Leitungen ist zu beachten. Um die Schutzwirkung aufrechtzuerhalten, ist eine regelmäßige Wartung der Klimatisierungseinrichtung vorzusehen.

M 1.28 Lokale unterbrechungsfreie Stromversorgung
Mit einer unterbrechungsfreien Stromversorgung (USV) kann ein kurzzeitiger Stromausfall überbrückt werden oder die Stromversorgung solange aufrechterhalten werden, daß ein geordnetes Herunterfahren angeschlossener Rechner möglich ist. Dies ist insbesondere dann sinnvoll,

- wenn im Rechner umfangreiche Daten zwischengespeichert werden (z.B. Cache-Speicher im Netz-Server), bevor sie auf nichtflüchtige Speicher ausgelagert werden,
- beim Stromausfall ein großes Datenvolumen verloren gehen würde und nachträglich nochmals erfaßt werden müßte,
- wenn die Stabilität der Stromversorgung nicht ausreichend gewährleistet ist. Zwei Arten der USV sind zu unterscheiden:

- Off-Line-USV: Hierbei werden die angeschlossenen Verbraucher im Normalfall direkt aus dem Stromversorgungsnetz gespeist. Erst wenn dieses ausfällt, schaltet sich die USV selbsttätig zu und übernimmt die Versorgung.

- On-Line-USV: Hier ist die USV ständig zwischen Netz und Verbraucher geschaltet. Die gesamte Stromversorgung läuft immer über die USV.

Beide USV-Arten können neben der Überbrückung von Totalausfällen der Stromversorgung und Unterspannungen auch dazu dienen, Überspannungen zu glätten. Auch hier gilt hinsichtlich des Überspannungsschutzes die in M 1.25 - Überspannungsschutz erläuterte Begrenzung auf 20 m.
Werden IT-Geräte in einem Gebäude mit TN-S-Netz (siehe dazu M 1.39 - Verhinderung von Ausgleichsströmen auf Schirmungen) mit einer lokalen USV versorgt, ist folgendes zu beachten: Um die Schutzwirkung des TN-S-Netzes gegen Ausgleichsströme auf Schirmen von Datenleitungen aufrecht zu erhalten, darf der PE-Leiter der Stromzuleitung nicht mit dem PE-Leiter der Ausgangsseite der USV verbunden werden.
Bei der Dimensionierung einer USV kann man i.d.R. von einer üblichen Überbrückungszeit von ca. 10 bis 15 Minuten ausgehen. Die Mehrzahl aller Stromausfälle ist innerhalb von 5 bis 10 Minuten behoben, so daß nach Abwarten dieser Zeitspanne noch 5 Minuten übrigbleiben, um die angeschlossene IT geordnet herunterfahren zu können, sollte der Stromausfall länger andauern. Die meisten modernen USV-Geräte bieten Rechnerschnittstellen an, die nach einer vorher festgelegten Zeit, entsprechend dem Zeitbedarf der IT und der Kapazität der USV, ein rechtzeitiges automatisches Herunterfahren (Shut-down) einleiten können.
Für spezielle Anwendungsfälle (z.B. TK-Anlagen) kann die erforderliche Überbrückungszeit auch mehrere Stunden betragen. Um die Schutzwirkung aufrechtzuerhalten, ist eine regelmäßige Wartung der USV vorzusehen.
Falls die Möglichkeit besteht, die Stromversorgung unterbrechungsfrei aus einer anderen Quelle zu beziehen (z.B. durch Anschluß an eine zentrale USV), so stellt dies eine Alternative zur lokalen USV dar.

M 1.29 Geeignete Aufstellung eines IT-Systems

Bei der Aufstellung eines IT-Systems sollten verschiedene Voraussetzungen beachtet werden, die die Lebensdauer und Zuverlässigkeit der Technik verbessern und die Ergonomie berücksichtigen. Einige seien hier genannt:

- ein IT-System sollte nicht in unmittelbarer Nähe der Heizung aufgestellt werden, um eine Überhitzung zu vermeiden,

- ein IT-System sollte nicht der direkten Sonneneinstrahlung ausgesetzt sein,

- Staub und Verschmutzungen sollten vermieden werden, da die mechanischen Bauteile (Diskettenlaufwerke, mechanische Maus, Festplatten) beeinträchtigt werden können,

- direkte Lichteinstrahlung auf den Bildschirm sollte aus ergonomischen Gründen vermieden werden,

- der Standort in der Nähe eines Fensters oder einer Tür erhöht die Gefahr des Beobachtens von außerhalb. Weitere Hinweise sind den Empfehlungen der Berufsgenossenschaften zu entnehmen.

M 1.30 Absicherung der Datenträger mit TK-Gebührendaten
Auf den TK-Anlagen fallen während des Betriebes Gebührendaten an. Diese enthalten Informationen über:

- Zeit und Datum eines Gespräches,
- Quell- und Zielrufnummer sowie die
- Gesprächsdauer.

Gebührendaten sind personenbezogene Daten im Sinne der einschlägigen Bundes- und Landesdatenschutzgesetze. Hieraus folgt, daß auch nach den im folgenden vorgeschlagenen Maßnahmen des IT-Grundschutzes in jedem Fall eine gesonderte Betrachtung im Hinblick auf die Anforderungen der Datenschutzgesetze (z.B. aus der Anlage zum § 9 Bundesdatenschutzgesetz) durchzuführen ist.
Diese Daten können sowohl auf der Festplatte der TK-Anlage selbst als auch auf einem externen Gebührenrechner gespeichert werden. In vielen Fällen wird es eine Kombination beider Varianten geben. Die Rechner sind - wenn möglich - so zu schützen, daß nur Berechtigte auf die Gebührendaten zugreifen können. Dazu ist es erforderlich, den Gebührenrechner in einem besonders geschützten Raum (vgl. Kapitel 4.3.2 - Serverraum) aufzustellen. Für Einrichtungen, auf denen Gebührendaten gespeichert sind, müssen ferner die Maßnahmen M 1.23 - Abgeschlossene Türen, M 2.5 - Aufgabenverteilung und Funktionstrennung, M 2.6 - Vergabe von Zutrittsberechtigungen, M 2.7 - Vergabe von Zugangsberechtigungen, M 2.8 - Vergabe von Zugriffsrechten, M 2.13 - Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln und M 2.17 - Zutrittsregelung und -kontrolle realisiert werden.

M 1.31 Fernanzeige von Störungen
IT-Geräte und Supportgeräte, die keine oder nur seltene Bedienung durch eine Person erfordern, werden oft in ge- und verschlossenen Räumen untergebracht (z.B. Serverraum). Das führt dazu, daß Störungen, die sich in ihrem Frühstadium auf die IT noch nicht auswirken und einfach zu beheben sind, erst zu spät, meist durch ihre Auswirkungen auf die IT, entdeckt werden. Feuer, Funktionsstörungen einer USV oder der Ausfall eines Klimagerätes seien als Beispiele für solche „schleichenden“ Gefährdungen angeführt.
Durch eine Fernanzeige ist es möglich, solche Störungen früher zu erkennen. Viele Geräte, auf die man sich verlassen muß, ohne sie ständig prüfen oder beobachten zu können, haben heute einen Anschluß für Störungsfernanzeigen. Die technischen Möglichkeiten reichen dabei von einfachen Kontakten, über die eine Warnlampe eingeschaltet werden kann, bis zu Rechnerschnittstellen mit dazugehörigem Softwarepaket für die gängigen Betriebssysteme. Über die Schnittstellen ist es oft sogar möglich, jederzeit den aktuellen Betriebszustand der angeschlossenen Geräte festzustellen und so Ausfällen rechtzeitig begegnen zu können.

M 1.32 Geeignete Aufstellung von Konsole, Geräten mit austauschbaren Datenträgern und Druckern
Diese Maßnahme dient der Absicherung der Schnittstellen eines IT-Systems zur Außenwelt, um auch dort den Sicherheitsanforderungen in bezug auf die gespeicherten und verarbeiteten Daten zu entsprechen, die im IT-System durch die internen Sicherheitsmechanismen und durch die Maßnahmen im Bereich Hardware/Software gewährleistet sind. Der Schutz vor unbefugtem Lesen von Informationen, der innerhalb des Systems durch die Mechanismen der Zugriffskontrolle gegeben ist, muß an diesen Schnittstellen hauptsächlich durch infrastrukturelle oder organisatorische Maßnahmen gewährleistet werden.
Um Manipulationen an der Konsole, an Geräten mit austauschbaren Datenträgern und an Druckern zu verhindern, müssen diese so aufgestellt werden, daß nur Berechtigte Zugang haben. Insbesondere gilt:

- Bei Unix-Systemen dürfen Unbefugte keinen Zugang zur Konsole erhalten, weil sie dort unter Umständen den Unix-Rechner in den Single-User-Modus booten bzw. den Monitor-Modus aktivieren können und damit Systemadministrator-Rechte erlangen.

- Es ist sicherzustellen, daß an den Geräten für austauschbare Datenträger - wie Streamern, Diskettenlaufwerken, Wechselplatten usw. - kein mißbräuchliches Ein- und Auslesen von Dateien möglich ist.

- Nur Berechtigte dürfen Zutritt zu Räumen mit Druckern / Ausdrucken haben. Dieses kann z. B. durch Aufstellung der Drucker in einem geschlossenen Raum und Verteilung der Ausdrucke in nur für den jeweiligen Empfänger zugängliche Fächer durch eine vertrauenswürdige Person erreicht werden. Druckerausgaben müssen daher mit dem Namen des Empfängers gekennzeichnet sein. Dieses kann automatisch durch die Druckprogramme erfolgen.

Diese Maßnahme wird ergänzt durch folgende Maßnahmen:

- M 4.18 - Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus

- M 4.21 - Verhinderung des unautorisierten Erlangens von Administratorrechten

M 1.33 Geeignete Aufbewahrung tragbarer PCs bei mobilem Einsatz
Da die Umfeldbedingungen bei mobilem Einsatz meist außerhalb der direkten Einflußnahme des Benutzers liegen, muß er versuchen, den tragbaren PC auch außer Haus sicher aufzubewahren. Hierfür können nur einige Hinweise gegeben werden, die bei der mobilen Nutzung zu beachten sind:

- Nach Möglichkeit sollten die Zeiten, in denen das Gerät unbeaufsichtigt bleibt, minimiert werden.

- Wird ein tragbarer PC in einem Kraftfahrzeug aufbewahrt, so sollte das Gerät von außen nicht sichtbar sein. Das Abdecken des Gerätes oder das Einschließen in den Kofferraum bieten Abhilfe. Ein tragbarer PC stellt einen hohen Wert dar, der potentielle Diebe anlockt, zumal tragbare PCs leicht veräußert werden können

- Wird der tragbare PC in fremden Büroräumen vor Ort benutzt, so ist dieser Raum nach Möglichkeit auch bei kurzzeitigem Verlassen zu verschließen.

- Wird der Raum für längere Zeit verlassen, sollte zusätzlich der tragbare PC ausgeschaltet werden, um über das Bootpaßwort die unerlaubte Nutzung zu verhindern.

- In Hotelräumen sollte der tragbare PC nicht offen ausliegen. Das Verschließen des Gerätes in einem Schrank behindert Gelegenheitsdiebe.

- Einige neuere Geräte bieten zusätzlich die Möglichkeit zum Anketten des Gerätes. Der Diebstahl setzt dann den Einsatz von Werkzeug voraus.

M 1.34 Geeignete Aufbewahrung tragbarer PCs im stationären Einsatz
Wird ein tragbarer PC zeitweise stationär in einem Büro betrieben, so sind die für ein Büro zutreffenden Maßnahmen zu beachten. Da ein tragbarer PC jedoch besonders leicht zu transportieren und zu verbergen ist, sollte das Gerät außerhalb der Nutzungszeit in einem Schrank verschlossen werden.

M 1.35 Sammelaufbewahrung mehrerer tragbarer PCs
Sind in einer Behörde bzw. einem Unternehmen eine Vielzahl von tragbaren PCs im (mobilen) Einsatz und wechseln die Benutzer häufig, kann es angebracht sein, die zeitweise nicht genutzten tragbaren PCs in einer Sammelaufbewahrung (Pool) zu halten. Der dafür genutzte Raum sollte den Anforderungen an einen Raum für technische Infrastruktur entsprechen.
Darüber hinaus ist die Stromversorgung der tragbaren PCs sicherzustellen, damit die Batterien dieser Geräte den sofortigen Einsatz erlauben. Zusätzlich müssen die Rücknahme und die Ausgabe von tragbaren PCs dokumentiert werden.

M 1.36 Sichere Aufbewahrung der Datenträger vor und nach Versand
Vor dem Versand eines Datenträgers ist zu gewährleisten, daß für den Zeitraum zwischen dem Speichern der Daten auf dem Datenträger und dem Transport ein ausreichender Zugriffsschutz besteht. Sind die zu übermittelnden Daten auf den Datenträger geschrieben, so sollte dieser bis zum Transport in entsprechenden Behältnissen (Schrank, Tresor) verschlossen aufbewahrt werden. Die für den Transport oder für die Zustellung Verantwortlichen (z.B. Poststelle) sind auf sachgerechte und sichere Aufbewahrung und Handhabung des Datenträgers hinzuweisen.

M 1.37 Geeignete Aufstellung eines Fax-Gerätes
Ein Fax-Gerät sollte in einem Bereich installiert werden, der nicht öffentlich zugänglich ist. Eine Kontrolle des Zutritts zu diesem Bereich oder der Nutzung des Fax-Gerätes ist sinnvoll.

Sinnvollerweise kann dies durch die Aufstellung in einem ständig besetzten Raum (z.B. Geschäftszimmer, Sekretariat, Poststelle) erreicht werden. Außerhalb der Dienstzeiten oder bei Abwesenheit der berechtigten Benutzer sollte das Gerät eingeschlossen werden (Raum oder Schrank). Wichtig ist in diesem Zusammenhang, daß verhindert werden muß, daß eingegangene Fax-Sendungen von Unberechtigten eingesehen oder entnommen werden können (vgl. M 2.48 - Festlegung berechtigter Fax-Bediener).

M 1.38 Geeignete Aufstellung eines Modems
Um den Mißbrauch von Modems zu verhindern, muß sichergestellt werden, daß nur Berechtigte physikalischen Zugriff darauf haben. Mißbrauch bedeutet hier zum einem die Durchführung unbefugter Datenübertragungen, durch die Kosten verursacht, Viren eingeschleppt oder Interna nach außen transferiert werden können, und zum anderen das unbefugte Ändern oder Auslesen der Modem-Konfiguration, wodurch Sicherheitslücken entstehen können.
Um den physikalischen Zugriff auf ein externes Modem oder ein PCMCIA-Modem abzusichern, ist z.B. bei einem ständig benutzten Modem das Abschließen des Raumes oder bei einem nur zeitweise benutzten Modem das sichere Aufbewahren des inaktiven Modems in einem Schrank zu gewährleisten.
Über Modems darf kein Zugang zum internen Netz unter Umgehung einer bestehenden Firewall geschaffen werden.
Wenn mit einem Modempool weitere externe Zugänge zu einem durch eine Firewall geschützten Netz geschaffen werden sollen, muß dieser auf der unsicheren Seite der Firewall aufgestellt werden (siehe auch M 2.77 - Sichere Anordnung weiterer Komponenten). Der Modempool sollte zusammen mit dem zugehörigen Server in einem gesicherten Serverraum aufgestellt sein.

M 1.39 Verhinderung von Ausgleichsströmen auf Schirmungen
Um Ausgleichsströme auf den Schirmungen von Datenleitungen in Gebäuden zu verhindern, gibt es verschiedene Möglichkeiten:
Ausgleichsströme können im TN-C-Netz vermieden werden, indem nur solche IT-Geräte miteinander über geschirmte Datenleitungen miteinander verbunden werden, die an einer gemeinsamen Elektro-Verteilung angeschlossen sind. Bei jeder Erweiterung des Daten-Netzes ist diese Bedingung zu prüfen und sicherzustellen.

Ist die Beschränkung auf Datenverbindungen von IT-Geräten an einer Verteilung nicht möglich, können Ausgleichsströme dadurch vermieden werden, daß man die Schirmung der Datenleitung nur einseitig auflegt. Bei jeder Änderung im Daten-Netz ist darauf zu achten, daß nur entsprechend geeignete Kabel (mit nur einseitig aufgelegtem Schirm) Verwendung finden.
Die optimale, weil sicherste Möglichkeit besteht darin, das Stromverteilnetz im gesamten Gebäude komplett als TN-S-Netz auszulegen. Dabei wird der PE- und der N-Leiter ab der Potentialausgleichsschiene (PAS) getrennt geführt. Einzelmaßnahmen an IT-Geräten sind dann in der Regel nicht mehr erforderlich. Zu beachten ist jedoch der Hinweis in M 1.28 - Lokale unterbrechungsfreie Stromversorgung hinsichtlich der Bildung eines neuen TN-S-Netzes für die angeschlossenen Geräte.

M 1.40 Geeignete Aufstellung von Schutzschränken
Aufgrund des in der Regel hohen Gewichts von Schutzschränken muß vor der Aufstellung die Tragfähigkeit des Fußbodens am Aufstellungsort geprüft werden. Schutzschränke, die aufgrund ihrer geringen Größe relativ einfach weggetragen werden könnten, sollten in der Wand oder im Boden verankert werden. Evtl. vorhandene Herstellerhinweise zur geeigneten Aufstellung (z.B. freie Lüftungsöffnungen, Kabelführungen) sind zu berücksichtigen.

M 1.41 Schutz gegen elektromagnetische Einstrahlung
Werden in einem Schutzschrank informationstechnische Geräte untergebracht, so kann durch benachbarte Einrichtungen elektromagnetische Strahlung erzeugt werden, die die Funktion der Geräte beeinträchtigt (insbesondere in industriellen Produktionsbereichen). Durch Nachrüstung von Filtern und Türdichtungen kann die Einstrahlung innerhalb des Schutzschrankes reduziert werden. Gleichzeitig verhindern diese Maßnahmen auch eine Verbreitung von kompromittierender Abstrahlung der im Schrank befindlichen Geräte.

M 1.43 Gesicherte Aufstellung von ISDN-Routern
Um den manipulationssicheren Betrieb von ISDN-Routern sicherzustellen, ist es zwingend erforderlich, diese in einer gesicherten Umgebung aufzustellen. Dies kann entweder ein Serverraum sein (vgl. Kapitel 4.3.2 - Serverraum) oder ein Serverschrank, wenn kein separater Serverraum zur Verfügung steht (vgl. Kapitel 4.4 - Schutzschränke). Unbefugte dürfen zum Aufstellungsort von ISDN-Routern keinen unbeaufsichtigten Zugang erhalten.

M 1.44 Geeignete Einrichtung eines häuslichen Arbeitsplatzes
Für den häuslichen Arbeitsplatz ist die Nutzung eines Arbeitszimmers wünschenswert. Zumindest sollte der häusliche Arbeitsplatz von der übrigen Wohnung durch eine Tür abgetrennt sein.
Die Einrichtung sollte unter Berücksichtigung von Ergonomie, Sicherheit und Gesundheitsschutz ausgewählt werden.
Dies bedeutet u.a.:

- ausreichend Platz für Möbel und Bildschirmarbeitsplatz,
- regelbare Raumtemperatur und ausreichende Lüftungsmöglichkeiten,
- Abschirmung gegenüber Lärmquellen,
- Tageslicht sowie ausreichend künstliche Beleuchtung,
- Sichtschutz des Monitors, falls er durch ein Fenster beobachtet werden könnte,
- Vermeidung von störenden Blendungen, Reflexen oder Spiegelungen am Arbeitsplatz und
- Anschlüsse für Telefon und Strom.

Dienstlich genutzte IT sollte vom Arbeitgeber bereitgestellt werden, um z.B. per Dienstanweisung ausschließen zu können, daß die IT für private Zwecke benutzt wird.

M 1.45 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger
Dienstliche Unterlagen und Datenträger dürfen auch am häuslichen Arbeitsplatz nur dem autorisierten Mitarbeiter zugänglich sein. Aus diesem Grund muß ein verschließbares Behältnis (Schrank, Schreibtisch o.ä.) verfügbar sein. Die dienstlichen Unterlagen und Datenträger müssen außerhalb der Nutzungszeit in diesem Behältnis verschlossen aufbewahrt werden. Die Schutzwirkung des Behältnisses sollte den Sicherheitsanforderungen der darin zu verwahrenden Unterlagen und Datenträger entsprechen.

H.2 Maßnahmenkatalog Organisation

M 2.1 Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz
Für die Aufgabenbereiche „IT-Einsatz“ und „IT-Sicherheit“ müssen sowohl Verantwortlichkeiten als auch Befugnisse festgelegt sein. Für den „IT-Einsatz“ ist eine Festlegung der Fachverantwortung und der Betriebsverantwortung vorzunehmen. Der Fachverantwortliche ist zuständig für die Erarbeitung der fachlichen Vorgaben, die es in einem IT-Verfahren umzusetzen gilt. Hingegen umfaßt die Betriebsverantwortung u.a. folgende Aufgaben:

- Datenerfassung,
- Arbeitsplanung und -vorbereitung,
- Datenverarbeitung,
- Nachbereitung von Datenausgaben,
- Datenträgerverwaltung und
- Überwachung des Verfahrensbetriebes.

Übergreifende Regelungen zur „IT-Sicherheit“ als ein Aspekt des IT-Einsatzes müssen verbindlich festgelegt werden. Es empfiehlt sich, Regelungen über

- Datensicherung,
- Datenarchivierung,
- Datenträgertransport,
- Datenübertragung,
- Datenträgervernichtung,
- Dokumentation von IT-Verfahren, Software, IT-Konfiguration,
- Gebrauch von Paßwörtern,
- Zutrittsberechtigungen,
- Zugangsberechtigungen,
- Zugriffsberechtigungen,
- Betriebsmittelverwaltung,
- Kauf und Leasing von Hardware und Software,
- Wartungs- und Reparaturarbeiten,

- Software: Abnahme und Freigabe,
- Software: Anwendungsentwicklung,
- Datenschutz,
- Schutz gegen Computer-Viren,
- Revision,
- Notfallvorsorge und
- Vorgehensweise bei der Verletzung der Sicherheitspolitik

zu treffen. Hinweise dazu finden sich in den nachfolgenden Maßnahmenbeschreibungen.
Diese Regelungen sind den betroffenen Mitarbeitern in geeigneter Weise bekanntzugeben (siehe M 3.2 - Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen). Es empfiehlt sich, die Bekanntgabe zu dokumentieren. Darüber hinaus sind sämtliche Regelungen in der aktuellen Form an einer Stelle vorzuhalten und bei berechtigtem Interesse zugänglich zu machen.
Die getroffenen Regelungen sind regelmäßig zu aktualisieren, um Mißverständnisse, ungeklärte Zuständigkeiten und Widersprüche zu verhindern.

M 2.2 Betriebsmittelverwaltung
Betriebsmittel (oder Sachmittel) für den IT-Einsatz sind alle erforderlichen Mittel wie Hardwarekomponenten (Rechner, Tastatur, Drucker usw.), Software (Systemsoftware, Individualprogramme, Standardprogramme u.ä.), Verbrauchsmaterial (Papier, Toner, Druckerpatronen), Datenträger (Magnetbänder, Disketten, Streamertapes, Festplatten, Wechselplatten, CD-ROMs u.ä.).
Die Betriebsmittelverwaltung umfaßt die Abwicklung der Aufgaben:

- Beschaffung der Betriebsmittel,
- Prüfung vor Einsatz,
- Kennzeichnung und
- Bestandsführung.

Die Beschaffung von Betriebsmitteln ist beim Einsatz von Informationstechnik von besonderer Bedeutung. Mit einem geregelten Beschaffungsverfahren lassen sich insbesondere die Ziele unterstützen, die mit dem Einsatz von Informationstechnik angestrebt werden: Leistungssteigerung, Wirtschaftlichkeit, Verbesserung der Kommunikationsmöglichkeiten.
Neben reinen Wirtschaftlichkeitsaspekten kann durch ein geregeltes Beschaffungsverfahren - das von zentraler Stelle aus vorgenommen werden kann - auch die Neu- und Weiterentwicklung im Bereich der Informationstechnik stärker berücksichtigt werden.

Eine zentrale Beschaffung sichert darüber hinaus die Einführung und Einhaltung eines „Hausstandards“, der die Schulung der Mitarbeiter und Wartungsaktivitäten vereinfacht.
Mit einem geregelten Prüfverfahren vor Einsatz der Betriebsmittel lassen sich unterschiedliche Gefährdungen abwenden.
Erst mit Hilfe einer Bestandsführung der eingesetzten Betriebsmittel ist es möglich, den Verbrauch zu ermitteln und Nachbestellungen zu veranlassen. Darüber hinaus ermöglicht die Bestandsführung Vollständigkeitskontrollen, Überprüfung des Einsatzes von nicht genehmigter Software oder die Feststellung der Entwendung von Betriebsmitteln. Hierzu bedarf es einer eindeutigen Kennzeichnung der wesentlichen Betriebsmittel mit eindeutigen Identifizierungsmerkmalen (z.B. gruppierte fortlaufende Inventarnummern). Zusätzlich sollten die Seriennummern vorhandener Geräte wie Bildschirm, Drucker, Festplatten etc. dokumentiert werden, damit sie nach einem Diebstahl identifiziert werden können.
Für die Bestandsführung müssen die Betriebsmittel in Bestandsverzeichnissen aufgelistet werden. Ein solches Bestandsverzeichnis muß Auskunft geben können über:

- Identifizierungsmerkmale,
- Beschaffungsquellen, Lieferzeiten,
- Verbleib der Betriebsmittel,
- Lagervorhaltung,
- Aushändigungsvorschriften und
- Wartungsverträge, Wartungsintervalle.

M 2.3 Datenträgerverwaltung
Aufgabe der Datenträgerverwaltung als Teil der Betriebsmittelverwaltung ist es, den Zugriff auf Datenträger im erforderlichen Umfang und in angemessener Zeit gewährleisten zu können. Dies erfordert eine geregelte Verwaltung der Datenträger, die eine einheitliche Kennzeichnung sowie eine Führung von Bestandsverzeichnissen erforderlich macht. Weiterhin ist im Rahmen der Datenträgerverwaltung die sachgerechte Behandlung und Aufbewahrung der Datenträger, deren ordnungsgemäßer Einsatz und Transport und schließlich auch noch die Löschung bzw. Vernichtung der Datenträger zu gewährleisten.
Bestandsverzeichnisse ermöglichen einen schnellen und zielgerichteten Zugriff auf Datenträger. Bestandsverzeichnisse geben Auskunft über: Aufbewahrungsort, Aufbewahrungsdauer, berechtigte Empfänger.
Die äußerliche Kennzeichnung von Datenträgern ermöglicht deren schnelle Identifizierung. Die Kennzeichnung sollte jedoch für Unbefugte keine Rückschlüsse auf den Inhalt erlauben (z.B. die Kennzeichnung eines Magnetbandes mit dem Stichwort „Telefongebühren“), um einen Mißbrauch zu erschweren. Eine festgelegte Struktur von Kennzeichnungsmerkmalen (z.B. Datum, Ablagestruktur, lfd. Nummer) erleichtert die Zuordnung in Bestandsverzeichnissen.
Für eine sachgerechte Behandlung von Datenträgern sind die Herstellerangaben, die üblicherweise auf der Verpackung zu finden sind, heranzuziehen. Hinsichtlich der Aufbewahrung von

Datenträgern sind einerseits Maßnahmen zur Lagerung (magnetfeld-/staubgeschützt, klimagerecht) und andererseits Maßnahmen zur Verhinderung des unbefugten Zugriffs (geeignete Behältnisse, Schränke, Räume) zu treffen.
Der Versand oder Transport von Datenträgern muß in der Weise erfolgen, daß eine Beschädigung der Datenträger möglichst ausgeschlossen werden kann (z.B. Magnetbandversandtasche, luftgepolsterte Umschläge). Die Verpackung des Datenträgers ist an seiner Schutzbedürftigkeit auszurichten (z.B. mittels verschließbaren Transportbehältnissen). Versand- oder Transportarten (z.B. Kuriertransport) müssen ebenso festgelegt werden wie das Nachweisverfahren über den Versand (z.B. Begleitzettel, Versandscheine) und den Eingang beim Empfänger (z.B. Empfangsbestätigung). Der Datenträger darf über die zu versendenden Daten hinaus, keine „Restdaten“ enthalten. Dies kann durch physikalisches Löschen erreicht werden. Stehen hierzu keine Werkzeuge zur Verfügung, so sollte der Datenträger zumindest formatiert werden. Dabei sollte sichergestellt werden, daß mit dem zugrundeliegenden Betriebssystem eine Umkehr des Befehls nicht möglich ist. Weiterhin ist zu beachten, daß vor Abgabe wichtiger Datenträger eine Sicherungskopie erstellt wird.
Für die interne Weitergabe von Datenträger können Regelungen getroffen werden wie Quittungsverfahren, Abhol-/Mitnahmeberechtigungen sowie das Führen von Bestandsverzeichnissen über den Verbleib der Datenträger.
Für den Fall, daß von Dritten erhaltene Datenträger eingesetzt werden, sind Regelungen über deren Behandlung vor dem Einsatz zu treffen. Werden zum Beispiel Daten für PCs übermittelt, sollte generell ein Computer-Viren-Check des Datenträgers erfolgen. Dies gilt entsprechend auch vor dem erstmaligen Einsatz neuer Datenträger. Es ist empfehlenswert, nicht nur beim Empfang, sondern auch vor dem Versenden von Datenträgern diese auf Computer-Viren zu überprüfen.
Eine geregelte Vorgehensweise für die Löschung oder Vernichtung von Datenträgern verhindert den Mißbrauch der gespeicherten Daten. Vor der Wiederverwendung von Datenträgern muß die Löschung der gespeicherten Daten vorgenommen werden, z.B. durch vollständiges Überschreiben oder Formatieren. Beim Formatieren von DOS-Datenträgern ist darauf zu achten, daß der Parameter /U (in DOS 6.2 enthalten) benutzt wird, damit das Formatieren nicht über den Befehl unformat wieder rückgängig gemacht werden kann. Unter Windows 95 und Windows NT ist aus gleichem Grunde eine Formatierung mit dem Parameter Vollständig und nicht mit Quick-Format durchzuführen. Eine einfache Möglichkeit, Datenträger zu vernichten, besteht darin, daß Disketten und Magnetbänder zerschnitten und Festplatten mechanisch zerstört werden.

M 2.4 Regelungen für Wartungs- und Reparaturarbeiten

Als vorbeugende Maßnahme, um IT vor Störungen zu bewahren, ist die ordnungsgemäße Durchführung von Wartungsarbeiten von besonderer Bedeutung. Die rechtzeitige Einleitung von Wartungsarbeiten und die Überprüfung ihrer Durchführung sollte von einer zentralen Stelle aus wahrgenommen werden (z.B. Beschaffungsstelle). Dabei sollten die Wartungsarbeiten von vertrauenswürdigen Personen oder Firmen durchgeführt werden.

Wartungs- und Reparaturarbeiten im Hause
Für Wartungs- und Reparaturarbeiten, insbesondere wenn sie durch Externe durchgeführt werden, sind Regelungen über deren Beaufsichtigung zu treffen: während der Arbeiten sollte eine fachkundige Kraft die Arbeiten soweit beaufsichtigen, daß sie beurteilen kann, ob während der Arbeit nicht-autorisierte Handlungen vollzogen werden. Weiterhin ist zu überprüfen, ob der Wartungsauftrag ausgeführt wurde.
Als Maßnahmen vor und nach Wartungs- und Reparaturarbeiten sind einzuplanen:

- Ankündigung der Maßnahme gegenüber den betroffenen Mitarbeitern.
- Wartungstechniker müssen sich auf Verlangen ausweisen.
- Der Zugriff auf Daten durch den Wartungstechniker ist soweit wie möglich zu vermeiden. Falls erforderlich, sind Speichermedien vorher auszubauen oder zu löschen (nach einer kompletten Datensicherung), insbesondere wenn die Arbeiten extern durchgeführt werden müssen. Falls das Löschen nicht möglich ist (z. B. aufgrund eines Defektes), sind die Arbeiten auch extern zu beobachten bzw. es sind besondere vertragliche Vereinbarungen zu treffen.
- Die dem Wartungstechniker eingeräumten Zutritts-, Zugangs- und Zugriffsrechte sind auf das notwendige Minimum zu beschränken und nach den Arbeiten zu widerrufen bzw. zu löschen.
- Nach der Durchführung von Wartungs- oder Reparaturarbeiten sind – je nach „Eindringtiefe“ des Wartungspersonals – Paßwortänderungen erforderlich. Im PC-Bereich sollte ein Computer-Viren-Check durchgeführt werden.
- Die durchgeführten Wartungsarbeiten sind zu dokumentieren (Umfang, Ergebnisse, Zeitpunkt, evtl. Name des Wartungstechnikers).

Externe Wartungs- und Reparaturarbeiten
Werden IT-Systeme zur Wartung oder Reparatur außer Haus gegeben, sind alle sensitiven Daten, die sich auf Datenträgern befinden, vorher physikalisch zu löschen. Ist dies nicht möglich, weil aufgrund eines Defekts nicht mehr auf die Datenträger zugegriffen werden kann, sind die mit der Reparatur beauftragten Unternehmen auf die Einhaltung der erforderlichen IT-Sicherheitsmaßnahmen zu verpflichten. Entsprechend M 3.2 - Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen sind mit diesen vertragliche Regelungen über die Geheimhaltung von Daten zu treffen. Insbesondere ist festzulegen, daß Daten, die im Rahmen der Wartung extern gespeichert wurden, nach Abschluß der Arbeiten sorgfältig gelöscht werden. Ebenso sind die Pflichten und Kompetenzen des externen Wartungspersonals sorgfältig festzulegen.
Die Durchführung externer Wartungsarbeiten muß protokolliert werden, welche IT-Systeme oder Komponenten wann an wen zur Reparatur gegeben wurden, wer dies veranlaßt hat, zu welchem Zeitpunkt die Reparatur abgeschlossen sein sollte und wann das Gerät wieder zurückgebracht wurde. Um dies nachhalten zu können, ist eine Kennzeichnung der IT-Systeme oder

Komponenten erforderlich, aus der zum einem hervorgeht, welcher Organisation diese gehören, und zum anderen eine eindeutige Zuordnung innerhalb der Organisation möglich ist.
Bei Versand oder Transport der zu reparierenden IT-Komponenten sollte darauf geachtet werden, daß Beschädigungen und Diebstahl vorgebeugt wird. Befinden sich auf den IT-Systemen noch sensitive Informationen, müssen sie entsprechend geschützt transportiert werden, also z.B. in verschlossenen Behältnissen oder durch Kuriere. Weiterhin müssen Nachweise über den Versand (Begleitzettel, Versandscheine) und den Eingang beim Empfänger (Empfangsbestätigung) geführt und archiviert werden.
Bei IT-Systemen, die durch Paßwörter geschützt sind, müssen je nach Umfang der Reparaturarbeiten und der Art der Paßwortabsicherung, alle oder einige Paßwörter entweder bekanntgegeben oder auf festgelegte Einstellungen wie „REPARATUR“ gesetzt werden, damit die Wartungstechniker auf die Geräte zugreifen können.
Nach der Rückgabe der IT-Systeme oder Komponenten sind diese auf Vollständigkeit zu überprüfen. Alle Paßwörter sind zu ändern. PC-Datenträger sind nach der Rückgabe mittels eines aktuellen Viren-Suchprogramms auf Computer-Viren zu überprüfen. Alle Dateien oder Programme, die sich auf dem reparierten Gerät befinden, sind auf Integrität zu überprüfen.

Fernwartung
Regelungen für die Fernwartung können der Maßnahme M 5.33 - Absicherung der per Modem durchgeführten Fernwartung entnommen werden.

M 2.5 Aufgabenverteilung und Funktionstrennung
Die von der Behörde bzw. dem Unternehmen im Zusammenhang mit dem IT-Einsatz wahrzunehmenden Funktionen sind festzulegen. Zu unterscheiden sind hier zwei Ebenen:

- Die erste Ebene besteht aus den Funktionen, die den IT-Einsatz ermöglichen oder unterstützen wie Arbeitsvorbereitung, Datennachbereitung, Operating, Programmierung, Netzadministration, Rechteverwaltung, Revision.

- Die zweite Ebene besteht aus den Funktionen, die die zur Aufgabenerfüllung bereitstehenden IT-Verfahren anwenden. Beispiele solcher Funktionen sind: Fachverantwortlicher, IT-Anwendungsbetreuer, Datenerfasser, Sachbearbeiter, Zahlungsanordnungsbefugter. Im nächsten Schritt ist die Funktionstrennung festzulegen und zu begründen, d.h. welche Funktionen nicht miteinander vereinbar sind, also auch nicht von einer Person gleichzeitig wahrgenommen werden dürfen. Vorgaben hierfür können aus den Aufgaben selbst oder aus gesetzlichen Bestimmungen resultieren. Beispiele dafür sind:

  - Rechteverwaltung und Revision,
  - Netzadministration und Revision,
  - Programmierung und Test bei eigenerstellter Software,
  - Datenerfassung und Zahlungsanordnungsbefugnis,
  - Revision und Zahlungsanordnungsbefugnis.

Insbesondere wird deutlich, daß meistens operative Funktionen nicht mit kontrollierenden Funktionen vereinbar sind.
Nach der Festlegung der einzuhaltenden Funktionstrennung kann die Zuordnung der Funktionen zu Personen erfolgen. Die hier getroffenen Festlegungen sind zu dokumentieren und bei Veränderungen im IT-Einsatz zu aktualisieren. Sollte bei dieser Zuordnung eine Person miteinander unvereinbare Funktionen wahrnehmen müssen, so ist dies in einer entsprechenden Dokumentation über die Funktionsverteilung besonders hervorzuheben.

M 2.6 Vergabe von Zutrittsberechtigungen
Vor der Vergabe von Zutrittsberechtigungen für Personen sind die schutzbedürftigen Räume eines Gebäudes zu bestimmen, z.B. Büro, Datenträgerarchiv, Serverraum, Operating-Raum, Maschinensaal, Belegarchiv, Rechenzentrum. Der Schutzbedarf eines Raumes ist festzustellen anhand der im Raum befindlichen Informationstechnik sowie am Schutzbedarf der eingesetzten IT-Anwendungen und ihrer Informationen. Anschließend ist festzulegen, welche Person zur Ausübung der wahrgenommenen Funktion welches Zutrittsrecht benötigt. Dabei ist die vorher erarbeitete Funktionstrennung (M 2.5 - Aufgabenverteilung und Funktionstrennung) zu beachten. Unnötige Zutrittsrechte sind zu vermeiden.
Um die Zahl zutrittsberechtigter Personen zu einem Raum möglichst gering zu halten, sollte auch beim IT-Einsatz der Grundsatz der Funktionstrennung berücksichtigt werden. So verhindert z.B. eine getrennte Lagerung von IT-Ersatzteilen und Datenträgern den unerlaubten Zugriff eines Wartungstechnikers auf die Datenträger.
Die Vergabe und Rücknahme von Zutrittsberechtigungen ist zu dokumentieren. Bei der Rücknahme einer Zutrittsberechtigung muß die Rücknahme des Zutrittsmittels gewährleistet sein. Zusätzlich ist zu dokumentieren, welche Konflikte bei der Vergabe der Zutrittsberechtigungen an Personen aufgetreten sind. Gründe für Konflikte können vorliegen, weil Personen Funktionen wahrnehmen, die bezüglich der Zutrittsberechtigungen der Funktionstrennung entgegenstehen, oder aufgrund räumlicher Notwendigkeiten.
Zur Überwachung der Zutrittsberechtigung können Personen (Pförtner, Schließdienst) oder technische Einrichtungen (Ausweisleser, Schloß) eingesetzt werden (vgl. M 2.14 - Schlüsselverwaltung). Der Zutritt zu schutzbedürftigen Räumen von nicht autorisiertem Personal (z.B. Besuchern) darf nur bei Anwesenheit oder in Begleitung Zutrittsberechtigter erfolgen.
Regelungen über die Vergabe und Rücknahme von Zutrittsberechtigungen für Fremdpersonal und Besucher müssen ebenfalls getroffen werden.

M 2.7 Vergabe von Zugangsberechtigungen
Zugangsberechtigungen erlauben der betroffenen Person, bestimmte IT-Systeme bzw. System-Komponenten und Netze zu nutzen. Dies ist für jede nutzungsberechtigte Person aufgrund ihrer Funktion, unter Beachtung der Funktionstrennung (vgl. M 2.5 - Aufgabenverteilung und Funktionstrennung), im einzelnen festzulegen. Entsprechend der Funktion ist der Zugang zum Rechner zu definieren, z.B. Zugang zum Betriebssystem (Systemverwalter) oder Zugang zu einer IT-Anwendung (Anwender). Ergänzend hierzu muß sichergestellt sein, daß personelle und aufgabenbezogene Änderungen unverzüglich berücksichtigt werden.
Der Zugang soll - sofern DV-technisch möglich - erst nach einer Identifikation (z.B. durch Name,

User-ID oder Chipkarte) und Authentisierung (z. B. durch ein Paßwort) des Nutzungsberechtigten möglich sein und protokolliert werden.
Die Ausgabe bzw. der Einzug von Zugangsmitteln wie Benutzerkennungen oder Chipkarten ist zu dokumentieren. Regelungen über die Handhabung von Zugangs- und Authentifikationsmitteln (z.B. Umgang mit Chipkarten, Paßworthandhabung, vgl. M 2.11 - Regelung des Paßwortgebrauchs) müssen ebenfalls getroffen werden.
Die vorübergehende Sperrung einer Zugangsberechtigung sollte bei längerwährender Abwesenheit der berechtigten Person vorgenommen werden, um Mißbräuche zu verhindern.
Es ist notwendig, die vorgenannten Festlegungen auf ihre korrekte Einhaltung sporadisch zu kontrollieren.

M 2.8 Vergabe von Zugriffsrechten
Über Zugriffsrechte wird geregelt, welche Person im Rahmen ihrer Funktion bevollmächtigt wird, IT-Anwendungen oder Daten zu nutzen. Die Zugriffsrechte (z.B. Lesen, Schreiben, Ausführen) auf IT-Anwendungen, Teilanwendungen oder Daten sind von der Funktion abhängig, die die Person wahrnimmt, z.B. Anwenderbetreuer, Arbeitsvorbereiter, Systemprogrammierer, Anwendungsentwickler, Systemadministrator, Revisor, Datenerfasser, Sachbearbeiter. Dabei sollten immer nur so viele Zugriffsrechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist („Need-to-know-Prinzip“). Umgesetzt werden müssen die Zugriffsrechte durch die Rechteverwaltung des IT-Systems.
Eine Vielzahl von IT-Systemen lassen es zu, daß verschiedene Rechte als Gruppenrechte bzw. als Rechte-Profil definiert werden (z.B. Gruppe Datenerfasser). Diese Definition entspricht der technischen Umsetzung der Rechte, die einer Funktion zugeordnet werden. Für die Administration der Rechte eines IT-Systems ist es vorteilhaft, solche Gruppen oder Profile zu erstellen, da damit die Rechtezuteilung und deren Aktualisierung erheblich vereinfacht werden kann.
Die Festlegung und Veränderung von Zugriffsrechten ist vom jeweils Verantwortlichen zu veranlassen und zu dokumentieren. Aus der Dokumentation muß hervorgehen:

- welche Funktion unter Beachtung der Funktionstrennung (vgl. M 2.5 - Aufgabenverteilung und Funktionstrennung) mit welchen Zugriffsrechten ausgestattet wird,
- welche Gruppen bzw. Profile eingerichtet werden,
- welche Person welche Funktion wahrnimmt,
- welche Zugriffsrechte eine Person erhält und
- welche Konflikte bei der Vergabe von Zugriffsrechten aufgetreten sind. Diese Konflikte können z.B. daraus resultieren, daß eine Person unvereinbare Funktionen wahrnimmt oder daraus, daß abhängig vom IT-System die Trennung bestimmter Zugriffsrechte nicht vorgenommen werden kann.

M 2.9 Nutzungsverbot nicht freigegebener Software
Es muß geregelt sein, wie Software abgenommen, freigegeben, eingespielt bzw. benutzt werden darf (vgl. M 2.62 - Software-Abnahme und -Freigabe-Verfahren). Das Einspielen bzw.

Benutzen nicht freigegebener Software muß verboten und außerdem durch technische Möglichkeiten soweit möglich verhindert werden. Beispielsweise kann dies unter Windows 95 durch Einschränkung der Benutzerumgebung (vgl. M 2.104 - Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95) erreicht werden. Damit soll verhindert werden, daß Programme mit unerwünschten Auswirkungen eingebracht werden. Zusätzlich soll verhindert werden, daß das System über den festgelegten Funktionsumfang hinaus unkontrolliert genutzt wird. Falls erforderlich, kann dieses Nutzungsverbot auch auf die Nutzung privater Hardware (Disketten, Wechselplatte, PC, Laptop) und privater Daten ausgedehnt werden.
Ausnahmeregelungen sollten einen Erlaubnisvorbehalt vorsehen.

M 2.10 Überprüfung des Software-Bestandes
Um Verstöße gegen das Verbot der Nutzung nicht freigegebener Software feststellen zu können, ist eine regelmäßige Überprüfung des Software-Bestandes notwendig. Ist die Zahl der IT-Systeme sehr groß, kann eine stichprobenartige Überprüfung durchgeführt werden. Die Ergebnisse der Überprüfung sind zu dokumentieren, um auch Wiederholungsfälle feststellen zu können.
Sollte bei der Überprüfung nicht freigegebene Software gefunden werden, so ist die Entfernung zu veranlassen. Um diese Überprüfung durchführen zu können, muß der überprüfenden Instanz die entsprechende Befugnis durch die Unternehmens- bzw. Behördenleitung verliehen werden. Zusätzlich muß der prüfenden Instanz bekannt sein, welche Software auf welchem IT-System freigegeben ist (Software-Bestandsverzeichnis).

M 2.11 Regelung des Paßwortgebrauchs
Werden in einem IT-System Paßwörter zur Authentisierung gebraucht, so ist die Sicherheit der Zugangs- und Zugriffsrechteverwaltung des Systems entscheidend davon abhängig, daß das Paßwort korrekt gebraucht wird. Dafür ist es empfehlenswert, eine Regelung zum Paßwortgebrauch einzuführen und den IT-Benutzer diesbezüglich zu unterweisen.
Folgende Regeln zum Paßwortgebrauch sollten beachtet werden:

- Das Paßwort darf nicht leicht zu erraten sein wie Namen, Kfz-Kennzeichen, Geburtsdatum.
- Innerhalb des Paßwortes sollte mindestens ein Zeichen verwendet werden, das kein Buchstabe ist (Sonderzeichen oder Zahl).
- Das Paßwort sollte mindestens 6 Zeichen lang sein. Es muß getestet werden, wieviele Stellen des Paßwortes vom Rechner überprüft werden.
- Voreingestellte Paßwörter (z.B. des Herstellers bei Auslieferung von Systemen) müssen durch individuelle Paßwörter ersetzt werden.
- Paßwörter dürfen nicht auf programmierbaren Funktionstasten gespeichert werden.
- Das Paßwort muß geheimgehalten werden und sollte nur dem Benutzer persönlich bekannt sein.

- Das Paßwort sollte nur für die Hinterlegung schriftlich fixiert werden, wobei es dann in einem verschlossenen Umschlag sicher aufbewahrt wird. Wird es darüber hinaus aufgeschrieben, ist das Paßwort zumindest so sicher wie eine Scheckkarte oder ein Geldschein aufzubewahren (vgl. M 2.22 - Hinterlegen des Paßwortes).
- Das Paßwort muß regelmäßig gewechselt werden, z.B. alle 90 Tage.
- Ein Paßwortwechsel ist durchzuführen, wenn das Paßwort unautorisierten Personen bekannt geworden ist.
- Alte Paßwörter sollten nach einem Paßwortwechsel nicht mehr gebraucht werden.
- Die Eingabe des Paßwortes sollte unbeobachtet stattfinden. Falls IT-technisch möglich, sollten folgende Randbedingungen eingehalten werden
- Die Wahl von Trivialpaßwörtern sollte verhindert werden.
- Jeder Benutzer muß sein eigenes Paßwort jederzeit ändern können.
- Für die Erstanmeldung neuer Benutzer sollten Einmalpaßwörter vergeben werden, also Paßwörter, die nach einmaligem Gebrauch gewechselt werden müssen. In Netzen, in denen Paßwörter unverschlüsselt übertragen werden, empfiehlt sich die dauerhafte Verwendung von Einmalpaßwörtern (vgl. M 5.34 Einsatz von Einmalpaßwörtern).
- Nach dreifacher fehlerhafter Paßworteingabe sollte eine Sperrung erfolgen, die nur vom Systemadministrator aufgehoben werden kann.
- Bei der Authentisierung in vernetzten Systemen sollten Paßwörter nicht unverschlüsselt übertragen werden.
- Bei der Eingabe sollte das Paßwort nicht auf dem Bildschirm angezeigt werden.
- Die Paßwörter sollten im System zugriffssicher gespeichert werden, z.B. mittels Einwegverschlüsselung.
- Der Paßwortwechsel sollte vom System regelmäßig initiiert werden.
- Die Wiederholung alter Paßwörter beim Paßwortwechsel sollte vom IT-System verhindert werden (Paßwort-Historie).

M 2.12 Betreuung und Beratung von IT-Benutzern

Der Einsatz von IT-Systemen erfordert eine umfassende Schulung der IT-Benutzer. Neben der Schulung, die die IT-Benutzer in die Lage versetzt, die eingesetzte Informationstechnik sachgerecht einzusetzen, bedarf es einer Betreuung und Beratung der IT-Benutzer für die im laufenden Betrieb auftretenden Probleme. Diese Probleme können aus Hardware-Defekten oder fehlerhafter Software-Installation resultieren, aber auch aus Bedienungsfehlern.
In größeren Behörden bzw. Unternehmen kann es daher sinnvoll sein, eine zentrale Stelle mit

der Betreuung der IT-Benutzer zu beauftragen und diese allen Mitarbeitern bekanntzugeben. Diese Notwendigkeit kann sich insbesondere bei einer hohen Zahl dezentraler Systeme wie PCs als praktikabel erweisen.

M 2.13 Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
Betriebsmittel (oder Sachmittel), die schützenswerte Daten enthalten (Druckerpapier, Disketten, Streamertapes, Magnetbänder, Festplatten, aber auch spezielle Tonerkassetten, Kohlepapier oder Carbonbänder) und nicht mehr gebraucht werden oder aufgrund eines Defektes ausgesondert werden sollen, sind so zu entsorgen, daß keine Rückschlüsse auf vorher gespeicherte Daten möglich sind. Bei funktionstüchtigen Datenträgern kann dies durch physikalisches Löschen der Daten vorgenommen, bei nicht funktionierenden Datenträgern durch mechanische Zerstörung erreicht werden. Die Art der Entsorgung schutzbedürftigen Materials sollte in einer speziellen Anordnung geregelt werden, entsprechende Entsorgungseinrichtungen sind vorzuhalten (siehe auch DIN 32757).
Wird schutzbedürftiges Material vor der Entsorgung gesammelt, so ist die Sammlung verschlossen zu halten und vor unberechtigtem Zugriff zu schützen.
Soweit im Unternehmen bzw. in der Behörde keine umweltgerechte und sichere Entsorgung durchgeführt werden kann, sind damit beauftragte Unternehmen auf die Einhaltung erforderlicher IT-Sicherheitsmaßnahmen zu verpflichten. Ein Mustervertrag ist als Hilfsmittel diesem Handbuch beigefügt.

M 2.14 Schlüsselverwaltung
Für alle Schlüssel des Gebäudes (von Etagen, Fluren und Räumen) ist ein Schließplan zu fertigen. Die Herstellung, Aufbewahrung, Verwaltung und Ausgabe von Schlüsseln ist zentral zu regeln. Reserveschlüssel sind vorzuhalten und gesichert aufzubewahren. Das gleiche gilt auch für alle Identifikationsmittel wie Magnetstreifen- oder Chipkarten. Zu beachten bleibt:

- - Ist eine Schließanlage vorhanden, sind für schutzbedürftige Bereiche eigene Schließgruppen zu bilden, ggf. einzelne Räume aus der Schließgruppe herauszunehmen und mit Einzelschließung zu versehen.
- Nicht ausgegebene Schlüssel und die Reserveschlüssel sind gegen unbefugten Zugriff geschützt aufzubewahren.
- Die Ausgabe der Schlüssel erfolgt gegen Quittung und ist zu dokumentieren.
- Es sind Vorkehrungen zu treffen, wie bei Verlust einzelner Schlüssel zu reagieren ist (Meldung, Ersatz, Kostenerstattung, Austausch des Schlosses, Austausch von Schließgruppen etc.).
- Bei Zuständigkeitsänderungen von Mitarbeitern sind deren Schließberechtigungen zu prüfen, Schlüssel ggf. einzuziehen.
- Beim Ausscheiden von Mitarbeitern sind alle Schlüssel einzuziehen (Aufnahme der Schlüsselverwaltung in den Laufzettel).

- Schlösser und Schlüssel zu besonders schutzbedürftigen Bereichen (zu denen nur sehr wenige Schlüssel ausgegeben werden sollten) können bei Bedarf getauscht werden, um so illegal nachgefertigten Schlüsseln die Funktion zu nehmen.

M 2.15 Brandschutzbegehungen
Bei der Errichtung und der Nutzung von Gebäuden sind Brandschutzvorschriften zu beachten. Diese werden durch DIN- und VDE-Vorschriften festgeschrieben und durch Auflagen der örtlichen Feuerwehr ergänzt (siehe auch M 1.6 - Einhaltung von Brandschutzvorschriften und Auflagen der örtlichen Feuerwehr).
Die Erfahrungen zeigen, daß nach Nutzungsbeginn im täglichen Betrieb diese Regelungen immer nachlässiger gehandhabt werden - bis hin zur völligen Ignoranz.
Brandschutzbegehungen sollten ein- bis zweimal im Jahr angekündigt oder unangekündigt erfolgen.
Da die Handlungsweise der Mitarbeiter in der Regel nicht vom böswilligen Vorsatz, sondern von der betrieblichen Notwendigkeit oder Bequemlichkeit bestimmt wird, kann es nicht Sinn einer Brandschutzbegehung sein, Täter zu finden und zu bestrafen. Vielmehr sollten die vorgefundenen Mißstände dazu Anlaß geben, die Zustände sofort und ggf. deren Ursachen unverzüglich zu beheben.

M 2.16 Beaufsichtigung oder Begleitung von Fremdpersonen
Fremde (Besucher, Handwerker, Wartungs- und Reinigungspersonal) sollten, außer in Räumen, die ausdrücklich dafür vorgesehen sind, nicht unbeaufsichtigt sein (siehe auch M 2.6 - Vergabe von Zutrittsberechtigungen). Wird es erforderlich, einen Fremden allein im Büro zurückzulassen, sollte man einen Kollegen ins Zimmer oder den Besucher zu einem Kollegen bitten.
Ist es nicht möglich, Fremdpersonen (z.B. Reinigungspersonal) ständig zu begleiten oder zu beaufsichtigen, sollte zumindest der persönliche Arbeitsbereich abgeschlossen werden: Schreibtisch, Schrank und PC (Schloß für Diskettenlaufwerk, Tastaturschloß). Siehe auch M 2.37 - „Der aufgeräumte Arbeitsplatz“.
Für den häuslichen Arbeitsplatz gilt, daß Familienmitglieder und Besucher sich nur dann alleine im Arbeitsbereich aufhalten dürfen, wenn alle Arbeitsunterlagen verschlossen aufbewahrt sind und die IT über einen aktivierten Zugangsschutz gesichert ist.
Die Notwendigkeit dieser Maßnahme ist den Mitarbeitern zu erläutern und ggf. in einer Dienstanweisung festzuhalten. Eine Dokumentationen über den Aufenthalt von Fremdpersonen kann in einem Besucherbuch geführt werden.

M 2.17 Zutrittsregelung und -kontrolle
Der Zutritt zu schutzbedürftigen Gebäudeteilen und Räumen ist zu regeln und zu kontrollieren (siehe M 2.6 - Vergabe von Zutrittsberechtigungen). Die Maßnahmen reichen dabei von einer einfachen Schlüsselvergabe bis zu aufwendigen Identifizierungssystemen mit Personenvereinzelung, wobei auch die Nutzung eines mechanischen Schlüssels nebst Schloß eine Zutrittskontrolle darstellt. Für eine Zutrittsregelung und -kontrolle ist es erforderlich, daß

- der von der Regelung betroffene Bereich eindeutig bestimmt wird,

- die Zahl der zutrittsberechtigten Personen auf ein Mindestmaß reduziert wird; diese Personen sollen gegenseitig ihre Berechtigung kennen, um Unberechtigte als solche erkennen zu können,
- der Zutritt anderer Personen (Besucher) erst nach vorheriger Prüfung der Notwendigkeit erfolgt,
- erteilte Zutrittsberechtigungen dokumentiert werden.

Die Vergabe von Rechten allein reicht nicht aus, wenn deren Einhaltung bzw. Überschreitung nicht kontrolliert wird. Die Ausgestaltung von Kontrollmechanismen sollte nach dem Grundsatz erfolgen, daß einfache und praktikable Lösungen oft ebenso effizient sind wie aufwendige Technik.

M 2.18 Kontrollgänge
Eine Maßnahme kann nur so gut wirken, wie sie auch tatsächlich umgesetzt wird. Kontrollgänge bieten das einfachste Mittel, die Umsetzung von Maßnahmen und die Einhaltung von Auflagen und Anweisungen zu überprüfen.
Die Kontrollgänge sollen nicht dem Finden von Tätern dienen, um diese zu bestrafen. Sinn der Kontrollen soll es in erster Linie sein, erkannte Nachlässigkeiten möglichst sofort zu beheben (Fenster zu schließen, Unterlagen in Aufbewahrung zu nehmen etc.). In zweiter Linie können Ursachen für diese Nachlässigkeiten erkannt und evtl. in der Zukunft vermieden werden.
Die Kontrollgänge sollten durchaus auch während der Dienstzeit erfolgen und zur Information der Mitarbeiter über das Wie und Warum von Regelungen genutzt werden. So werden sie von allen Beteiligten eher als Hilfe denn als Gängelung angesehen.

M 2.19 Neutrale Dokumentation in den Verteilern
In jedem Verteiler sollte sich eine Dokumentation befinden, die den derzeitigen Stand von Rangierungen und Leitungsbelegungen wiedergibt. Diese Dokumentation ist möglichst neutral zu halten. Nur bestehende und genutzte Verbindungen sind darin aufzuführen. Es sollen, soweit nicht ausdrücklich vorgeschrieben (z.B. für Brandmeldeleitungen) keine Hinweise auf die Nutzungsart der Leitungen gegeben werden. Leitungs-, Verteiler-, und Raumnummern reichen in vielen Fällen aus. Alle weitergehenden Informationen sind in einer Revisions-Dokumentation aufzuführen.

M 2.20 Kontrolle bestehender Verbindungen
Alle Verteiler und Zugdosen sind einer (zumindest stichprobenartigen) Sichtprüfung zu unterziehen. Dabei ist auf folgende Punkte zu achten:

- Spuren von gewaltsamen Öffnungsversuchen an verschlossenen Verteilern,
- Aktualität der im Verteiler befindlichen Dokumentation,
- Übereinstimmung der tatsächlichen Beschaltungen und Rangierungen mit der Dokumentation,

- Unversehrtheit der Kurzschlüsse und Erdungen nicht benötigter Leitungen und
- unzulässige Einbauten/Veränderungen.

Neben der reinen Sichtkontrolle kann zusätzlich eine funktionale Kontrolle durchgeführt werden. Dabei werden bestehende Verbindungen auf ihre Notwendigkeit und die Einhaltung technischer Werte hin geprüft. In zwei Fällen ist diese Prüfung anzuraten:

- bei Verbindungen, die sehr selten genutzt und bei denen Manipulationen nicht sofort erkannt werden,
- bei Verbindungen, auf denen häufig und regelmäßig schützenswerte Informationen übertragen werden.

M 2.21 Rauchverbot
In Räumen mit IT oder Datenträgern (Serverraum, Datenträgerarchiv, aber auch Belegarchiv), in denen Brände oder Verschmutzungen zu hohen Schäden führen können, sollte ein Rauchverbot erlassen werden. Dieses Rauchverbot dient gleicherweise dem vorbeugenden Brandschutz wie der Betriebssicherheit von IT mit mechanischen Funktionseinheiten.

M 2.22 Hinterlegen des Paßwortes
Ist der Zugriff auf ein IT-System durch ein Paßwort geschützt, so müssen Vorkehrungen getroffen werden, die bei Abwesenheit eines Mitarbeiters, z.B. im Urlaubs- oder Krankheitsfall, seinem Vertreter den Zugriff auf das IT-System ermöglichen. Zu diesem Zweck ist das aktuelle Paßwort durch jeden Mitarbeiter an einer geeigneten Stelle (in einem geschlossenen Umschlag) zu hinterlegen und bei jeder Änderung des Paßwortes zu aktualisieren. Wird es notwendig, dieses hinterlegte Paßwort zu nutzen, so sollte dies nach dem Vier-Augen-Prinzip, d.h. von zwei Personen gleichzeitig, geschehen. Bei einem Telearbeiter ist sicherzustellen, daß dessen Paßwörter auch in der Institution hinterlegt werden, damit im Notfall sein Vertreter auf die im Telearbeitsrechner gespeicherten Daten zugreifen kann.
Bei allen von Administratoren betreuten Systemen, insbesondere bei vernetzten Systemen, ist durch regelmäßige Überprüfung sicherzustellen, daß das aktuelle Systemadministrator-Paßwort hinterlegt ist.

M 2.23 Herausgabe einer PC-Richtlinie
Um einen sicheren und ordnungsgemäßen Einsatz von Personalcomputern in größeren Unternehmen bzw. Behörden zu fördern, sollte eine PC-Richtlinie erstellt werden, in der verbindlich vorgeschrieben wird, welche Randbedingungen eingehalten werden müssen und welche IT-Sicherheitsmaßnahmen zu ergreifen sind. Diese PC-Richtlinie soll zumindest den Einsatz von unvernetzten PCs regeln; werden PCs vernetzt betrieben oder als intelligente Terminals genutzt, ist die Richtlinie um diese Punkte zu erweitern. Im folgenden soll grob umrissen werden, welche Inhalte für eine solche PC-Richtlinie sinnvoll sind.
Möglicher inhaltlicher Aufbau einer PC-Richtlinie:

- Zielsetzung und Begriffsdefinitionen
  Dieser erste Teil der PC-Richtlinie dient dazu, die PC-Anwender für IT-Sicherheit zu sensibilisieren und zu motivieren. Gleichzeitig werden die für das gemeinsame Verständnis notwendigen Begriffe definiert, wie z.B. PC, Anwender, Benutzer, schutzbedürftige Objekte.

- Geltungsbereich
  In diesem Teil muß verbindlich festgelegt werden, für welche Teile des Unternehmens bzw. der Behörde die PC-Richtlinie gilt.

- Rechtsvorschriften und interne Regelungen
  Hier wird dargestellt, welche Rechtsvorschriften, z.B. das Bundesdatenschutzgesetz und das Urheberrechtsgesetz, einzuhalten sind. Darüber hinaus kann diese Stelle genutzt werden, um alle relevanten betriebsinternen Regelungen aufzuführen.

- Verantwortungsverteilung
  In diesem Teil wird definiert, welcher Funktionsträger im Zusammenhang mit dem PC-Einsatz welche Verantwortung tragen muß. Dabei sind insbesondere die Funktionen IT-Benutzer, Vorgesetzte, Revisionsbeauftragter, Datenschutzbeauftragter und IT-Sicherheitsmanagement zu unterscheiden.

- Umzusetzende und einzuhaltende IT-Sicherheitsmaßnahmen
  Im letzten Teil der PC-Richtlinie ist festzulegen, welche IT-Sicherheitsmaßnahmen vom IT-Benutzer einzuhalten bzw. umzusetzen sind. Es kann je nach Schutzbedarf auch über die IT-Grundschutz-Maßnahmen hinausgehen.

Sind Telearbeiter im Unternehmen bzw. in der Behörde beschäftigt, sollte die PC-Richtlinie um die Telearbeitsplatz-spezifischen Regelungen ergänzt werden.

M 2.24 Einführung eines PC-Checkheftes

Um die durchgeführten IT-Sicherheitsmaßnahmen am PC zu dokumentieren, bietet es sich an, ein PC-Checkheft einzuführen, in dem der PC-Nutzer folgendes dokumentieren kann:

- Name des PC-Benutzers,
- Aufstellungsort des PC,
- Beschreibung der Konfiguration,
- Zugangsmittel,
- eingesetzte Hard- und Software,
- planmäßige Zeitpunkte für die Datensicherungen,
- durchgeführte Wartungen und Reparaturen,
- durchgeführte Computer-Viren-Kontrollen,

- Zeitpunkt von Paßwort-Änderungen,
- zur Verfügung stehendes Zubehör,
- durchgeführte Revisionen,
- Ansprechpartner für Problemfälle und
- Zeitpunkte der durchgeführten Datensicherungen.

Ein Muster eines solchen PC-Checkheftes ist der CD-ROM zum Handbuch [BSI1998] beigefügt. Wird das Führen eines solchen PC-Checkheftes angeordnet, so werden Kontrolltätigkeiten entschieden erleichtert, da die Dokumentation aller durchgeführten PC-relevanten Änderungen und IT-Sicherheitsmaßnahmen aus diesem PC-Checkheft hervorgehen. Außerdem unterstützt das Führen dieses Heftes für den PC-Benutzer eine notwendige Selbstkontrolle, damit er regelmäßig Datensicherungen, Paßwort-Änderungen und Viren-Checks durchführt.

M 2.25 Dokumentation der Systemkonfiguration
Planung, Steuerung, Kontrolle und Notfallvorsorge des IT-Einsatzes basieren auf einer aktuellen Dokumentation des vorhandenen IT-Systems. Nur eine aktuelle Dokumentation der Systemkonfiguration ermöglicht im Notfall einen geordneten Wiederanlauf des IT-Systems.
Bei einem Netzbetrieb ist die physikalische Netzstruktur (vgl. M 5.4 - Dokumentation und Kennzeichnung der Verkabelung) und die logische Netzkonfiguration zu dokumentieren. Dazu gehören auch die Zugriffsrechte der einzelnen Benutzer (siehe M 2.31 - Dokumentation der zugelassenen Benutzer und Rechteprofile) und der Stand der Datensicherung. Dabei ist auf Aktualität und Verständlichkeit der Dokumentation zu achten, damit auch ein Vertreter die Administration jederzeit weiterführen kann, ebenso wie auf eine sichere Aufbewahrung der Unterlagen, um deren Verfügbarkeit im Bedarfsfall zu gewährleisten.

M 2.26 Ernennung eines Administrators und eines Vertreters
Um einen geordneten Betrieb von IT-Systemen zu ermöglichen, ist ein Administrator zu bestimmen. Ihm obliegt neben allgemeinen Administrationsarbeiten insbesondere die Benutzerverwaltung einschließlich der Verwaltung der Zugriffsrechte. Zusätzlich ist er für die Sicherheitsbelange des betreuten IT-Systems zuständig.
Beim Einsatz von Protokollierung sollte auf die Rollentrennung von Administration und Revision geachtet werden. Hier ist zu überprüfen, inwieweit die IT-Systeme dies unterstützen.
Um bei Verhinderung des Administrators die Funktionen weiter aufrechtzuerhalten, ist ein Vertreter zu benennen.
Für die Übernahme von Administrationsaufgaben muß gewährleistet sein, daß dem Administrator und seinem Vertreter für eine sorgfältige Aufgabenerfüllung auch die hierfür erforderliche Zeit zur Verfügung steht. Hierbei muß auch berücksichtigt werden, daß Aus- und Fortbildungsmaßnahmen erforderlich sind.

M 2.27 Verzicht auf Fernwartung der TK-Anlage
Der Verzicht auf Fernwartung ist eine wirkungsvolle Maßnahme, um Externe an Manipulationen

an der TK-Anlagenkonfiguration zu hindern. Für Einzelanlagen und kleine Anlagenverbunde mit geringen räumlichen Entfernungen zwischen den einzelnen Verbundmitgliedern kann dies auch aus ökonomischen Gründen sinnvoll sein.
Vorteil: Im Gegensatz zu allen anderen in [BSI1998] Kapitel 8.1 - TK-Anlage - aufgeführten Maßnahmen kann hierdurch garantiert werden, daß auch bei direktem Zugriff auf die Leitungen der Telekom keine Zugriffsmöglichkeit auf den Wartungseingang der Anlage möglich ist. Eine ähnliche Sicherheit wäre sonst nur unter Zuhilfenahme von Kryptomitteln erreichbar.
Nachteil: Alle Wartungsarbeiten müssen direkt an der Anlage durchgeführt werden. Ohne zusätzliche Maßnahmen, z.B. Verlagerung des Wartungs-PCs in den Nachbarraum, hat das Wartungspersonal auch immer Zutritt zur TK-Anlage. Oft werden die Remote-Schnittstellen nicht nur für den Zweck der Fernwartung genutzt. Über dieselben Schnittstellen werden teilweise auch Fernsignalisierungen geführt, die für den Betrieb eines TK-Netzes notwendig sind. In solchen Fällen wäre mit dem Verzicht auf Fernwartung auch ein Verzicht auf ein zentrales Netzmanagement verbunden. Soll eine Remote-Schnittstelle nur für Fernsignalisierungszwecke via Modem benutzt werden, so sollte dieses Modem so konfiguriert werden, daß keine Rufe entgegengenommen werden.

M 2.28 Bereitstellung externer TK-Beratungskapazität
Um in schwierigen Fällen schnell auf fachkundige Hilfe zurückgreifen zu können, sollte schon beim Kauf bzw. der Miete einer TK-Anlage an die Bereitstellung entsprechender Beratungsdienstleistung gedacht werden. Wichtig hierbei ist, daß in einer Notfallsituation die Unterstützung schnell erfolgen kann, da der Ausfall einer TK-Anlage die Handlungsfähigkeit einer gesamten Institution erheblich beeinträchtigen und ggf. nur für kurze Zeit toleriert werden kann.

M 2.29 Bedienungsanleitung der TK-Anlage für die Benutzer
Dem Benutzer der TK-Anlage sind die notwendigen Unterlagen zur Bedienung seiner Endgeräte (z.B. Bedienungsanleitung für das Telefon) zur Verfügung zu stellen. Neben der normalen Bedienung seines Telefons sollte der Benutzer vor allem in der Lage sein, etwaige Warnanzeigen (LEDs oder Piktogramme im Display) und -töne zu interpretieren (siehe M 3.12 - Information aller Mitarbeiter über mögliche TK-Warnanzeigen, -symbole und -töne).

M 2.30 Regelung für die Einrichtung von Benutzern / Benutzergruppen
Regelungen für die Einrichtung von Benutzern / Benutzergruppen bilden die Voraussetzung für eine angemessene Vergabe von Zugriffsrechten und für die Sicherstellung eines geordneten und überwachbaren Betriebsablaufs.
Es sollte ein Formblatt existieren, um von jedem Benutzer bzw. für jede Benutzergruppe zunächst die erforderlichen Daten abzufragen:

- Name, Vorname,
- Vorschlag für die Benutzer- bzw. Gruppenkennung, wenn diese nicht durch Konventionen vorgegeben sind,
- Organisationseinheit,

- Erreichbarkeit (z.B. Telefon, Raum),
- ggf. Projekt,
- ggf. Angaben über die geplante Tätigkeit im System und die dazu erforderlichen Rechte sowie die Dauer der Tätigkeit,
- ggf. Restriktionen auf Zeiten, Endgeräte, Plattenvolumen, Zugriffsberechtigungen (für bestimmte Verzeichnisse, Remote-Zugriffe, etc.), eingeschränkte Benutzerumgebung,
- ggf. Zustimmung von Vorgesetzten.

Falls Zugriffsberechtigungen vergeben werden, die über den Standard hinausgehen, sollte dies begründet werden.Dieses kann auch in elektronischer Form erfolgen durch ein spezielles Login, dessen Name und Paßwort den einzurichtenden Benutzern bekanntgegeben wird. Dort wird ein entsprechendes Programm durchlaufen, das mit einem Logout endet. Die erfaßten Daten können zur Vorlage beim Vorgesetzten ausgedruckt werden. Ein Paßwort, das einem neuen Benutzer für die erstmalige Systemnutzung mitgeteilt wird, muß danach gewechselt werden. Dies sollte vom System initiiert werden.
Es sollte eine begrenzte Anzahl von Rechteprofilen festgelegt werden. Ein neuer Benutzer wird dann einem solchen Profil zugeordnet und erhält damit genau die für seine Tätigkeit erforderlichen Rechte. Dabei sind die systemspezifischen Möglichkeiten bei der Einrichtung von Benutzern und Gruppen zu beachten. Es ist sinnvoll, Namenskonventionen für die Benutzer- und Gruppennamen festzulegen (z.B. Benutzer-ID = Kürzel Organisationseinheit / lfd. Nummer).
Die Zugriffsberechtigung für Dateien ist auf Benutzer bzw. Gruppen mit berechtigtem Interesse zu beschränken. Wenn mehrere Personen auf eine Datei zugreifen müssen, soll für diese eine Gruppe eingerichtet werden. In der Regel muß jedem Benutzer eine eigene Benutzerkennung zugeordnet sein, es dürfen nicht mehrere Benutzer unter derselben Kennung arbeiten. Für jeden Benutzer muß ein eindeutiges Heimatverzeichnis angelegt werden. Für die Einrichtungsarbeiten im System sollte eine administrative Rolle geschaffen werden: Die Einrichtung sollte mit Hilfe eines speziellen Logins, unter dem ein entsprechendes Programm oder Shellskript gestartet wird, erfolgen. Die zuständigen Administratoren können Benutzer bzw. Benutzergruppen somit nur auf definierte Weise einrichten, und es ist nicht erforderlich, ihnen Rechte für andere Administrationsaufgaben zu geben. Diese Maßnahme wird ergänzt durch folgende Maßnahmen:

- M 4.13 - Sorgfältige Vergabe von IDs
- M 4.19 - Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen
- M 4.20 - Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen

M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile
Die Dokumentation dient der Übersicht über die zugelassenen Benutzer, Benutzergruppen und Rechteprofile und ist Voraussetzung für Kontrollen. Es soll jede der folgenden drei Dokumentationsmöglichkeiten genutzt werden:

- vorgegebene Administrationsdateien des Systems,
- individuelle Dateien, die vom zuständigen Administrator verwaltet werden,
- in Papierform.

Dokumentiert werden sollen insbesondere

- die zugelassenen Benutzer mit folgenden Angaben: zugeordnetes Rechteprofil (ggf. Abweichungen vom verwendeten Standard-Rechteprofil), Begründung für die Wahl des Rechteprofils (und ggf. der Abweichungen), Erreichbarkeit des Benutzers, Zeitpunkt und Grund der Einrichtung, Befristungen,
- die zugelassenen Gruppen mit den zugehörigen Benutzern, Zeitpunkt und Grund der Einrichtung, Befristung.

M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung

Falls Benutzer nur bestimmte Aufgaben wahrzunehmen brauchen, ist es oftmals nicht erforderlich, ihnen alle mit einem eigenen Login verbundenen Rechte (ggf. sogar Systemadministrator-Rechte) zu geben. Beispiele sind bestimmte Tätigkeiten der routinemäßigen Systemverwaltung (wie Erstellung von Backups, Einrichten eines neuen Benutzers), die mit einem Programm menügesteuert durchgeführt werden, oder Tätigkeiten, für die ein Benutzer nur ein einzelnes Anwendungsprogramm benötigt.
Für diese Benutzer sollte eine eingeschränkte Benutzerumgebung geschaffen werden. Sie kann z.B. unter Unix durch eine Restricted Shell (rsh) und eine Beschränkung der Zugriffspfade mit dem Unix-Kommando chroot realisiert werden. Für einen Benutzer, der nur ein Anwendungsprogramm benötigt, kann dieses als Login-Shell eingetragen werden, so daß nach dem Einloggen dieses direkt gestartet und er bei Beendigung des Programms automatisch ausgeloggt wird.
Der verfügbare Funktionsumfang des IT-Systems kann für einzelne Benutzer oder Benutzergruppen eingeschränkt werden. Die Nutzung von Editorprogrammen oder Compilern sollte verhindert werden, wenn dies nicht für die Aufgabenerfüllung des Benutzers erforderlich ist. Dies kann bei Stand-alone-Systemen durch die Entfernung solcher Programme und bei vernetzten Systemen durch die Rechtevergabe geregelt werden.

M 2.33 Aufteilung der Administrationstätigkeiten unter Unix

In den meisten Unix-Systemen gibt es nur eine Administrationsrolle (den Super-User namens root mit der Benutzer-ID (UID) 0). Personen mit Zugang zu dieser Rolle haben die volle Kontrolle über das System. Insbesondere können sie unabhängig von Zugriffsrechten jede Datei lesen, verändern und löschen.
Das Super-User-Paßwort darf nur den Administratoren bekannt sein. Die Weitergabe des Paßworts ist auf die in Regelungen festgelegte Fälle zu beschränken und zu dokumentieren. Der Super-User-Login root kann durch Anwendung des Vier-Augen-Prinzips zusätzlich geschützt werden, z.B. durch organisatorische Maßnahmen wie ein geteiltes Paßwort. Dabei muß das Paßwort eine erhöhte Mindestlänge (12 oder mehr Zeichen) haben. Hierbei muß darauf geachtet werden, daß das Paßwort in voller Mindestlänge vom System überprüft wird.

Bei etlichen Unix-Systemen ist eine Aufgabenteilung durch die Ausnutzung vorhandener Administratorrollen möglich. Diese Rollen sollen dann durch verschiedene Personen wahrgenommen werden.
Eine Reihe von Administrationstätigkeiten können auch ohne Zugang zum Login root ausgeführt werden. Wenn es Administratoren mit solchen Spezialaufgaben gibt, sollte davon Gebrauch gemacht werden. Insbesondere wenn in großen Systemen mehrere Personen mit Administrationsaufgaben betraut werden müssen, kann das Risiko durch eine entsprechende Aufgabenteilung vermindert werden. Es gibt dazu zwei Möglichkeiten:

- Schaffung administrativer Logins: Sie haben zwar die UID 0, jedoch wird beim Login nur ein Programm gestartet, mit dem die administrative Aufgabe ausgeführt werden kann und das mit einem Logout endet. Beispiele: Einrichten neuer Benutzer, Mounten eines Laufwerks. Zu UNIX V.4 können z.B. die administrativen Login-Namen setup, sysadm, powerdown, checkfsys, mountfsys und umountfsys mit den gleichnamigen Programmen eingerichtet werden.

- Benutzung von Logins ohne UID 0: Diese Login-Namen (sys, bin, adm, uucp, nuucp, daemon und lp) sind Eigentümer von Dateien und Programmen, die für die Funktionalität des Systems entscheidend sind und die daher besonderem Schutz unterliegen. Sie sind in den meisten Unix-Systemen zur Verwaltung der entsprechenden Dienste vorgegeben.

M 2.34 Dokumentation der Veränderungen an einem bestehenden System

Um einen reibungslosen Betriebsablauf zu gewährleisten, muß der Administrator einen Überblick über das System haben bzw. sich verschaffen können. Dieses muß auch für seinen Vertreter möglich sein, falls der Administrator unvorhergesehen ausfällt. Der Überblick ist auch Voraussetzung, um Prüfungen des Systems (z.B. auf problematische Einstellungen, Konsistenz bei Änderungen) durchführen zu können.
Daher sollten die Veränderungen, die Administratoren am System vornehmen, dokumentiert werden, nach Möglichkeit automatisiert. Dieses gilt insbesondere für Änderungen an Systemverzeichnissen und -dateien.
Bei Installation neuer Betriebssysteme oder bei Updates sind die vorgenommenen Änderungen besonders sorgfältig zu dokumentieren. Möglicherweise kann durch die Aktivierung neuer oder durch die Änderung bestehender Systemparameter das Verhalten das Verhalten des IT-Systems (insbesondere auch Sicherheitsfunktionen) maßgeblich verändert werden.
Unter Unix müssen ausführbare Dateien, auf die auch andere Benutzer als der Eigentümer Zugriff haben oder deren Eigentümer root ist, vom Systemadministrator freigegeben und dokumentiert werden (siehe auch M 2.9 - Nutzungsverbot nicht freigegebener Software). Insbesondere müssen Listen mit den freigegebenen Versionen dieser Dateien geführt werden, die außerdem mindestens das Erstellungsdatum, die Größe jeder Datei und Angaben über evtl. gesetzte s-Bits enthalten. Sie sind Voraussetzung für den regelmäßigen Sicherheitscheck und für Überprüfungen nach einem Verlust der Integrität.

M 2.35 Informationsbeschaffung über Sicherheitslücken des Systems

Gegen bekannt gewordene und durch Veröffentlichungen zugänglich gemachte Sicherheitslücken

müssen die erforderlichen organisatorischen und administrativen Maßnahmen ergriffen oder zusätzliche Sicherheitshardware bzw. Sicherheitssoftware eingesetzt werden. Es ist daher sehr wichtig, sich über neu bekannt gewordene Schwachstellen zu informieren. Informationsquellen:

- Bundesamt für Sicherheit in der Informationstechnik (BSI), Postfach 20 03 63, 53133 Bonn,
  Telefon: (0228) 9582-444, Fax -427,
  E-Mail: cert@bsi.de
  BSI-Mailbox: (0228) 9580971 (weitere Informationen zur Mailbox: s.Anhang)

- Hersteller bzw. Vertreiber des Betriebssystems informieren registrierte Kunden über bekannt gewordene Sicherheitslücken ihrer Systeme und stellen korrigierte Varianten des Systems oder Patches zur Behebung der Sicherheitslücken zur Verfügung.

- Computer Emergency Response Teams (CERT) sind Organisationen, die über bekannt gewordene Betriebssystemfehler und deren Behebungsmöglichkeiten informieren.
  Computer Emergency Response Team / Coordination Center (CERT/CC), Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890, Tel. +1 412 268-7090 (24-Stunden-Hotline), E-Mail: cert@cert.sei.cmu.edu oder cert@cert.org, ftp: cert.sei.cmu.edu (192.88.209.5)
  Die CERT-Mitteilungen werden in Newsgruppen (comp.security.announce und info.nsfnet.cert) und über Mailinglisten
  (Aufnahme durch E-Mail an: cert-advisory-request@cert.org) veröffentlicht.

- CERT in Deutschland:

  - BSI-CERT, Bundesamt für Sicherheit in der Informationstechnik , Postfach 20 03 63, 53133 Bonn,
    Telefon: (0228) 9582-444, Fax -427,
    E-Mail: cert@bsi.de
  - DFN-CERT, Universität Hamburg, Fachbereich Informatik, Vogt-Kölln-Straße 30, 22527 Hamburg, Tel. 040 54715-262, Fax -241,
    E-Mail: dfncert@cert.dfn.de,
    ftp: ftp.cert.dfn.de: /pub/security,
    gopher: gopher.cert.dfn.de,
    Aufnahme in Mailingliste für CERT-Mitteilungen durch E-Mail
    an: dfncert-request@cert.dfn.de
    Mailinglisten für Diskussionen: win-sec@cert.dfn.de
    Mailinglisten für sicherheitsrelevante Informationen: win-sec-ssc@cert.dfn.de
    URLs: FTP: ftp://ftp.cert.dfn.de/pub/security
    WWW: http://www.cert.dfn.de
  - Micro-BIT Virus Center/CERT, Universität Karlsruhe, Postfach 6980, 76128 Karlsruhe, Tel. (0721) 376422, Fax (0721) 32550,
    E-Mail: cert@rz.uni-karlsruhe.de

- hersteller- und systemspezifische sowie sicherheitsspezifische Newsgruppen
- IT-Fachzeitschriften

M 2.36 Geregelte Übergabe und Rücknahme eines tragbaren PC
Bei der Übergabe und Rücknahme eines tragbaren PCs sind folgende Punkte zu beachten:
Übergabe:

- Die fachliche Notwendigkeit der Benutzung eines tragbaren PCs sollte vorab geprüft sein.
- Der neue Benutzer wird aufgefordert, direkt bei der Übergabe das alte Paßwort des tragbaren PCs bzw. das Standardpaßwort zu ändern.
- Dem neuen Benutzer wird ein Merkblatt für den sicheren Umgang mit dem tragbaren PC übergeben (optional).
- Der neue Benutzer wird mit Namen, Organisationseinheit, Telefonnummer, Einsatzzweck in das Übergabe-/Rücknahmejournal eingetragen.

Rücknahme bzw. Weitergabe:

- Der Benutzer gibt sein zuletzt benutztes Paßwort bekannt bzw. stellt ein Standardpaßwort wie „LAPTOP“ ein.
- Die Vollständigkeit des Gerätes, des Zubehörs und der Dokumentation ist sicherzustellen.
- Der Benutzer muß sicherstellen, daß vor Übergabe des Gerätes sämtliche Daten, die der Benutzer noch benötigt, auf ihm zugängliche Datenträger (z.B. seinen PC) übertragen werden. Darüber hinaus hat der Benutzer dafür Sorge zu tragen, daß sämtliche von ihm erzeugten Dateien und Daten (nach Möglichkeit physikalisch) gelöscht sind.
- Die empfangende Stelle prüft den tragbaren PC mittels eines aktuellen Viren-Suchprogramms auf einen Computer-Viren-Befall.
- Die Rückgabe des tragbaren PC und das Untersuchungsergebnis der Virensuche werden dokumentiert.
- Zurückgegebene Disketten werden neu formatiert. Beim Formatieren von DOS-Datenträgern ist darauf zu achten, daß der Parameter /U (in DOS 6.2 enthalten) benutzt wird, damit das Formatieren nicht über den Befehl unformat wieder rückgängig gemacht werden kann.

M 2.37 „Der aufgeräumte Arbeitsplatz“
Jeder Mitarbeiter sollte dazu angehalten werden, seinen Arbeitsplatz „aufgeräumt“ zu hinterlassen. Ein IT-Benutzer hat nicht nur dafür Sorge zu tragen, daß bei Verlassen seines Arbeitsplatzes entsprechende Vorkehrungen getroffen sind, daß Unbefugte keinen Zugang zu

IT-Anwendungen oder Zugriff auf Daten erhalten. Der IT-Benutzer muß mit der gleichen Sorgfalt auch seinen Arbeitsplatz überprüfen und sicherstellen, daß durch den Zugriff Unbefugter auf Datenträger (Diskette, Festplatte) oder Unterlagen (Ausdrucke) kein Verlust an Verfügbarkeit, Vertraulichkeit oder Integrität entstehen kann.
Für eine kurze Abwesenheit während der Arbeitszeit ist das Verschließen des Raumes ausreichend; außerhalb der Arbeitszeit ist der Arbeitsplatz so aufzuräumen, daß keine schutzbedürftigen Datenträger oder Unterlagen unverschlossen am Arbeitsplatz zurückgelassen werden.

M 2.38 Aufteilung der Administrationstätigkeiten
Viele Netzbetriebssysteme bieten die Möglichkeit, die Administratorrolle aufzuteilen und Administrationstätigkeiten an verschiedene Benutzer zu verteilen.
So können z.B. unter Novell Netware 3.11 die folgenden Administratorrollen eingerichtet werden: Workgroup Manager, User Account Manager, File Server Console Operator, Print Server Operator, Print Queue Operator.
Unter Windows NT können durch die gezielte Vergabe von Benutzerrechten an einzelne Benutzer oder besser an Gruppen definierte Administratorrollen geschaffen werden. Neben der Gruppe der Administratoren sind hier die Gruppen Hauptbenutzer (d.h. Administratoren mit eingeschränkten Rechten), Sicherungs-Operatoren, Druck-Operatoren, Server-Operatoren sowie Reproduktions-Operatoren zu nennen. Darüber hinaus können weitere Rollen durch explizite Zuweisung von Benutzerrechten definiert werden (siehe auch M 4.50 - Strukturierte Systemverwaltung unter Windows NT).
Wenn es Administratorrollen für Spezialaufgaben gibt, sollte davon Gebrauch gemacht werden. Insbesondere wenn in großen Systemen mehrere Personen mit Administrationsaufgaben betraut werden müssen, kann das Risiko der übergroßen Machtbefugnis der Administratorrollen durch eine entsprechende Aufgabenteilung vermindert werden, so daß Administratoren nicht unkontrolliert unautorisierte oder unbeabsichtigte Veränderungen am System vornehmen können.
Trotz des Aufteilens von Administrationstätigkeiten legt das System meist noch automatisch einen Account für einen Administrator an, der keinen Beschränkungen unterliegt, den Supervisor. Das Supervisor-Paßwort sollte, wenn überhaupt, nur einem kleinen Personenkreis bekannt sein. Es darf keinem der Subadministratoren bekannt sein, damit diese nicht auf diese Weise ihre Rechte erweitern können. Das Paßwort ist gesichert zu hinterlegen (siehe M 2.22 - Hinterlegen des Paßwortes). Das Supervisor-Login kann durch Anwendung des Vier-Augen-Prinzips zusätzlich geschützt werden, z. B. durch organisatorische Maßnahmen wie ein geteiltes Paßwort. Dabei muß das Paßwort eine erhöhte Mindestlänge (12 oder mehr Zeichen) haben. Hierbei muß darauf geachtet werden, daß das Paßwort in voller Mindestlänge vom System überprüft wird.

M 2.39 Reaktion auf Verletzungen der Sicherheitspolitik
Es ist festzulegen, welche Reaktion auf Verletzungen der Sicherheitspolitik erfolgen soll, um eine klare und sofortige Reaktion gewährleisten zu können. Untersuchungen sollten durchgeführt werden, um festzustellen, wie und wo die Verletzung entstanden ist. Anschließend müssen die angemessenen schadensbehebenden oder -mindernden Maßnahmen durchgeführt werden. Soweit erforderlich, müssen zusätzliche schadensvorbeugende Maßnahmen ergriffen werden. Die durchzuführenden Aktionen hängen sowohl von der Art der Verletzung als auch vom Verursa-

cher ab.
Es muß geregelt sein, wer für Kontakte mit anderen Organisationen verantwortlich ist, um Informationen über bekannte Sicherheitslücken einzuholen (siehe auch M 2.35 - Informationsbeschaffung über Sicherheitslücken des Systems) oder um Informationen über aufgetretene Sicherheitslücken weiterzugeben. Es muß dafür Sorge getragen werden, daß evtl. mitbetroffene Stellen schnellstens informiert werden.

M 2.40 Rechtzeitige Beteiligung des Personal- / Betriebsrates
Maßnahmen, die geeignet sind eine Verhaltens- oder Leistungsüberwachung eines Mitarbeiters zu ermöglichen, z.B. Protokollierung, bedürfen der Mitbestimmung der Personalvertretung. Grundlage dessen sind die Betriebsverfassungs- und Personalvertretungsgesetze von Bund und Ländern. Die rechtzeitige und umfassende Information des Betriebs- oder Personalrates kann Zeitverzögerung bei der Umsetzung von Maßnahmen im Bereich des IT-Grundschutzes verhindern.

M 2.41 Verpflichtung der Mitarbeiter zur Datensicherung
Da die Datensicherung eine wichtige IT-Sicherheitsmaßnahmen ist, sollten die betroffenen Mitarbeiter auf die Einhaltung des Datensicherungskonzeptes bzw. des Minimaldatensicherungskonzeptes verpflichtet werden. Eine regelmäßige Erinnerung und Motivation zur Datensicherung sollte erfolgen.

M 2.42 Festlegung der möglichen Kommunikationspartner
Sollen Informationen an einen Kommunikationspartner übertragen werden, so muß sichergestellt werden, daß der Empfänger die notwendigen Berechtigungen zum Weiterverarbeiten dieser Informationen besitzt. Werden Informationen zwischen mehreren kommunizierenden Stellen ausgetauscht, so soll für alle Beteiligten ersichtlich sein, wer diese Informationen ebenfalls erhalten hat bzw. erhalten wird. Um die oben genannten Kriterien zu erfüllen, bedarf es einer Festlegung, welche Kommunikationspartner welche Informationen erhalten dürfen.
Im Sinne des [BDSG], Anlage zu §9 Satz 1 (Übermittlungskontrolle) sollte eine Übersicht erstellt werden, welche Empfänger berechtigt sind, Informationen, insbesondere personenbezogene Daten, per Datenträgeraustausch erhalten können.

M 2.43 Ausreichende Kennzeichnung der Datenträger beim Versand
Neben den in Maßnahme M 2.3 - Datenträgerverwaltung dargestellten Umsetzungshinweisen ist bei einer ausreichenden Kennzeichnung von auszutauschenden Datenträgern darauf zu achten, daß Absender und (alle) Empfänger unmittelbar zu identifizieren sind. Die Kennzeichnung muß den Inhalt des Datenträgers eindeutig für den Empfänger erkennbar machen. Es ist jedoch bei schützenswerten Informationen wichtig, daß diese Kennzeichnung für Unbefugte nicht interpretierbar ist.
Darüber hinaus sollten die Datenträger mit den für das Auslesen notwendigen Parametern gekennzeichnet werden. So sind bei der Übermittlung von Magnetbändern unter anderem das Label, die Geschwindigkeit (z.B. 800 bpi), die Satzlänge, Blocklänge und Satzformat (z.B. 132 Byte, 13200 Byte, Fixed) auf einem Etikett zu vermerken.

Datum des Versandes, eventuelle Versionsnummern oder Ordnungsmerkmale können gegebenenfalls nützlich sein.

M 2.44 Sichere Verpackung der Datenträger
Neben den in Maßnahme M 2.3 - Datenträgerverwaltung dargestellten Umsetzungshinweisen sollte die Verpackung dergestalt sein, daß Manipulationen am Datenträger durch Veränderungen an der Verpackung erkennbar sind.
Mögliche Maßnahmen sind die Verwendung von

- Umschlägen mit Siegel,
- verplombten Behältnissen oder
- Umschlägen, die mit Klebefilm überklebt und anschließend mit nicht-wasserlöslicher Tinte mehrmals unregelmäßig überzeichnet werden. Verfügt der Datenträger über einen Schreibschutz (Schieber bei Disketten, Schreibring bei Bändern) so sollte dieser genutzt werden. Sollen Manipulationen an den Informationen auf dem Datenträger selbst erkannt werden, sind Verschlüsselungs- oder Checksummenverfahren einzusetzen (siehe M 4.34 - Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen).

M 2.45 Regelung des Datenträgeraustausches
Sollen zwischen zwei oder mehreren Kommunikationspartnern Datenträger ausgetauscht werden, so sind zum ordnungsgemäßen Austausch folgende Punkte zu beachten:

- Die Adressierung muß eindeutig erfolgen, um eine fehlerhafte Zustellung zu vermeiden. So sollte neben dem Namen des Empfängers auch Organisationseinheit und die genaue Bezeichnung der Behörde/des Unternehmens angegeben sein. Entsprechendes gilt für die Adresse des Absenders.
- Dem Datenträger sollte (optional) ein Datenträgerbegleitzettel beigelegt werden, der folgende Informationen umfaßt:
- Absender,
- Empfänger,
- Art des Datenträgers,
- Seriennummer (soweit vorhanden),
- Identifikationsmerkmal für den Inhalt des Datenträgers,
- Datum des Versandes, ggf. Datum bis wann der Datenträger spätestens den Empfänger erreicht haben muß,
- Hinweis, daß Datenträger auf Viren überprüft sind,

- Parameter, die zum Lesen der Informationen benötigt werden, z.B. Bandgeschwindigkeit.

Jedoch sollte nicht vermerkt werden,

- welches Paßwort für die eventuell geschützten Informationen vergeben wurde,
- welche Schlüssel ggf. für eine Verschlüsselung der Informationen verwendet wurde,
- welchen Inhalt der Datenträger hat.
- Der Versand des Datenträgers kann (optional) dokumentiert werden. Für jede stattgefundene Übermittlung ist dann in einem Protokoll festzuhalten, wer wann welche Informationen erhalten hat. Je nach Schutzbedarf beziehungsweise Wichtigkeit der übermittelten Informationen ist der Empfang zu quittieren ein Quittungsvermerk und dem erwähnten Protokoll beizufügen.
- Es sind jeweils Verantwortliche für den Versand und für den Empfang zu benennen.
- Die Versandart ist festzulegen.

M 2.46 Angepaßtes Schlüsselmanagement bei Verschlüsselung
Wird zum Schutz der Vertraulichkeit der zu übermittelnden Informationen ein Verschlüsselungsverfahren eingesetzt, so muß vorab ein angepaßtes Schlüsselmanagement initiiert werden. Berücksichtigt werden muß

- Schlüsselgenerierung
  Die Auswahl der Schlüssel muß sich am eingesetzten Verfahren orientieren. Schlüssel dürfen nicht leicht erratbar oder rekonstruierbar sein (analog Paßwort). Für eine „gute" Schlüsselwahl eignen sich insbesondere Zufallszahlengeneratoren. Auch muß sichergestellt werden, daß bei der Installation des Verschlüsselungsverfahrens voreingestellte Schlüssel geändert werden.
- Aufbewahrung und Hinterlegung
  Der Vertraulichkeitsschutz durch Verschlüsselung kann nur dann umfassend erreicht werden, wenn die verwendeten kryptographischen Schlüssel geheimgehalten werden können. Bieten die IT-Systeme, auf denen das Verschlüsselungsverfahren eingesetzt ist, keinen ausreichenden Zugriffsschutz für die Schlüssel, sollten diese nicht auf diesem IT-System gespeichert werden. Besser ist eine bedarfsorientierte manuelle Eingabe. Werden Schlüssel nicht mehr benötigt oder verwendet, sind sie physikalisch zu löschen oder zu vernichten. Bei Bedarf ist aus Gründen der Notfallvorsorge das Hinterlegen der verwendeten Schlüssel in gesicherten Bereichen (Tresore) vorzusehen.
- Übermittlung
  Die Schlüssel sollten von den verschlüsselten Daten getrennt (zeitlich und räumlich) zum Empfänger übertragen werden. Hierfür ist ggf. ein Bote oder der Versand mittels PIN-Brief (geschwärzter Umschlag wie bei Gehaltsmitteilungen) vorzusehen. Eine Übermittlung per Telefon ist für den mittleren Schutzbedarf in vielen Fällen ausreichend.

- Schlüsselwechsel
  Die verwendeten Schlüssel sind abhängig von der Häufigkeit ihres Einsatzes, von dem relevanten Bedrohungspotential und der Sicherheit ihrer lokalen Aufbewahrung hinreichend oft präventiv zu wechseln. Besteht der Verdacht, daß ein verwendeter Schlüssel bloßgestellt wurde, so ist dieser Schlüssel nicht mehr zu verwenden und alle Beteiligten sind zu informieren. Bereits mit diesem Schlüssel verschlüsselte Informationen sind zu entschlüsseln und mit einem anderen Schlüssel zu verschlüsseln.

M 2.47 Ernennung eines Fax-Verantwortlichen
Für jedes Fax-Gerät ist ein Verantwortlicher zu benennen, der folgende Aufgaben übernehmen muß:

- Verteilung der eingehenden Fax-Sendungen an die Empfänger,
- Koordination der Versorgung des Fax-Gerätes mit notwendigen Verbrauchsgütern,
- geeignete Entsorgung von Fax-Verbrauchsgütern,
- Löschen von Restinformationen im Fax-Gerät vor Wartungs- und Reparaturarbeiten,
- Beaufsichtigung von Wartungs- und Reparaturarbeiten (vgl. M 2.4 - Regelungen für Wartungs- und Reparaturarbeiten),
- gelegentliche Kontrolle programmierter Zieladressen und Protokolle, insbesondere nach Wartungs- und Reparaturarbeiten,
- Ansprechpartner bei Problemen bei der Fax-Nutzung.

M 2.48 Festlegung berechtigter Fax-Bediener
Die Berechtigung zur Bedienung des Fax-Gerätes ist auf einen ausgewählten Kreis zuverlässiger Mitarbeiter zu beschränken. Diese Mitarbeiter sind in die korrekte Handhabung des Gerätes einzuweisen und mit den erforderlichen IT-Sicherheitsmaßnahmen vertraut zu machen. Jeder berechtigte Benutzer sollte darüber unterrichtet werden, wer das Gerät bedienen darf und wer der Fax-Verantwortliche ist. Darüber hinaus sollte am Fax-Gerät eine verständliche Bedienungsanleitung ausliegen.
Durch die Einschränkung des Fax-Bedienerkreises auf die für den operativen Einsatz notwendige Mindestzahl wird erreicht, daß die Anzahl der Personen, die eingehende Fax-Sendungen mitlesen können, begrenzt ist.

M 2.49 Beschaffung geeigneter Fax-Geräte
Bei Neuanschaffungen von Fax-Geräten sollte darauf geachtet werden, daß übliche Standardsicherheitsfunktionen implementiert sind wie:

- Austausch einer Teilnehmerkennung,

- Sendebericht,
- Journalführung.

Unter Beachtung des Preis-/Leistungsverhältnisses sind darüber hinaus folgende zusätzliche Sicherheitsfunktionen zu begrüßen:

- paßwortgeschützter Zugang,
- paßwortgeschützter Pufferspeicher,
- Einrichten einer geschlossenen Benutzergruppe,
- Ausschließen bestimmter Fax-Anschlüsse von Versendung oder Empfang.

M 2.50 Geeignete Entsorgung von Fax-Verbrauchsgütern und -Ersatzteilen
Alle Fax-Verbrauchsgüter, aus denen Informationen über Faxtexte gewonnen werden könnten, wie z.B. Zwischenträgerfolien oder fehlerhafte Ausdrucke, sollten vor der Entsorgung vernichtet oder durch eine zuverlässige Fachfirma entsorgt werden.
Das gleiche gilt beim Austausch informationstragender Ersatzteile, wie z.B. photo-elektrische Trommeln. Wartungsfirmen, die Faxgeräte periodisch warten oder reparieren, sind auf eine entsprechende Handhabung zu verpflichten und ggf. zu kontrollieren.

M 2.51 Fertigung von Kopien eingehender Fax-Sendungen
Ein Fax auf Thermopapier kann nach einiger Zeit stark verblassen oder schwarz werden. Daher sollten von Faxen auf Thermopapier, deren Informationsgehalt länger benötigt wird, Kopien auf Normalpapier erstellt werden.

M 2.52 Versorgung und Kontrolle der Fax-Verbrauchsgüter
Die Benutzer sollten angewiesen werden, den Fax-Verantwortlichen zu benachrichtigen, wenn Verbrauchsmaterial (z.B. Papier, Toner) nachgefüllt werden muß. Der Fax-Verantwortliche selbst sollte eine solche Prüfung regelmäßig (mindestens einmal pro Monat, bei besonderem Bedarf öfter) vornehmen. Die Versorgung mit Fax-Verbrauchsgütern ist vom Fax-Verantwortlichen ausreichend sicherzustellen.

M 2.53 Abschalten des Fax-Gerätes außerhalb der Bürozeiten
Um die Brandgefahr, die von Fax-Geräten immer ausgehen kann, zu reduzieren, sollten Geräte, die außerhalb der Arbeitszeit nicht benötigt werden (Abteilungs-Fax-Gerät, persönliches Gerät) zum Dienstschluß abgeschaltet werden. Damit kann auch erreicht werden, daß eingehende Fax-Sendungen nicht unkontrolliert längere Zeit im Fax-Gerät verbleiben. Realisierbar ist die Abschaltung auf einfache Weise durch Zeitschaltuhren, die die Stromversorgung des Gerätes auf die üblichen Bürozeiten einschränken. Für später eingehende Sendungen kann ein anderer (möglichst ständig kontrollierter) Fax-Anschluß benannt werden oder bei modernen TK-Anlagen eine Anrufumleitung eingerichtet werden.

Gleichzeitig kann mit dem Abschalten des Fax-Gerätes die Überlastung des Gerätes aufgrund eines technischen Versagens oder aufgrund beabsichtigter Massenfaxsendungen außerhalb der Bürozeit verhindert werden.

Das Abschalten sollte unterbleiben, wenn für die Verfügbarkeit des Gerätes besondere Anforderungen bestehen, die bei den Ausweichlösungen nicht umgesetzt werden können.

M 2.54 Beschaffung geeigneter Anrufbeantworter
Diese Maßnahme ist bei der Neubeschaffung von Anrufbeantwortern zu beachten. Sollten vorhandene Geräte den Sicherheitsansprüchen nicht genügen, ist eine Neuanschaffung oder die Abschaltung dieser Geräte in Erwägung zu ziehen. Bei der Beschaffung von Anrufbeantwortern sollten unter Beachtung der Wirtschaftlichkeit einige Kriterien beachtet werden, um Gefährdungen möglichst auszuschließen:

- Zur Sicherstellung einwandfreier fernmeldetechnischer Funktionen müssen die Geräte eine BZT-Zulassung (Postzulassung) besitzen.
- Bei ganz oder teilweise digital speichernden Geräten empfiehlt es sich, solche auszuwählen, die eine Notstromversorgung durch Batterien oder vom Benutzer wechselbare Akkumulatoren bieten. Bei fest eingebauten Akkumulatoren wird bei einem Austausch der Einsatz eines Servicetechnikers notwendig, was zu einem längeren Ausfall des Anrufbeantworters führen kann.
- Aufgrund unterschiedlicher Güte der Nachrichtenaufzeichnung (z.B. bei analoger oder digitaler Aufzeichnung) sollte vor der Beschaffung die Aufzeichnungsqualität getestet werden.
- Ganz oder teilweise digital speichernde Anrufbeantworter sollten mit einer Anzeige der Batteriekapazität sowie einem deutlichem Warnzeichen (evtl. auch akustisch) ausgestattet sein, um verminderte Batterieleistung rechtzeitig anzeigen zu können.
- Bei Anrufbeantwortern, die eine einzige Kassette sowohl für Aufzeichnungen als auch für den Ansagetext verwenden, entstehen durch Bandspulvorgänge Wartezeiten. Es sollte abgewogen werden, ob diese Wartezeiten in Kauf genommen werden können.
- Die Bedienungsfreundlichkeit des Anrufbeantworters sollte beachtet werden. Ergonomische und übersichtliche Tastenanordnung, Funktionstasten ohne Doppelbelegungen und für jedermann verständliche Bedienungsanleitungen sind vorteilhaft.
- Die Fernabfrage sollte nach Möglichkeit mechanisch oder elektronisch deaktivierbar, der Sicherungscode zumindest drei- bis vierstellig und frei programmierbar sein. Eine zusätzliche Sperrschaltung, die den Anrufbeantworter nach drei vergeblichen Versuchen die Verbindung unterbrechen läßt, bietet einen erhöhten Schutz. Hieraus ergeben sich zumindest ein höherer Zeitaufwand und höhere Telefonkosten für den potentiellen Angreifer. Besser noch sind Geräte, bei denen die Fernabfragefunktionen nach drei vergeblichen

Versuchen vollkommen gesperrt werden und nur noch am Gerät selbst wieder aktivierbar sind. Auch Sperrzeiten, die nach jedem Fehlversuch verlängert werden, sind sinnvoll.

M 2.55 Einsatz eines Sicherungscodes
Verfügt der Anrufbeantworter über Fernabfragemöglichkeiten und einen Sicherungscode, so ist anzustreben, daß die Fernabfrage nur mittels eines individuell gewählten, geheimzuhaltenden Sicherungscodes aktiviert werden kann. Insbesondere ist ein evtl. werkseitig eingestellter Code zu ändern. Der Sicherungscode ist wie ein Paßwort zu hinterlegen (vgl. hierzu M 2.22 - Hinterlegen des Paßwortes) und auch regelmäßig zu ändern.

Bei der Bedienung des Anrufbeantworters mittels Fernabfragegerät sollte darauf geachtet werden, daß sich kein Fremder in der Nähe aufhält, der die Eingabe der Codes beobachten oder erlauschen könnte.

M 2.56 Vermeidung schutzbedürftiger Informationen auf dem Anrufbeantworter
Da sich zur Zeit Anrufbeantworter nicht vollständig gegen Mißbrauch absichern lassen, sollte die Aufzeichnung schutzbedürftiger Informationen vermieden werden oder sogar in Bereichen, in denen typischerweise schutzbedürftige Informationen ausgetauscht werden, der Einsatz von Anrufbeantwortern überdacht werden. Im Ansagetext sollte daher darauf hingewiesen werden, daß keine schutzbedürftigen Informationen auf dem Anrufbeantworter hinterlassen werden sollten.

M 2.57 Regelmäßiges Abhören und Löschen aufgezeichneter Gespräche
Die im Anrufbeantworter gespeicherten Gespräche sollten regelmäßig abgehört und gelöscht werden. Ist das Löschen bei analog aufzeichnenden Geräten nicht möglich, sollte das Magnetband an den Anfang zurückgespult werden, damit die Aufzeichnung neuer Gespräche gespeicherte alte Nachrichten überschreibt.

M 2.58 Begrenzung der Sprechdauer
Zur Verhinderung von vorzeitiger Füllung des Speichermediums, sollte die maximale Sprechdauer pro Anruf auf 2-4 Minuten begrenzt werden, wenn das Gerät eine solche Einstellung erlaubt.

M 2.59 Auswahl eines geeigneten Modems in der Beschaffung
Bei der Beschaffung eines Modems sind folgende Punkte zu beachten:

- Modem-Zulassung
  Ein Modem, daß in Deutschland an das öffentliche Telekommunikationsnetz angeschlossen werden soll, muß eine BZT-Zulassung (früher ZZF-Zulassung, davor FTZ-Zulassung, im allgemeinen Sprachgebrauch auch Post-Zulassung genannt) haben. Hinweis: Entgegen der Angaben in vielen Modem-Handbüchern muß die Inbetriebnahme eines zugelassenen Modems nicht mehr der Telekom gemeldet werden.

- Bauweise
  Ein internes Modem bietet den Vorteil, daß die Modem-Konfiguration nur über den Rechner, in dem es eingebaut ist, geändert werden kann. Verfügt der Rechner über Zugangs- oder Zugriffsschutzmechanismen, können sie zum Schutz der Modem-Konfigurationsdaten eingesetzt werden. Gleichzeitig kann damit die Nutzung des Modems auf autorisierte Personen beschränkt werden. Manipulationen am Modem sind durch den Einbau im Rechner erschwert. Bei vernetzten Systemen, die nicht über derartige Schutzmechanismen verfügen (einige Peer-to-Peer-Netze), besteht der Nachteil eines internen Modems darin, daß das Modem unkontrolliert von allen Arbeitsplätzen genutzt werden kann.

  Ein externes Modem kann nach Nutzung verschlossen aufbewahrt werden. Es bietet außerdem den Vorteil, daß es üblicherweise über diverse Anzeigen sowie den Modemlautsprecher über den aktuellen Status informieren kann. Über den Modemlautsprecher kann auch gehört werden, ob von extern eine Verbindung aufgebaut wird oder ob eine Applikation unaufgefordert versucht, Informationen über die Installation und die System-Konfiguration an den Hersteller zu übertragen. Ein weiterer Vorteil eines externen Modems ist, daß es unabhängig vom IT-System nur für die jeweilige Datenübertragung eingeschaltet werden kann und somit z.B. sichergestellt werden kann, daß die letzte Verbindung getrennt worden ist und daß keine Verbindung von außerhalb aufgebaut werden kann. Nachteilig ist, daß ein externes Modem zur Manipulation der Konfigurationsdaten oder zum Auslesen gespeicherter Paßwörter einfach an ein nicht geschütztes IT-System angeschlossen werden kann.

  PCMCIA-Modems bieten aufgrund der Baugröße den Vorteil, daß sie nach Nutzung einfach verwahrt werden können. Eine sichere Aufbewahrung verhindert, daß sie zur Manipulation an ungeschützte Rechner angeschlossen werden.

- Übertragungsgeschwindigkeit
  Je höher die Übertragungsgeschwindigkeit eines Modems ist, desto geringer sind die Kosten für die Übertragung großer Datenmengen aufgrund der Zeiteinsparung.

  Zunächst ist zu klären, welche Übertragungsgeschwindigkeiten für den gewünschten Einsatzzweck notwendig ist. Ausreichend sind z.B. bei ASCII-Terminalemulation 2400 bit/sec, bei Fax-Übertragung 9600 bit/sec, bei Datex-J (T-Online) zur Zeit 14400 bit/sec. Für Datenübertragung großen Ausmaßes sind die aktuell größtmöglichen Übertragungsgeschwindigkeiten einzusetzen. Übertragungsgeschwindigkeiten von mehr als 2400 bit/sec erschweren darüber hinaus das Abhören erheblich.

  Anschließend muß bei Geschwindigkeiten über 9600 bit/sec überprüft werden, ob die Schnittstelle des IT-Systems, an dem das Modem betrieben werden soll, höhere Geschwindigkeiten zuläßt.

Bei der Auswahl des Modems sollte beachtet werden, daß die Leistungsmerkmale, die für die tatsächlich erreichte Übertragungsgeschwindigkeit ausschlaggebend sind, genormt sind. Dies sind zum einen Normen für die Übertragungsgeschwindigkeit wie V.32bis für 14400 bit/sec und zum anderen Protokolle zur Übertragungsoptimierung durch Datenkompression und Fehlerkorrektur wie MNP 5 oder V.24bis.

- Befehlssatz
  Die meisten Modems arbeiten heute nach dem herstellerabhängigen Hayes-Standard (auch AT-Standard genannt). Aufgrund der weiten Verbreitung dieses Standards kann bei Einsatz eines Modems, das diesen Standard beherrscht, davon ausgegangen werden, daß die Kommunikation mit anderen Modems meist problemlos möglich ist. Bei der Anschaffung von Modems der neuesten Generation sollte bedacht werden, daß die versprochenen hohen Übertragungsraten oftmals nur erreicht werden können, wenn Geräten desselben Herstellers auf beiden Seiten eingesetzt werden.

- Handbuch
  Ein gut lesbares und ausführliches Handbuch ist zur schnellen Installation und bestmöglichen Konfiguration eines Modems wichtig.

- Sicherheitsmechanismen
  Es gibt vielfältige Sicherheitsmechanismen, die in Modems integriert sein können wie Paßwortmechanismus oder Callback-Funktion. Einige Modems bieten sogar die Möglichkeit, die übertragenen Daten zu verschlüsseln.

  Die Anschaffung eines Modems mit Verschlüsselungsoption ist vorteilhaft, wenn regelmäßig Übertragungen großer Datenmengen innerhalb einer Organisation mit verstreuten Liegenschaften durchgeführt werden sollen. Diese Online-Verschlüsselung bedingt einen geringeren organisatorischen Aufwand als das Verschlüsseln der Daten mittels Zusatzprodukten. Generelle Aussagen zur Sicherheit der eingesetzten Algorithmen können nicht gemacht werden. Für den IT-Grundschutz bietet der DES-Algorithmus bei entsprechendem Schlüsselmanagement ausreichende Sicherheit.

  Die vielfach angebotene Callback-Funktion bietet unter Sicherheitsgesichtspunkten den Vorteil, daß auf einfache Weise unautorisierte Anrufer abgewiesen werden können (siehe auch M 5.30 - Aktivierung einer vorhandenen Callback-Option).

M 2.60 Sichere Administration eines Modems

Der sichere Einsatz eines Modems bedingt einige administrative Maßnahmen:

- Die Telefonnummer eines Modem-Zugangs darf nur den Kommunikationspartnern bekanntgegeben werden, um den Zugang vor Einwählversuchen zu schützen. Sie darf nicht im Telefonverzeichnis der Organisation erscheinen.

- Ist ein Modem in einen Netzserver integriert, können Benutzer von ihren Arbeitsplatzrechnern auf das Modem zugreifen. Dann darf ein Zugriff auf die Kommunikationssoftware nur den Benutzern möglich sein, die für die Datenübertragung berechtigt sind (siehe auch M 2.42 - Festlegung der möglichen Kommunikationspartner).

- Außerdem müssen regelmäßig die Einstellungen des Modems und der Kommunikationssoftware überprüft werden sowie die durchgeführten Datenübertragungen protokolliert werden.

- Es muß sichergestellt sein, daß das Modem die Telefonverbindung unterbricht, sobald der Benutzer sich vom System abmeldet. Bei einem Stand-alone-System kann dies dadurch realisiert sein, daß das Modem nur solange mit dem Telefonnetz verbunden ist, wie es für die Datenübertragung eingesetzt wird, und es anschließend ausgeschaltet bzw. von der Leitung getrennt wird. Bei einem im Netzserver integrierten Modem muß dies über die Konfiguration sichergestellt werden. Ein externes Modem kann einfach ausgeschaltet werden. Außerdem müssen alle Benutzer darauf hingewiesen werden, daß nach der Datenübertragung auch das Kommunikationsprogramm zu beenden ist.

- Es muß außerdem darauf geachtet werden, daß nach einem Zusammenbruch der Modem-Verbindung der externe Benutzer automatisch vom IT-System ausgeloggt wird. Andernfalls kann der nächste Anrufer unter dieser Benutzerkennung weiterarbeiten, ohne sich einzuloggen.

M 2.61 Regelung des Modem-Einsatzes
Es ist festzulegen:

- wer der Verantwortliche für den sicheren Betrieb des Modems ist (beispielsweise im Stand-alone Einsatz der IT-Benutzer, in vernetzten Systemen der Administrator),

- wer das Modem benutzen darf,

- in welchen Fällen vertrauliche Informationen bei der Übertragung verschlüsselt werden sollten,

- in welchen Fällen durchgeführte Datenübertragungen zu protokollieren sind (z. B. bei Übermittlung personenbezogener Daten). Bietet die Kommunikationssoftware Protokollierungsfunktion an, sollte diesen im sinnvollen Rahmen genutzt werden.

Alle Login-Vorgänge, ob erfolgreich oder erfolglos, müssen protokolliert werden. Korrekt eingegebene Paßwörter sollten nicht mitprotokolliert werden, es ist aber zu überlegen, die bei erfolglosen Login-Versuchen eingegebenen Paßwörter mitzuprotokollieren, um Paßwort-Attacken zu entdecken.

Indizien für Paßwort-Attacken können z.B. sein: häufige erfolglose Login-Versuche für einen Benutzer, erfolglose Login-Versuche immer vom selben Anschluß, Versuche sich auf verschiedene Benutzernamen anzumelden während einer Verbindung oder von einem Anschluß.

Nach dem Verbindungsaufbau muß dem Anrufenden ein Anmelde-Prompt angezeigt werden. Dabei sollte darauf geachtet werden, daß vor der erfolgreichen Anmeldung möglichst wenig Informationen über das angewählte IT-System weitergegeben werden. Es sollte weder die Art der eingesetzten Hardware noch des Betriebssystems gegeben werden. Der Anmelde-Prompt sollte den Namen des IT-Systems und/oder der Organisation enthalten, einen Hinweis, daß alle Verbindungen protokolliert werden und eine Eingabeaufforderung für Benutzername und Paßwort. Bei erfolglosen Anmeldeversuchen darf keine Ursache angezeigt werden (falscher Benutzername, falsches Paßwort).

Trennung Dial-In / Dial-Out
Für ein- bzw. abgehende Verbindungen sollten getrennte Leitungen und Modems benutzt werden. Ein Anrufer sollte keine Möglichkeit haben, sich über das angewählte IT-System wieder nach außen verbinden zu lassen. (Wenn dies für Außendienstmitarbeiter unbedingt notwendig ist, muß dem eine starke Authentisierung vorangehen, z.B. über Chipkarten.) Ansonsten besteht die Gefahr, daß Hacker den Zugang mißbrauchen, zum einen um teure Fernverbindungen aufzubauen und zum anderen um ihre Spuren zu verwischen.

Beim Callback sollte für den Rückruf ein anderes Modem oder eine andere Leitung benutzt werden, als das anrufende Modem benutzt hat (siehe auch M 5.44 - Einseitiger Verbindungsaufbau).

M 2.62 Software-Abnahme- und Freigabe-Verfahren
Der Einsatz von IT zur Aufgabenbewältigung setzt voraus, daß die maschinelle Datenverarbeitung soweit wie möglich fehlerfrei arbeitet, da die Kontrolle der Einzelergebnisse in den meisten Fällen nicht mehr zu leisten ist. Im Zuge eines Software-Abnahme-Verfahrens wird deshalb überprüft, ob die betrachtete Software fehlerfrei arbeitet, das heißt, ob die Software die erforderliche Funktionalität zuverlässig bereitstellt und ob sie darüber hinaus keine unerwünschten Nebeneffekte hat. Mit der anschließenden Freigabe der Software durch die fachlich zuständige Stelle wird die Erlaubnis erteilt, die Software zu nutzen. Gleichzeitig übernimmt diese Stelle damit auch die Verantwortung für das IT-Verfahren, daß durch die Software realisiert wird.

Bei der Software-Abnahme unterscheidet man sinnvollerweise zwischen Software, die selbst oder im Auftrag entwickelt wurde, und Standardsoftware, die nur für den speziellen Einsatzzweck angepaßt wird.

Abnahme von selbst- oder im Auftrag entwickelter Software
Bevor der Auftrag zur Software-Entwicklung intern oder extern vergeben wird, muß die Anforderungsdefinition für die Software erstellt sein, aus der dann das Grob- und Feinkonzept für die Realisierung entwickelt wird. Anhand dieser Dokumente erstellt die fachlich zuständige Stelle,

nicht die für die Software-Entwicklung zuständige Stelle, im allgemeinen einen Abnahmeplan.

Üblicherweise werden hierzu Testfälle und die erwarteten Ergebnisse für die Software erarbeitet. Anhand dieser Testfälle wird die Software getestet und der Abgleich zwischen berechnetem und erwartetem Ergebnis wird als Indiz für die Korrektheit der Software benutzt.
Zur Entwicklung der Testfälle und zur Durchführung der Tests ist folgendes zu beachten:

- die Testfälle werden von der fachlich zuständigen Stelle entwickelt,
- für Testfälle werden keine Daten des Wirkbetriebs benutzt,
- Testdaten, insbesondere wenn sie durch Kopieren der Wirkdaten erstellt werden, dürfen keine vertraulichen Informationen beinhalten; personenbezogene Daten sind zu anonymisieren oder zu simulieren,
- die Durchführung der Tests darf keine Auswirkungen auf den Wirkbetrieb haben; nach Möglichkeit sollte ein logisch oder physikalisch isolierter Testrechner benutzt werden.

Eine Abnahme ist zu verweigern, wenn:

- Schwerwiegende Fehler in der Software festgestellt werden,
- Testfälle auftreten, in denen die erwarteten Ergebnisse nicht mit den berechneten übereinstimmen,
- Benutzerhandbücher oder Bedienungsanleitungen nicht vorhanden oder von nicht ausreichender Qualität sind und
- Dokumentation der Software nicht vorhanden oder nicht ausreichend ist.

Die Ergebnisse der Abnahme sind schriftlich festzuhalten. Die Dokumentation des Abnahmeergebnisses sollte umfassen:

- Bezeichnung und Versionsnummer der Software und ggf. des IT-Verfahrens,
- Beschreibung der Testumgebung,
- Testfälle und Testergebnisse und
- Abnahmeerklärung.

Abnahme von Standardsoftware
Wird Standardsoftware beschafft, so sollte auch diese einer Abnahme und einer Freigabe unterzogen werden. In der Abnahme sollte überprüft werden, ob

- die Software frei von Computer-Viren ist,
- die Software kompatibel zu den anderen eingesetzten Produkten ist,

- die Software in der angestrebten Betriebsumgebung lauffähig ist und welche Parameter zu setzen sind,
- die Software komplett einschließlich der erforderlichen Handbücher ausgeliefert wurde und
- die geforderte Funktionalität erfüllt wird.

Freigabe-Verfahren
Ist die Abnahme der Software erfolgt, muß die Software für die Nutzung freigegeben werden. Dazu ist zunächst festzulegen, wer berechtigt ist, Software freizugeben. Die Freigabe der Software ist schriftlich festzulegen und geeignet zu hinterlegen.

Die Freigabeerklärung sollte umfassen:

- Bezeichnung und Versionsnummer der Software und ggf. des IT-Verfahrens,
- Bestätigung, daß die Abnahme ordnungsgemäß vorgenommen wurde,
- Einschränkungen für die Nutzung (Parametereinstellung, Benutzerkreis, ...),
- Freigabedatum, ab wann die Software eingesetzt werden darf und
- die eigentliche Freigabeerklärung.

Falls IT-technisch möglich muß verhindert werden, daß Software nach der Freigabe verändert oder manipuliert werden kann. Andernfalls ist dies durch eine Regelung festzulegen.
Auch nach intensiven Abnahmetests kann es vorkommen, daß im laufenden Einsatz Fehler in der Software festgestellt werden. Für diesen Fall ist festzulegen, wie in einem solchen Fehlerfall verfahren werden soll (Ansprechpartner, Fehlerbeseitigungsablauf, Beteiligung der fachlich zuständigen Stelle, Wiederholung der Abnahme und Freigabe, Versionskontrolle). Für weiterführende Erklärungen siehe Kapitel 9.1 - Standardsoftware in [BSI1998].

M 2.63 Einrichten der Zugriffsrechte
Arbeiten mit einem IT-System mehrere Benutzer, so muß durch eine ordnungsgemäße Administration der Zugriffsrechte sichergestellt werden, daß die Benutzer das IT-System nur gemäß ihren Aufgaben nutzen können.

Vorausgesetzt sei, daß von den Fachverantwortlichen die Zugangs- und Zugriffsberechtigungen für die einzelnen Funktionen festgelegt wurden (vgl. M 2.7 - Vergabe von Zugangsberechtigungen und M 2.8 - Vergabe von Zugriffsrechten). Anschließend werden die Benutzer des IT-Systems den einzelnen Funktionen zugeordnet. Die Ergebnisse sind schriftlich zu dokumentieren. Der Administrator muß dann das IT-System so konfigurieren, daß diese Benutzer Zugang zum IT-System erhalten und mit den ihnen zugewiesenen Zugriffsrechten nur ihre Aufgaben wahrnehmen können. Bietet das IT-System keine Möglichkeit, Zugriffsrechte zuzuweisen

(z.B. beim DOS-PC mit mehreren Benutzern), so ist ein Zusatzprodukt zu diesem Zweck einzusetzen (vgl. z.B. M 4.41 Einsatz eines angemessenen PC-Sicherheitsproduktes).

Läßt das IT-System es zu, so sind die sinnvoll einsetzbaren Protokollfunktionen zur Beweissicherung durch den Administrator zu aktivieren. Dazu gehören erfolgreiche und erfolglose An- und Abmeldevorgänge, Fehlermeldungen des Systems, unerlaubte Zugriffsversuche.

Für den Vertretungsfall muß der Administrator vorab kontrollieren, ob der Vertreter vom Fachverantwortlichen autorisiert ist. Erst dann darf er die erforderlichen Zugriffsrechte im akuten Vertretungsfall einrichten.

M 2.64 Kontrolle der Protokolldateien
Die Protokollierung sicherheitsrelevanter Ereignisse ist als Sicherheitsmaßnahme nur wirksam, wenn die protokollierten Daten in regelmäßigen Abständen durch einen Revisor ausgewertet werden. Ist es technisch nicht möglich, die Rolle eines unabhängigen Revisors für Protokolldateien zu implementieren, kann ihre Auswertung auch durch den Administrator erfolgen. Für diesen Fall bleibt zu beachten, daß damit eine Kontrolle der Tätigkeiten des Administrators nur schwer möglich ist. Das Ergebnis der Auswertung sollte daher dem IT-Sicherheitsbeauftragten, dem IT-Verantwortlichen oder einem anderen besonders zu bestimmenden Mitarbeiter vorgelegt werden.

Die regelmäßige Kontrolle dient darüber hinaus auch dem Zweck, durch die anschließende Löschung der Protokolldaten ein übermäßiges Anwachsen der Protokolldateien zu verhindern.

Da Protokolldateien in den meisten Fällen personenbezogene Daten beinhalten, ist sicherzustellen, daß diese Daten nur zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes verwendet werden dürfen (vgl. § 14 Abs. 4 BDSG).

Die nachfolgenden Auswertungskriterien dienen als Beispiele, die Hinweise auf eventuelle Sicherheitslücken, Manipulationsversuche und Unregelmäßigkeiten erkennen lassen:

- Liegen die Zeiten des An- und Abmeldens außerhalb der Arbeitszeit (Hinweis auf Manipulationsversuche)?
- Häufen sich fehlerhafte Anmeldeversuche (Hinweis auf den Versuch, Paßwörter zu erraten)?
- Häufen sich unzulässige Zugriffsversuche (Hinweis auf Versuche zur Manipulation)?
- Gibt es auffällig große Zeitintervalle, in denen keine Protokolldaten aufgezeichnet wurden (Hinweis auf eventuell gelöschte Protokollsätze)?
- Ist der Umfang der protokollierten Daten zu groß (eine umfangreiche Protokolldatei erschwert das Auffinden von Unregelmäßigkeiten)?

- Gibt es auffällig große Zeitintervalle, in denen anscheinend kein Benutzer-Wechsel stattgefunden hat (Hinweis darauf, daß das konsequente Abmelden nach Arbeitsende nicht vollzogen wird)?
- Gibt es auffallend lange Verbindungszeiten in öffentliche Netze hinein (vgl. G 4.25 Nicht getrennte Verbindungen)?
- Wurde in einzelnen Netzsegmenten oder im gesamten Netz eine auffällig hohe Netzlast oder eine Unterbrechung des Netzbetriebes festgestellt (Hinweis auf Versuche, die Dienste des Netzes zu verhindern bzw. zu beeinträchtigen oder auf eine ungeeignete Konzeption bzw. Konfiguration des Netzes)?

Wenn regelmäßig umfangreiche Protokolldateien ausgewertet werden müssen, ist es sinnvoll, ein Werkzeug zur Auswertung zu benutzen. Dieses Werkzeug sollte wählbare Auswertungskriterien zulassen und besonders kritische Einträge (z. B. mehrfacher fehlerhafter Anmeldeversuch) hervorheben.
Das oben gesagte gilt analog auch für die Erhebung von Auditdaten, da es sich dabei im Prinzip nur um die Protokollierung sicherheitskritischer Ereignisse handelt.

M 2.65 Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System
Mittels Protokollauswertung oder durch Stichproben ist in angemessenen Zeitabständen zu überprüfen, ob die Benutzer des IT-Systems sich regelmäßig nach Aufgabenerfüllung abmelden oder ob mehrere Benutzer unter einer Kennung arbeiten.

Sollte festgestellt werden, daß tatsächlich mehrere Benutzer unter einer Kennung arbeiten, sind sie auf die Verpflichtung zum Abmelden nach Aufgabenerfüllung hinzuweisen. Gleichzeitig sollte der Sinn dieser Maßnahme erläutert werden, die im Interesse des einzelnen Benutzers liegt.

Stellt sich heraus, daß die An- und Abmeldevorgänge zu zeitintensiv sind und trotz Aufforderung nicht akzeptiert werden, sollten alternative Maßnahmen diskutiert werden wie zum Beispiel:

- Zuordnung des IT-Systems zu einem Benutzer für bestimmte Zeitintervalle, in denen andere Benutzer das IT-System nicht nutzen dürfen. Dies setzt voraus, daß der Arbeitsprozeß dementsprechend zeitlich variabel ist.
- Anschaffung zusätzlicher IT-Systeme, mit denen die quasiparallele Arbeit an einem IT-System vermieden werden kann. Zu beachten ist, daß zwar die Anschaffungskosten für die zusätzlichen IT-Systeme anfallen, aber andererseits die Anschaffungskosten für PC-Sicherheitsprodukte entfallen können. Anstelle des Bausteins 5.4 DOS-PC (mehrere Benutzer) ist dann die Umsetzung empfohlener Grundschutzmaßnahmen eines anderen Bausteins, z.B 5.1 DOS-PC (ein Benutzer), erforderlich.
- Sollten sich die Datenbestände der einzelnen Benutzer separieren lassen (beispielsweise Benutzer A bearbeitet die Daten A-L, Benutzer B die Daten M-Z), so können dafür unterschiedliche Zugriffsrechte eingeräumt werden. Will ein Benutzer dann mit seinen Daten

arbeiten, muß er sich zuvor beim System anmelden, da seine Kollegen kein Zugriffsrecht auf diese Daten besitzen.

M 2.66 Beachtung des Beitrags der Zertifizierung für die Beschaffung
Bei der Beschaffung von IT-Produkten und IT-Systemen muß frühzeitig festgelegt werden, ob die bloße Zusicherung des Herstellers oder Vertreibers über implementierte Sicherheitsfunktionen als ausreichend vertrauenswürdig anerkannt werden kann. Insbesondere bei einem hohen oder sehr hohen Schutzbedarf kann die Vertrauenswürdigkeit der Produkte in Hinblick auf IT-Sicherheit nur dadurch gewährleistet werden, daß unabhängige Prüfstellen die Produkte untersuchen und bewerten (evaluieren).

Eine allgemein anerkannte Grundlage dieser Evaluierungen bilden die europaweit harmonisierten „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC)" und das Evaluationshandbuch ITSEM. In Deutschland führen das BSI selbst und vom BSI akkreditierte Prüfstellen solche Evaluationen durch. Bei positivem Evaluationsergebnis und bei Einhaltung der Rahmenbedingungen von ITSEC und ITSEM wird für das untersuchte Produkt oder System vom BSI als Zertifizierungsstelle ein Sicherheitszertifikat erteilt.

Aus dem dazugehörenden Zertifizierungsreport geht hervor, welche Funktionalität mit welcher Prüftiefe (Evaluationsstufe E1 geringste Prüftiefe bis Evaluationsstufe E6 höchste Prüftiefe) untersucht wurde und welche Bewertung vorgenommen wurde. Zusätzlich wird die geprüfte Mechanismenstärke der Implementation der Sicherheitsfunktionen angegeben, die ein Maß darstellt für den Aufwand, den man zum Überwinden der Sicherheitsfunktionen aufbringen muß. ITSEC unterscheidet hier die Mechanismenstärken niedrig, mittel und hoch. Darüber hinaus werden Hinweise gegeben, welche Randbedingungen beim Einsatz des Produktes beachtet werden müssen.

Stehen bei der IT-Beschaffung mehrere Produkte mit angemessenem Preis-/Leistungsverhältnis zur Auswahl, so kann ein eventuell vorhandenes Sicherheitszertifikat als Auswahlkriterium positiv berücksichtigt werden. Hierbei sollten Sicherheitszertifikate insbesondere dann berücksichtigt werden, wenn der evaluierte Funktionsumfang die Mindestfunktionalität (weitestgehend) umfaßt und die Mechanismenstärke dem Schutzbedarf entspricht (vgl. M 4.41 - Einsatz eines angemessenen PC-Sicherheitsproduktes). Je höher dann die im Zertifikat angegebene Prüfungstiefe ist, desto mehr Vertrauen in Wirksamkeit und Korrektheit der Sicherheitsfunktionen kann dem Produkt entgegengebracht werden.

Die Zertifzierungsstellen geben regelmäßig Übersichten heraus, welche Produkte ein Zertifikat erhalten haben. Eine Zusammenstellung der vom BSI zertifizierten IT-Produkte und -Systeme kann beim BSI angefordert werden: BSI 7148 - BSI-Zertifikate. Weiterhin veröffentlicht das BSI neu erteilte Zertifikate in der Zeitschrift KES, Zeitschrift für Kommunikations- und EDV-Sicherheit. Diese Informationen lassen sich ebenfalls in der BSI-BOX (s. Anhang in [BSI1998]) per Modem abrufen.

M 2.69 Einrichtung von Standardarbeitsplätzen
Ein Standardarbeitsplatz ist gekennzeichnet durch einheitliche Hardware und Software sowie deren Konfiguration. Die Planung und Einrichtung erfolgt üblicherweise unter den Aspekten der Aufgabenstellung, Zuverlässigkeit, Ergonomie, Geschwindigkeit und Wartbarkeit. Sie wird durch fachkundiges Personal durchgeführt. Die Einrichtung von Standardarbeitsplätzen ist in mehrfacher Hinsicht vorteilhaft:

IT-Sicherheit:

- Standardarbeitsplätze sind leichter in Sicherheitskonzepte einzubinden.
- Der Aufwand für die Dokumentation des IT-Bestandes wird reduziert.

IT-Management:

- Die Beschaffung größerer Stückzahlen gleicher Komponenten ermöglicht Preisvorteile.
- Der Einsatz nicht zulässiger Software ist einfacher festzustellen.
- Durch gleiche IT-Ausstattung entfallen „Neidfaktoren“ zwischen den einzelnen Benutzern.

IT-Nutzer:

- Bei Gerätewechsel ist keine erneute Einweisung in die IT-Konfiguration erforderlich, Ausfallzeiten werden somit minimiert.
- Bei Fragen zu Hard- und Software können sich Anwender gegenseitig helfen.

Systemadministration bei Installation und Wartung:

- Eine gewissenhaft geplante und getestete Installation kann fehlerfrei und mit geringem Arbeitsaufwand installiert werden.
- Die einheitliche Arbeitsumgebung erleichtert den Benutzerservice (Wartung, Support und Pflege).

Schulung:

- Die Teilnehmer werden in dem Umfeld geschult, das sie am Arbeitsplatz vorfinden.

M 2.70 Entwicklung eines Firewall-Konzeptes
Die Vernetzung vorhandener Teilnetze mit globalen Netzen wie dem Internet führt zu einem neuen Informationsangebot. Gleichzeitig führt die zunehmende lokale Vernetzung von Rechnersystemen dazu, daß von jedem Arbeitsplatzrechner aus auf die vielfältigen Informationen zugegriffen werden kann.

Diese Vernetzung läßt aber auch neue Gefährdungen entstehen, da prinzipiell nicht nur ein Informationsfluß von außen in das zu schützende Netz stattfinden kann, sondern auch in die

andere Richtung. Darüber hinaus gefährdet die Möglichkeit remote, d.h. von einem entfernten Rechner aus (z.B. aus dem Internet) Befehle auf Rechnern im lokalen Netz ausführen zu lassen, die Integrität und die Verfügbarkeit der lokalen Rechner und dadurch indirekt auch die Vertraulichkeit der lokalen Daten.

Ein zu schützendes Teilnetz sollte daher nur dann an ein anderes Netz angeschlossen werden, wenn dies unbedingt erforderlich ist. Dies gilt insbesondere für Anschlüsse an das Internet. Dabei ist auch zu prüfen, inwieweit das zu schützende Netz in anschließbare, nicht anschließbare und bedingt anschließbare Teile segmentiert werden muß und ob für die Kopplung mit dem Internet nicht ein Stand-alone-System ausreicht (siehe M 5.46 - Einsatz von Stand-alone-Systemen zur Nutzung des Internets).

Um die Sicherheit des zu schützenden Netzes zu gewährleisten, muß eine geeignete Firewall eingesetzt werden. Damit eine Firewall effektiven Schutz bieten kann, müssen folgende grundlegende Bedingungen erfüllt sein. Die Firewall muß

- auf einer umfassenden Sicherheitspolitik aufsetzen,
- im IT-Sicherheitskonzept der Organisation eingebettet sein,
- korrekt installiert und
- korrekt administriert werden.

Der Anschluß an ein externes Netz darf erst dann erfolgen, wenn überprüft worden ist, daß mit dem gewählten Firewall-Konzept sowie den personellen und organisatorischen Randbedingungen alle Risiken beherrscht werden können.

Es gibt verschiedene Arten der Realisierung einer Firewall. Um festzustellen, welches Firewall-Konzept für den Einsatzzweck am geeignetsten ist, muß zunächst geklärt werden, welche Sicherheitsziele durch die Firewall erfüllt werden sollen. Beispiele für Sicherheitsziele sind:

- Schutz des internen Netzes gegen unbefugten Zugriff von außen,
- Schutz der Firewall gegen Angriffe aus dem externen Netz, aber auch gegen Manipulationen aus dem internen Netz,
- Schutz der lokal übertragenen und gespeicherten Daten gegen Angriffe auf deren Vertraulichkeit oder Integrität,
- Schutz der lokalen Netzkomponenten gegen Angriffe auf deren Verfügbarkeit (Insbesondere gilt dies auch für Informationsserver, die Informationen aus dem internen Bereich für die Allgemeinheit zu Verfügung stellen.),
- Verfügbarkeit der Informationen des externen Netzes im zu schützenden internen Netz, (Die Verfügbarkeit dieser Informationen muß aber gegenüber dem Schutz der lokalen Rechner und Informationen zurückstehen!),

- Schutz vor Angriffen, die auf IP-Spoofing beruhen oder die Source-Routing Option, das ICMP-Protokoll bzw. Routingprotokolle mißbrauchen,

- Schutz vor Angriffen durch das Bekanntwerden von neuen sicherheitsrelevanten Softwareschwachstellen. (Da die Anzahl der potentiellen Angreifer und deren Kenntnisstand bei einer Anbindung an das Internet als sehr hoch angesehen werden muß, ist dieses Sicherheitsziel von besonderer Bedeutung.)

Auf den Sicherheitszielen aufbauend muß eine Sicherheitspolitik erarbeitet werden, in der Aufgaben und Anforderungen an die Firewall festgelegt werden. Diese Sicherheitspolitik muß in die IT-Sicherheitsstrategie der jeweiligen Organisation eingebettet sein und daher mit dem IT-Sicherheitsmanagement vereinbart werden.
Die Umsetzung der Firewall-Sicherheitspolitik erfolgt dann durch die Realisierung der Firewall, durch geeignete Auswahl von Hardware-Komponenten wie Packet-Filter und Application-Gateway und die sorgfältige Implementation von Filterregeln.

Hinweis:
Packet-Filter sind IT-Systeme mit spezieller Software, die die Informationen der unteren Schichten des OSI-Modells filtern und entsprechend spezieller Regeln Pakete weiterleiten oder abfangen (siehe M 2.74 - Geeignete Auswahl eines Packet-Filters). Ein Application-Gateway ist ein Rechner, der die Informationen der Anwendungsschicht filtert und gemäß spezieller Regeln Verbindungen verbieten oder erlauben kann (siehe M 2.75 - Geeignete Auswahl eines Application-Gateway). Während Packet-Filter auf Schicht 3 und 4 des OSI-Modells arbeiten, arbeiten Gateways auf Schicht 7 und sind somit wesentlicher komplexer. Ein Application-Gateway ist im allgemeinen auf einem IT-System implementiert, das ausschließlich für diese Aufgabe eingesetzt wird und dessen Befehlsumfang auf das notwendigste reduziert ist.

Damit eine Firewall einen wirkungsvoller Schutz eines Netzes gegen Angriffe von außen darstellt, müssen einige grundlegende Voraussetzungen erfüllt sein:

- Jede Kommunikation zwischen den beiden Netzen muß ausnahmslos über die Firewall geführt werden. Dafür muß sichergestellt sein, daß die Firewall die einzige Schnittstelle zwischen den beiden Netzen darstellt. Es müssen Regelungen getroffen werden, daß keine weiteren externen Verbindungen unter Umgehung der Firewall geschaffen werden dürfen (siehe auch M 2.77 - Sichere Anordnung weiterer Komponenten).

- Eine Firewall darf ausschließlich als schützender Übergang zum internen Netz eingesetzt werden, daher dürfen auf einer Firewall nur die dafür erforderlichen Dienste verfügbar sein und keine weiteren Dienste wie z.B. Remote-Login angeboten werden.

- Ein administrativer Zugang zur Firewall darf nur über einen gesicherten Weg möglich sein, also z.B. über eine gesicherte Konsole, eine verschlüsselte Verbindung oder ein separates Netz. Zur Aufstellung einer gesicherten Konsole siehe M 1.32 - Geeignete Aufstellung von Konsole, Geräten mit austauschbaren Datenträgern und Druckern.

- Eine Firewall baut auf einer für das zu schützende Netz definierten Sicherheitspolitik auf und gestattet nur die dort festgelegten Verbindungen. Diese Verbindungen müssen nach IP-Adresse, Dienst, Zeit, Richtung und Benutzer getrennt festgelegt werden können.
- Für die Konzeption und den Betrieb einer Firewall muß geeignetes Personal zur Verfügung stehen. Der zeitliche Aufwand für den Betrieb einer Firewall darf nicht unterschätzt werden. Alleine die Auswertung der angefallenen Protokolldaten nimmt erfahrungsgemäß viel Zeit in Anspruch. Ein Firewall-Administrator muß fundierte Kenntnisse über die eingesetzten IT-Komponenten besitzen und auch entsprechend geschult werden.
- Die Benutzer des lokalen Netzes sollten durch den Einsatz einer Firewall möglichst wenig Einschränkungen hinnehmen müssen.

M 2.71 Festlegung einer Sicherheitspolitik für eine Firewall
Für die Erstellung einer Sicherheitspolitik muß als erstes festgelegt werden, welche Arten der Kommunikation mit dem äußeren Netz zugelassen werden. Bei der Auswahl der Kommunikationsanforderungen müssen speziell die folgenden Fragen beantwortet werden:

- Welche Informationen dürfen durch die Firewall nach außen hindurch- bzw. nach innen hereingelassen werden?
- Welche Informationen soll die Firewall verdecken (z.B. die interne Netzstruktur oder die Benutzernamen)?
- Welche Authentisierungsverfahren sollen innerhalb des zu schützendes Netzes bzw. für die Firewall benutzt werden (z.B. Einmalpaßwörter oder Chipkarten)?
- Welche Zugänge werden benötigt (z.B. nur über einen Internet-Service-Provider oder auch über einen Modempool)?
- Welcher Datendurchsatz ist zu erwarten?

Diensteauswahl
Aus den Kommunikationsanforderungen wird dann abgeleitet, welche Dienste im zu sichernden Netz erlaubt und welche verboten werden müssen.

Es muß unterschieden werden zwischen denjenigen Diensten, die für die Benutzer im zu schützenden Netz und denjenigen, die für externe Benutzer zugelassen werden.

Wenn zum Beispiel E-Mail empfangen werden soll, was im allgemeinen die Minimalanforderung ist, muß auf der Firewall das SMTP-Protokoll durchgelassen werden können. Wenn Dateien von externen IT-Systemen geholt werden sollen, muß FTP vorhanden sein. In der Sicherheitspolitik muß für jeden Dienst explizit festgelegt werden, welche Dienste für welche Benutzer und/oder Rechner zugelassen werden sollen und für welche Dienste Vertraulichkeit und/oder Integrität

gewährleistet werden müssen. Es sollten nur die Dienste zugelassen werden, die unbedingt notwendig sind. Alle anderen Dienste müssen verboten werden. Dies muß auch die Voreinstellung sein: Alle Dienste, für die noch keine expliziten Regeln festgelegt wurden, dürfen nicht zugelassen werden. Es muß festgelegt werden, ob und welche der übertragenen Nutzinformationen gefiltert werden sollen (z.B. zur Kontrolle auf Computer-Viren).

Die Sicherheitspolitik sollte so beschaffen sein, daß sie auch zukünftigen Anforderungen gerecht wird, d.h. es sollte eine ausreichende Anzahl von Verbindungsmöglichkeiten vorgesehen werden. Jede spätere Änderung muß streng kontrolliert werden und insbesondere auf Seiteneffekte überprüft werden.

Ausnahmeregelungen, insbesondere für neue Dienste und kurzzeitige Änderungen (z.B. für Tests), müssen vorgesehen werden. Es sind Forderungen an die Filter zu stellen, und zwar einmal an die Filter, die die Informationen der Dienste der Schichten drei und vier des OSI-Schichtenmodells (IP, ICMP, ARP, TCP und UDP) verwenden, sowie an die Filter, die die Informationen der Dienste der Anwendungsschicht (z.B. Telnet, FTP, SMTP, DNS, NNTP, HTTP) verwenden. Einen Überblick, was für einen sicheren Einsatz der einzelnen Protokolle und Dienste zu beachten ist, gibt M 5.39 - Sicherer Einsatz der Protokolle und Dienste. Darauf aufbauend müssen Filterregeln formuliert werden (siehe M 2.76 - Auswahl und Implementation geeigneter Filterregeln).

Neben der sorgfältigen Aufstellung und Umsetzung der Filterregeln sind darüber hinaus folgende organisatorische Regelungen erforderlich:

- Es müssen Verantwortliche sowohl für das Aufstellen als auch für die Umsetzung und das Testen der Filterregeln benannt werden. Es muß geklärt werden, wer befugt ist, die Filterregeln z.B. für Tests neuer Dienste zu verändern.
- Es muß festgelegt werden, welche Informationen protokolliert werden und wer die Protokolle auswertet. Es müssen sowohl alle korrekt aufgebauten als auch die abgewiesenen Verbindungen protokolliert werden. Die Protokollierung muß den datenschutzrechtlichen Bestimmungen entsprechen.
- Die Benutzer müssen über ihre Rechte, insbesondere auch über den Umfang der Nutzdaten-Filterung umfassend informiert werden.
- Angriffe auf die Firewall sollten nicht nur erfolgreich verhindert, sondern auch frühzeitig erkannt werden können. Angriffe können über die Auswertung der Protokolldateien erkannt werden. Die Firewall sollte aber auch in der Lage sein, aufgrund von vordefinierten Ereignissen, wie z.B. häufigen fehlerhaften Paßworteingaben auf einem Application-Gateway oder Versuchen, verbotene Verbindungen aufzubauen, Warnungen auszugeben oder evtl. sogar Aktionen auszulösen.
- Es ist zu klären, welche Aktionen bei einem Angriff gestartet werden, ob z.B. der Angreifer verfolgt werden soll oder ob die Netzverbindungen nach außen getrennt werden sollen. Da

hiermit starke Eingriffe in den Netzbetrieb verbunden sein können, müssen Verantwortliche bestimmt sein, die entscheiden können, ob ein Angriff vorliegt und die entsprechenden Maßnahmen einleiten. Die Aufgaben und Kompetenzen für die betroffenen Personen und Funktionen müssen eindeutig festgelegt sein.

Folgende Fragen müssen bei der Festlegung der Sicherheitspolitik geklärt werden:

- Welcher Schaden kann im zu schützenden Netz verursacht werden, wenn die Firewall überwunden wird? Da es keine absolute Sicherheit geben kann, muß entschieden werden, ob der maximal auftretende Schaden tragbar ist oder ob zusätzliche Maßnahmen ergriffen werden müssen.

- Welche Restrisiken existieren bei einem ordnungsgemäßen Betrieb der Firewall? Dies sind z.B. Schwachstellen in den benutzten Geräten und Betriebssystemen.

- Wie schnell wird ein Angriff auf die Firewall bemerkt?

- Welche Protokoll-Informationen sind auch nach einem erfolgreichen Angriff noch verfügbar?

- Sind die Benutzer bereit, die Einschränkungen durch die Firewall zu akzeptieren?

M 2.72 Anforderungen an eine Firewall
Vor der Beschaffung einer Firewall sollten die folgenden Punkte berücksichtigt werden:

- Die Struktur des zu schützenden Netzes (Rechnernummern, -namen und Mailadressen) muß verdeckt werden können, damit sich keine Rückschlüsse auf die interne Netzstruktur und die internen Anwender ziehen lassen. Dies läßt sich z.B. durch den Einsatz eines Application-Gateways und zweier DNS-Server erreichen.

- Die Firewall sollte in der Lage sein, bestimmte Rechner mit einem geringeren Schutzbedarf gegen Angriffe zu schützen, ohne daß diese Rechner im zu schützenden Netz stehen müssen. Für diese Rechner brauchen dann keine benutzerspezifischen Filterregeln festgelegt werden. Dies können z.B. Informationsserver sein, die an einem dedizierten Interface eines Packet-Filter oder des Application-Gateways (Multi-Homed Gateway) angeschlossen sind (siehe auch Abb. 1 in M 2.77 - Sichere Anordnung weiterer Komponenten).

- Die Verwaltung der Komponenten muß zentral über einen vertrauenswürdigen Pfad (z.B. über ein separates Netz oder eine verschlüsselte Verbindung) erfolgen und übersichtlich sein (z.B. über ein graphisches Interface auf einem separatem Rechner). Die Verwaltung sollte auf einem separatem Rechner erfolgen, d.h. die dafür erforderliche Management-Plattform sollte sich auf einem separatem Rechner befinden, damit auf der Firewall selber keine komplexe und damit fehleranfällige Software wie X-Windows erforderlich ist.

- Empfehlenswert ist eine Firewall-Anordnung, die aus mindestens zwei getrennten Einheiten besteht. Die Einheiten müssen hintereinander angeordnet sein, so daß für eine Verbindung zwischen den beiden beteiligten Netzen beide Einheiten passiert werden müssen. Die Einheiten sollten mit unterschiedlichen Betriebssystemen arbeiten und unterschiedliche Formate für die Beschreibung der Filterregeln benutzen.
  Die beiden Einheiten können z.B. ein Packet-Filter und ein Application-Gateway sein. Hierdurch wird sichergestellt, daß Fehler, die bei der Verwaltung einer Komponente gemacht werden, von der richtig konfigurierten anderen Komponente abgefangen werden.

M 2.73 Auswahl eines geeigneten Firewall-Typs
Nachdem eine Sicherheitspolitik für die Firewall festgelegt worden ist, muß entschieden werden, mit welchen Komponenten die Firewall realisiert werden soll. Dafür ist eine geeignete Anordnung auszuwählen.

Es gibt beispielsweise die folgenden Anordnungsmöglichkeiten

- Ausschließlicher Einsatz eines Packet-Filters Diese Anordnung besteht ausschließlich aus einem Packet-Filter, der die Informationen der unteren Schichten filtert und gemäß spezieller Regeln Pakete weiterleitet oder abweist.

- Dual-homed Gateway Diese Anordnung besteht aus einem Application-Gateway, das mit zwei Netz-Interfaces ausgerüstet ist und als alleiniger Übergang zwischen zwei Netzen eingesetzt wird. Application-Gateways filtern Informationen auf Schicht 7 des OSI-Schichtenmodells. Das Dual-homed Gateway muß so konfiguriert werden, daß keine Pakete ungefiltert passieren können, d.h. insbesondere, daß IP-Forwarding abgeschaltet werden muß.

- Screened-Subnet Bei einem Screened-Subnet handelt es sich um ein Teilnetz zwischen einem zu schützenden Netz und einem externen Netz, in dem Firewall-Komponenten für die Kontrolle der Verbindungen und Pakete sorgen.

  Ein Screened-Subnet besteht aus einem Application-Gateway und einem oder zwei Packet-Filtern. Die Packet-Filter befinden sich vor und/oder hinter dem Gateway und bilden mit diesem ein Teilnetz. Ein Screened-Subnet kann z.B. ein Dual-homed Gateway enthalten. Die Filterregeln werden so gestaltet, daß jede Verbindung von innen oder außen über das Gateway gehen muß.

Im folgenden werden Vor- und Nachteile der jeweiligen Anordnungsmöglichkeiten aufgezeigt.

Ausschließlicher Einsatz eines Packet-Filters
Vorteile:

- leicht realisierbar, da die Funktionalität von vielen Routern geliefert wird
- leicht erweiterbar für neue Dienste

Nachteile:

- IP-Spoofing u. U. möglich
- alle Dienste, die gestattet werden sollen, müssen auf allen Rechnern, die erreicht werden können, sicher sein
- komplexe Filterregeln
- keine Testmöglichkeiten, es ist insbesondere nicht möglich festzustellen, ob die Filterregeln in ihrer Reihenfolge verändert werden, was bei einigen Routern geschieht, um den Durchsatz zu steigern
- keine ausreichende Protokollierungsmöglichkeit

Diese Anordnung kann nur in kleinen Netzen eingesetzt werden, in denen alle Rechner gegen Angriffe abgesichert sind.

Dual-homed Gateway
Vorteile:

- umfangreiche Protokollierung möglich
- interne Netzstruktur wird verdeckt

Nachteile:

- relativ hoher Preis (da ein leistungsfähiger Rechner mit zwei Netz-Interfaces benötigt wird)
- Probleme bei neuen Diensten
- die Übernahme des Application-Gateways durch den Angreifer führt zu einem vollständigen Verlust der Sicherheit

Ein zusätzlicher Schutz läßt sich durch den Einsatz eines Packet-Filters vor dem Gateway erreichen, wie z.B. durch einen vorhandenen Router. In diesem Fall müßten Router und Gateway durchbrochen werden, um Zugang zum zu schützenden Netz zu erhalten.

Screened-Subnet
Vorteile:

- kein direkter Zugang zum Gateway möglich (bei Konfigurationen 1 und 2)
- die Struktur des internen Netzes wird verdeckt

- vereinfachte Regeln für die Packet-Filter
- zusätzliche Sicherheit durch einen zweiten Packet-Filter (bei Konfigurationen 1 und 2)
- durch den Einsatz mehrerer Gateways läßt sich die Verfügbarkeit steigern
- umfangreiche Protokollierung möglich

Nachteile:

- hoher Preis (da ein leistungsfähiger Rechner mit ein oder zwei Netz-Interfaces sowie mindestens ein Packet-Filter benötigt wird)
- wenn in einem Screened-Subnet mit einem Application-Gateway mit einem Interface die Packet-Filter manipuliert werden (siehe Konfiguration 2, 4 und 6), ist eine direkte Verbindung unter Umgehung des Gateways möglich. Dies kann evtl. auch eine gewünschte Funktionalität sein (z.B. bei neuen Diensten)

Auf Grund der oben beschriebenen Vor- und Nachteile der verschiedenen Anordnungen kann nur ein Screened-Subnet mit einem Dual-homed Gateway (Konfiguration 1) empfohlen werden. In diesem Fall befindet sich das Gateway zwischen dem zu schützenden und dem externen Netz und muß auf jeden Fall passiert werden.

Auf dem Application-Gateway laufen sogenannte Proxy-Prozesse, die den Verbindungsaufbau zum Zielrechner durchführen, nachdem eine Authentisierung des Benutzers stattgefunden hat, und die Daten gemäß den Informationen der Anwendungsschicht filtern. Verbindungen, für die keine Proxy-Prozesse existieren, sind nicht möglich.

Die flexiblere, aber unsicherere Lösung eines Application-Gateways mit nur einem Interface (Konfiguration 2) sollte nur dann benutzt werden, wenn die höhere Flexiblität unverzichtbar ist.

Die beteiligten Rechner müssen so eingerichtet werden, daß nur die unbedingt notwendigen Programme auf ihnen laufen (Minimal-System), diese richtig konfiguriert sind und alle bekannten Schwachstellen beseitigt werden.

M 2.74 Geeignete Auswahl eines Packet-Filters
Packet-Filter sind Router oder Rechner mit spezieller Software, welche die in den Schichten drei und vier der TCP/IP Protokollfamilie (IP, ICMP, ARP, TCP und UDP) vorhandenen Informationen zum Filtern der Pakete benutzen. Hierzu werden Access- bzw. Deny-Listen benutzt.

Sollte ein Packet-Filter für eine Firewall benötigt werden, so sind bei der Beschaffung folgende Forderungen zu stellen:

- Die Filterung muß getrennt für jedes Interface möglich sein.

- Die Filterung muß getrennt nach Quell- und Zieladresse für einzelne Rechner oder für komplette Teilnetze möglich sein.
- Die Filterung muß getrennt nach Quell- und Zielport möglich sein.
- Die Reihenfolge der Filterregeln darf nicht automatisch vom Packet-Filter verändert werden.
- Wenn mehr als zwei Interfaces vorhanden sind, muß eine Filterung getrennt für kommende und gehende Pakete möglich sein.
- Die Eingabe und Kontrolle der Filterregeln muß einfach und übersichtlich sein, z.B. durch symbolische Angabe von Dienst- und Protokollnamen.
- Bei TCP-Paketen muß eine Unterscheidung, ob ein Verbindungsaufbau stattfindet oder eine bestehende Verbindung benutzt wird, d.h. eine Unterscheidung zwischen ACK und ACK-losen Paketen, möglich sein.
- Die Protokollierung von IP-Nummer, Dienst, Zeit und Datum für jedes Paket muß durchführbar sein, wobei auch Einschränkungen auf bestimmte Pakete (z.B. nur Pakete mit einer speziellen Quell-Adresse) möglich sind.
- Sämtliche Protokollinformationen müssen an einen externen Host geschickt werden können.
- Spezielle, einstellbare Ereignisse müssen zu einer unverzüglichen Warnung führen (z.B. mehrfache fehlerhafte Authentisierungsversuche).
- Im Falle, daß ein Router als Packet-Filter eingesetzt wird, muß es möglich sein, statische Routingtabellen zu benutzen. Es sei aber darauf hingewiesen, daß Router in der Regel nicht als Packet-Filter eingesetzt werden sollten, da sie einen sehr umfangreichen Funktionsumfang haben und somit die Filtereigenschaften oftmals nur als Add-on angeboten werden - mit entsprechenden Konsequenzen bei der Erstellung und Prüfung der entsprechenden Software.
- Im Falle, daß ein Router als Packet-Filter eingesetzt wird, muß das dynamische Routing so konfigurierbar sein, daß Routing-Pakete (z.B. RIP), die das zu schützende Netz betreffen, nur an dem Interface zugelassen werden, das auch mit dem zu schützenden Netz verbunden ist.
- Source-Routing Informationen müssen standardmäßig ignoriert werden.
- Der Packet-Filter sollte ggf. eine dynamische Paket-Filterung unterstützen. D.h., daß z.B. bei der Übertragung von UDP-Paketen der entsprechende Kontext für eine gewisse Zeitspanne gespeichert wird und die zugehörigen Antwortpakete hindurchgelassen werden.

M 2.75 Geeignete Auswahl eines Application-Gateway
Ein Application-Gateway ist ein Rechner, der die in der Anwendungsschicht vorhandenen Informationen zum Filtern von Verbindungen nutzt.

Dies können z.B. Benutzernamen in Verbindung mit einer starken Authentisierung, spezielle Informationen in den übertragenen Daten (z.B. Kontrolle auf Computer-Viren) oder Informationen der Anwendungsschicht sein. Ein Application-Gateway bietet darüber hinaus die Möglichkeit, einen einheitlichen Zugang zum zu schützenden Teilnetz zu schaffen und die Struktur dieses Netzes zu verdecken. Die auf dem Application-Gateway laufenden Filterprozesse werden als Proxy-Prozesse bezeichnet.

Sollte ein Application-Gateway für eine Firewall benötigt werden, so sind bei der Beschaffung folgende Forderungen zu stellen:

- Es müssen alle wesentlichen Protokolle (wie Telnet, FTP, SMTP, DNS, NNTP, HTTP) der Anwendungsschicht behandelt werden.
- Für jedes unterstützte Protokoll muß eine Filterung nach allen in Maßnahme M 2.76 - swahl und Implementation geeigneter Filterregeln spezifizierten Informationen möglich sein. Insbesondere müssen die Filterregeln benutzerabhängig formulierbar sein, und es muß möglich sein, mehrere Benutzer zu einer Gruppe zusammenzufassen.
- Bei dem Einsatz eines Application-Gateways sollte keine Änderung der Software im zu schützenden Netz oder im externen Netz nötig sein.
- Die Eingabe und Kontrolle der Filterregeln muß einfach und übersichtlich sein.
- Die eingesetzten Programme müssen gut dokumentiert sein.
- Es muß leicht möglich sein, neue Protokolle hinzuzufügen.
- Für jede aufgebaute und abgewiesene Verbindung muß eine Protokollierung von Benutzer-Identifikation, IP-Nummer, Dienst, Zeit und Datum durchgeführt werden können, wobei auch Einschränkungen auf bestimmte Verbindungen (z.B. für einen speziellen Benutzer) möglich sein sollten.
- Die Protokollinformationen müssen an einen externen Host geschickt werden können.
- Spezielle, einstellbare Ereignisse müssen zu einer unverzüglichen Warnung führen (z.B. mehrfache fehlerhafte Authentisierungsversuche).
- Zur Benutzer-Identifikation müssen starke Authentisierungsmethoden verwendet werden.
- Vom Application Gateway müssen virtuelle private Netze unterstützt werden.

M 2.76 Auswahl und Implementation geeigneter Filterregeln
Das Aufstellen und die notwendige Aktualisierung der Filterregeln für eine Firewall ist keine einfache Aufgabe. Der Administrator muß dafür fundierte Kenntnisse der eingesetzten Protokolle besitzen und entsprechend geschult werden.

Beim Aufstellen der Filterregeln sollten folgende Punkte beachtet werden:

- Die Regeln sollten so formuliert werden, daß alle Zugänge, die nicht explizit erlaubt werden, verboten sind.
- Falls es Bedarf für eine benutzerspezifische Authentisierung gibt, muß geklärt werden, welche Benutzer sich im inneren Netz befinden, welche Dienste diese anwenden dürfen und welche Authentisierungsverfahren eingesetzt werden sollen.
- Es müssen alle Rechner, die sich im inneren Netz befinden, berücksichtigt werden.
- Es muß festgelegt werden, welche Dienste zu welchen Zeiten zur Verfügung stehen sollen. Wenn eine Organisation festgelegte Arbeitszeiten hat, Mitarbeiter z.B. nur zwischen 7.00 und 19.00 Uhr anwesend sein können, sollten außerhalb der üblichen Arbeitszeiten auch keine Verbindungen aufgebaut werden können.

Die Filterregeln sollten in einer Tabelle zusammengefaßt werden, deren eine Achse die Zielrechnernummern und deren andere Achse die Quellrechnernummern enthält. Die Einträge enthalten dann die erlaubten Portnummern, dabei ist die obere der Quell-, die untere der Zielport. Packet-Filter können die Überprüfung der Pakete unmittelbar nach dem Empfang oder vor der Weiterleitung durchführen. Hierbei sollte beachtet werden, daß eine Filterung der in den Packet-Filter eingehenden Pakete durchgeführt werden sollte. Außerdem müssen die Packet-Filter so konfiguriert werden, daß als Absenderadresse nur die Nummern der an dem Interface angeschlossenen Rechner zugelassen werden. Adressen, die mit den anderen Interfaces verknüpft sind, dürfen nicht durchgelassen werden. Dies verringert die Gefahr von IP-Spoofing Angriffen.

Diese Tabelle muß dann in entsprechende Filterregeln umgesetzt werden. Dies ist häufig nicht einfach und muß deshalb sehr genau kontrolliert werden. Durch regelmäßige Tests muß überprüft werden, daß alle Filterregeln korrekt umgesetzt worden sind. Insbesondere muß sichergestellt werden, daß nur die Dienste zugelassen werden, die in der Sicherheitspolitik vorgesehen sind. Für die Regeln eines Application-Gateways sind analoge Tabellen zu erstellen und in die entsprechenden Filterregeln umzusetzen.

M 2.77 Sichere Anordnung weiterer Komponenten
Neben Installation und Betrieb der Firewall müssen auch weitere Komponenten, die der Kommunikation zwischen geschütztem und externem Netz dienen, sicher angeordnet werden. Dazu gehören z.B. Informationsserver für die Bereitstellung von Informationen an interne oder externe Benutzer, Mail-Server und DNS-Server.

Für die Anordnung weiterer Komponenten ist zu unterscheiden, ob diese im zu schützenden Netz, im Screened-Subnet oder auf der externen Seite der Firewall aufgestellt werden sollen. Zur besseren Differenzierung wird der Bereich zwischen dem inneren Packet-Filter und dem Application-Gateway im folgenden auch als internes Screened-Subnet bezeichnet, der Bereich zwischen dem Application-Gateway und dem äußeren Packet-Filter als externes Screened-Subnet.

Externe Zugänge
Weitere externe Zugänge zum zu schützenden Netz, z.B. mit telnet über einen Modempool, sollten wie Zugänge aus dem unsicheren Netz behandelt werden. Dies läßt sich erreichen, indem z.B. ein Terminalserver mit angeschlossenen Modems auf die externe Seite der Firewall gestellt wird, so daß ein Zugang von dort nur über Telnet zum internen Rechner durchgeführt werden kann. Beim Einsatz von virtuellen privaten Netzen (VPNs) kann es auch sinnvoll sein, den notwendigen Zugang über ein weiteres Interface am Application Gateway zu realisieren.

Es müssen klare Regelungen darüber getroffen werden, daß keine externen Zugänge unter Umgehung der Firewall geschaffen werden. Diese Regelungen müssen allen Mitarbeitern bekanntgemacht werden. Es muß sichergestellt werden, daß sowohl das IT-Sicherheitsmanagement als auch der Firewall-Administrator rechtzeitig über entsprechende Pläne unterrichtet wird, um eine Einbettung in das IT-Sicherheitskonzept und die Firewall-Sicherheitspolitik zu gewährleisten.

Anordnung von Informationsservern
Informationsserver, die für die Bereitstellung von Informationen an externe Benutzer dienen, müssen außerhalb der Firewall stehen und wie andere im externen Netz vorhandene Server betrachtet werden. Ihre Verwaltung sollte entweder lokal oder über spezielle zeitlich begrenzte Zugänge vom geschützten Netz erfolgen. Die Daten sollten auf schreibgeschützten Datenträgern liegen.
Gibt es Daten, die nur für die Benutzer des zu schützenden Netzes erreichbar sein sollen, ist es sinnvoll, weitere Informationsserver im internen Screened-Subnet (siehe Abb. 277-1 in [BSI1998]) einzusetzen. Diese sind dann von außen nicht erreichbar und gegen Angriffe von innen durch den Packet-Filter geschützt.

Anordnung der Mail-Server
Ein Mail-Server innerhalb des geschützten Netzes wird zur Verwaltung der Alias-Datenbank, mit der die Benutzeradressen auf ein einheitliches Format umgesetzt werden können, für einen evtl. POP-Daemon oder auch als Gateway zum Übergang in ein anderes Mailsystem (z.B. X.400) eingesetzt. Alle internen Mails werden an diesen Server geschickt und von dort ggf. über einen externen Mail-Server nach außen weitergeleitet.

Der externe Mail-Server im externen Screened-Subnet stellt die Verbindungen mit externen Rechnern her und nimmt die Mails von dort entgegen, so daß die interne Struktur des geschützten Netzes verdeckt wird. Diese Funktion kann auch vom Application-Gateway wahrgenommen

werden.

Durch diese Konfiguration wird erreicht, daß interne Mails nicht in das äußere Netz gelangen und eine einheitliche Adreßstruktur benutzt werden kann.

Anordnung der DNS-Server
Der Domain Name Service (DNS) dient zur Umsetzung von Rechnernamen in IP-Nummern und umgekehrt und stellt ferner Informationen über im Netz vorhandene Rechnersysteme zur Verfügung. DNS-Informationen sollten vor der Außenwelt, d.h. dem Internet oder anderen externen Netzen, verborgen werden. Der bekannteste Ansatz zur Umsetzung dieser Forderung geht von einer speziellen Anordnung zweier DNS-Server (Nameserver) aus. Ein DNS-Server im internen Screened-Subnet verdeckt die Struktur des zu schützenden Netzes und kommuniziert mit einem DNS-Server im externen Screened-Subnet, um Namen von externen Rechnern umzusetzen. Da DNS-Clients sich nicht notwendigerweise mit einem DNS-Server auf denselben Rechnern unterhalten müssen, ist es möglich, beide Prozesse auf unterschiedlichen Rechnern ablaufen zu lassen.

Der externe DNS-Server muß so konfiguriert werden, daß er behauptet, die Autorität für die Domäne des zu schützenden Netzes zu sein (Primary-Server). Natürlich weiß dieses System nur das, was der Außenwelt bekanntgegeben werden soll, also Namen und IP-Nummern des externen Mail-Servers, des Application-Gateways und des externen Informationsservers. Es handelt sich dann um einen Public-DNS-Server.

Der interne DNS-Server muß auch so konfiguriert werden, daß er behauptet, die Autorität für die Domain des zu schützenden Netzes darzustellen. Im Gegensatz zum externen DNS-Server verwaltet dieser Privat-DNS-Server aber alle internen DNS-Informationen und leitet Suchanfragen interner Rechner über externe Hosts an den externen DNS-Server weiter.
Alle DNS-Clients einschließlich der auf dem Application-Gateway müssen so konfiguriert werden, daß sie immer den internen DNS-Server benutzen (z.B. mittels Einträgen in der Datei /etc/resolv.conf).

Fragt nun ein interner Client nach einem internen Rechner, wird der interne DNS-Server benutzt. Fragt ein interner Client oder ein Client auf dem Application-Gateway nach einem externen Rechner, wird der interne DNS-Server befragt, der wiederum den externen DNS-Server befragt, der wiederum das Internet befragt, das eine Antwort zurückgibt.

Ein externer Client, der nach einem internen Host fragt, erhält die eingeschränkte Liste vom externen DNS-Server. Der eingesetzte Packet-Filter muß so konfiguriert werden, daß zwischen den Servern nur der DNS-Dienst gestattet ist, d.h. DNS Port 53 als Quell- und Zielport. Die Freigabe weiterer Ports (> 1023) ist also nicht nötig.

M 2.78 Sicherer Betrieb einer Firewall
Für einen sicheren Betrieb einer Firewall sind die umgesetzten Sicherheitsmaßnahmen regelmäßig auf ihre korrekte Einhaltung zu überprüfen. Insbesondere müssen die für den Betrieb der

Firewall getroffenen organisatorische Regelungen regelmäßig/sporadisch auf ihre Einhaltung überprüft werden. Es sollte in zyklischen Abständen kontrolliert werden, ob neue Zugänge unter Umgehung der Firewall geschaffen wurden.

Durch regelmäßige Tests muß außerdem überprüft werden, daß alle Filterregeln korrekt umgesetzt worden sind. Dabei ist zu testen, daß nur die Dienste zugelassen werden, die in der Sicherheitspolitik vorgesehen sind.

Falls nachträgliche Änderungen der Sicherheitspolitik erforderlich sind, müssen diese streng kontrolliert werden und insbesondere auf Seiteneffekte überprüft werden.

Die bei der Beschaffung an Packet-Filter bzw. an Application-Gateways gestellten Forderungen sind umzusetzen. Sie sind regelmäßig zu aktualisieren und auf Vollständigkeit zu prüfen.

Die Defaulteinstellung der Filterregeln und die Anordnung der Komponenten muß sicherstellen, daß alle Verbindungen, die nicht explizit erlaubt sind, blockiert werden. Dies muß auch bei einem völligen Ausfall der Firewall-Komponenten gelten. Es muß die Regel „Alles was nicht ausdrücklich erlaubt ist, ist verboten“ realisiert sein. So darf z.B. ein Benutzer, der keinen Eintrag in einer Access-Liste hat, keine Möglichkeit haben, Dienste des Internets zu benutzen.

Darüber hinaus sind die folgenden Punkte zu beachten:

- Um ein Mitlesen oder Verändern der Authentisierungsinformationen zu verhindern, dürfen sich Administrator und Revisor nur über einen vertrauenswürdigen Pfad authentisieren. Dies könnte z. B. direkt über die Konsole, eine verschlüsselte Verbindung oder ein separates Netz erfolgen.

- Es müssen in regelmäßigen Abständen Integritätstests der eingesetzten Software durchgeführt werden und im Fehlerfall die Firewall abgeschaltet werden.

- Die Firewall muß auf ihr Verhalten bei einem Systemabsturz getestet werden. Insbesondere darf kein automatischer Neustart möglich sein, und die Access-Listen müssen auf einem schreibgeschützten Medium speicherbar sein. Die Access-Listen sind die wesentlichen Daten für den Betrieb der Firewall und müssen besonders gesichert werden, damit keine alten oder fehlerhaften Access-Listen bei einem Neustart benutzt werden, der durch einen Angreifer provoziert wird.
  Bei einem Ausfall der Firewall muß sichergestellt sein, daß in dieser Zeit keine Netzverbindungen aus dem zu schützenden Netz heraus oder zu diesem aufgebaut werden können.

- Auf den eingesetzten Komponenten dürfen nur Programme, die für die Funktionsfähigkeit der Firewall nötig sind, vorhanden sein. Der Einsatz dieser Programme muß ausführlich dokumentiert und begründet werden. Beispielsweise sollte die Software für die graphische Benutzeroberfläche entfernt werden sowie alle Treiber, die nicht benötigt werden. Diese sollten auch aus dem Betriebssystem-Kern entfernt werden. Das Verbleiben von Software muß dokumentiert und begründet werden.

- Beim Wiedereinspielen von gesicherten Datenbeständen muß darauf geachtet werden, daß für den sicheren Betrieb der Firewall relevante Dateien wie Access-Listen, Paßwortdateien oder Filterregeln auf dem aktuellsten Stand sind.

M 2.79 Festlegung der Verantwortlichkeiten im Bereich Standardsoftware
Vor der Einführung von Standardsoftware müssen eine Reihe von Verantwortlichkeiten geregelt werden. Beispielhaft seien die Verantwortlichkeiten genannt für die Erstellung eines Anforderungskataloges, die Vorauswahl von Produkten, das Testen und Freigeben und die Installation.

Nachfolgend wird zum Vergleich aufgezeigt, wie diese Verantwortlichkeiten sinnvoll verteilt werden können. Da jedoch die Bezeichnungen in den meisten Organisationen voneinander abweichen, werden vorab einige Instanzen anhand ihrer Aufgaben definiert, denen anschließend die einzelnen Verantwortlichkeiten zugeordnet werden können:

- Die Fachabteilung ist der Anwender der Standardsoftware. Sie äußert ihren Bedarf an neuer Software und gibt damit den Anstoß zu deren Beschaffung. Sie wird bei Vorauswahl und Test beteiligt, um die Anforderungen der Anwender einzubringen.

- Die Behörden-/Unternehmensleitung ist verantwortlich für die Freigabe von Standardsoftware. Diese Verantwortung wird meist an den Leiter der Fachabteilung delegiert, womit nach Freigabe die Verantwortung für den korrekten Einsatz der Standardsoftware auf die Fachabteilung übergeht.

- Der IT-Bereich hat die Aufgabe, IT-Lösungen für die Erfüllung der Aufgaben der Fachabteilung bereitzustellen und den sicheren und zuverlässigen Betrieb der IT zu gewährleisten.

- Die Beschaffungsstelle muß die Interoperabilität und Kompatibilität der zu beschaffenden Standardsoftware sowie die Einhaltung von Hausstandards und gesetzlichen Vorschriften sicherstellen. Oft gibt es in den einzelnen Fachabteilungen IT-Koordinatoren, die Teile der Aufgaben der Beschaffungsstelle für die Fachabteilung beratend wahrnehmen und evtl. auch die Haushaltsmittel der Fachabteilung koordinieren.

- Der Haushalt ist verantwortlich für das Rechnungswesen, die IT-Budgetverwaltung und für die Bereitstellung der benötigten Haushaltsmittel.

- Der IT-Sicherheitsbeauftragte muß überprüfen, ob mit den eingesetzten oder zu beschaffenden Produkte ein angemessenes IT-Sicherheitsniveau gewährleistet werden kann. Im Rahmen des IT-Sicherheitsmanagements (vgl. Teil 1, Kapitel 1 in [BSI1998]) muß er die IT-Sicherheit im laufenden Betrieb sicherstellen.

- Der Datenschutzbeauftragte muß die Einhaltung der datenschutzrechtlichen Bestimmungen und eines ausreichenden Schutzes personenbezogener Daten gewährleisten.

- Der Personal- bzw. Betriebsrat muß in vielen Fällen bei der Auswahl neuer Standardsoftware beteiligt werden, insbesondere wenn damit größere Änderungen im Arbeitsablauf

verbunden sind oder wenn die zu beschaffende Software zur Leistungskontrolle geeignet ist (siehe M 2.40 - Rechtzeitige Beteiligung des Personal- / Betriebsrates).

Im Gesamtprozeß „Standardsoftware“ muß für jeden einzelnen Schritt festgelegt werden, welche der zuvor beschriebenen Instanzen für die Durchführung verantwortlich sind und welche Instanzen dabei beteiligt werden müssen. Eine mögliche sinnvolle Verantwortungsverteilung ist zur Orientierung in nachfolgender Tabelle zusammengefaßt:

	verantwortlich	**zu beteiligen**
Erstellung des Anforderungskatalogs	Fachabteilung, IT-Bereich	Beschaffungsstelle, Haushälter, IT-Sicherheitsbeauftragter, Datenschutzbeauftragter, Personal- oder Betriebsrat
Vorauswahl eines geeigneten Produktes	Beschaffungsstelle	IT-Bereich, Fachabteilung
Testen	Fachabteilung und IT-Bereich	IT-Sicherheitsbeauftragter, Datenschutzbeauftragter, Personal- oder Betriebsrat
Freigabe	Behörden-/Unternehmensleitung evtl. delegiert an Leiter Fachabteilung	-
Beschaffung	Beschaffungsstelle	Haushalt
Sicherstellen der Integrität der Software	IT-Bereich	-
Installation und Konfiguration	IT-Bereich	-
Versionskontrolle und Lizenzverwaltung	IT-Bereich	-
Deinstallation	IT-Bereich	-
Kontrolle des IT-Betriebs	IT-Sicherheitsbeauftragter	-

Die getroffenen Zuordnungen sind verbindlich festzuschreiben und deren Einhaltung ist periodischen Kontrollen zu unterziehen.

M 2.80 Erstellung eines Anforderungskataloges für Standardsoftware
Zur Lösung einer Aufgabe, die mit IT bearbeitet wird, bietet der Markt meist eine Vielzahl gleichartiger Standardsoftwareprodukte an. In ihrer Grundfunktionalität vergleichbar, unterscheiden sie sich jedoch in Kriterien wie Anschaffungs- und Betriebskosten, Zusatzfunktionalitäten, Kompatibilität, Administration, Ergonomie und IT-Sicherheit.

Anforderungskatalog
Für die Auswahl eines geeigneten Produktes muß daher zunächst ein Anforderungskatalog erstellt werden. Der Anforderungskatalog sollte u.a. zu den folgenden Punkten Aussagen enthalten:

- Funktionale Anforderungen, die das Produkt zur Unterstützung der Aufgabenerfüllung der Fachabteilung erfüllen muß. Die für die Fachaufgabe relevanten Einzelfunktionalitäten sollten hervorgehoben werden.
- IT-Einsatzumgebung, diese wird einerseits beschrieben durch die Rahmenbedingungen, die durch die vorhandene oder geplante IT-Einsatzumgebung vorgegeben werden, und andererseits durch die Leistungsanforderungen, die durch das Produkt an die Einsatzumgebung vorgegeben werden.
- Kompatibilitätsanforderungen zu anderen Programmen oder IT-Systemen, also Migrationsunterstützung und Aufwärts- und Abwärtskompatibilität.
- Performanceanforderungen beschreiben die erforderlichen Leistungen hinsichtlich Durchsatz und Laufzeitverhalten. Für die geforderten Funktionen sollten möglichst genaue Angaben über die maximal zulässige Bearbeitungszeit getroffen werden.
- Interoperabilitätsanforderungen, d. h. die Zusammenarbeit mit anderen Produkten über Plattformgrenzen hinweg muß möglich sein.
- Zuverlässigkeitsanforderungen betreffen die Stabilität des Produktes, also Fehlererkennung und Toleranz sowie Ausfall- und Betriebssicherheit.
- Konformität zu Standards, dies können internationale Normen, De-facto-Standards oder auch Hausstandards sein.
- Einhaltung von internen Regelungen und gesetzlichen Vorschriften (z.B. ausreichender Datenschutz bei der Verarbeitung personenbezogener Daten)
- Anforderungen an die Benutzerfreundlichkeit, die durch die leichte Bedienbarkeit, Verständlichkeit und Erlernbarkeit gekennzeichnet ist, also insbesondere durch die Güte der Benutzeroberfläche sowie die Qualität der Benutzerdokumentation und der Hilfefunktionen.

- Anforderungen an die Wartbarkeit ergeben sich für den Anwender hauptsächlich aus der Fehlerbehandlung des Produktes.
- die Obergrenze der Kosten, die durch die Beschaffung dieses Produktes verursacht würden, werden vorgegeben. Dabei müssen nicht nur die unmittelbaren Beschaffungskosten für das Produkt selber einbezogen werden, sondern auch Folgekosten, wie z.B. eine Aufrüstung der Hardware, Personalkosten oder notwendige Schulungen.
- Aus den Anforderungen an die Dokumentation muß hervorgehen, welche Dokumente in welcher Güte (Vollständigkeit, Verständlichkeit) erforderlich sind.
- Bezüglich der Softwarequalität können Anforderungen gestellt werden, die von Herstellererklärungen über das eingesetzten Qualitätssicherungsverfahren, über ISO 9000 ff. Zertifikate bis hin zu unabhängigen Softwareprüfungen nach ISO 12119 reichen.
- Sollen durch das Produkt IT-Sicherheitsfunktionen erfüllt werden, sind sie in Form von Sicherheitsanforderungen zu formulieren (vgl. M 4.42 - Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung). Dies wird nachfolgend noch ausführlich erläutert.

Sicherheitsanforderungen
Abhängig davon, ob das Produkt Sicherheitseigenschaften bereitstellen muß, können im Anforderungskatalog Sicherheitsfunktionen aufgeführt werden. Typische Sicherheitsfunktionen, die hier in Frage kommen, seien kurz erläutert. Weitere Ausführungen findet man in den ITSEC.

- Identifizierung und Authentisierung
  In vielen Produkten wird es Anforderungen geben, diejenigen Benutzer zu bestimmen und zu überwachen, die Zugriff auf Betriebsmittel haben, die vom Produkt kontrolliert werden. Dazu muß nicht nur die behauptete Identität des Benutzers festgestellt, sondern auch die Tatsache nachgeprüft werden, daß der Benutzer tatsächlich die Person ist, die er zu sein vorgibt. Dies geschieht, indem der Benutzer dem Produkt Informationen liefert, die fest mit dem betreffenden Benutzer verknüpft sind.
- Zugriffskontrolle
  Bei vielen Produkten wird es erforderlich sein sicherzustellen, daß Benutzer und Prozesse, die für diese Benutzer tätig sind, daran gehindert werden, Zugriff auf Informationen oder Betriebsmittel zu erhalten, für die sie kein Zugriffsrecht haben oder für die keine Notwendigkeit zu einem Zugriff besteht. Desgleichen wird es Anforderungen bezüglich der unbefugten Erzeugung oder Änderung (einschließlich Löschung) von Informationen geben.
- Beweissicherung
  Bei vielen Produkten wird es erforderlich sein sicherzustellen, daß über Handlungen, die von Benutzern bzw. von Prozessen im Namen solcher Benutzer ausgeführt werden, Informationen aufgezeichnet werden, damit die Folgen solcher Handlungen später dem betreffenden Benutzer zugeordnet werden können und der Benutzer für seine Handlungen verantwortlich gemacht werden kann.

- Protokollauswertung
  Bei vielen Produkten wird sicherzustellen sein, daß sowohl über gewöhnliche Vorgänge als auch über außergewöhnliche Vorfälle ausreichend Informationen aufgezeichnet werden, damit durch Nachprüfungen später festgestellt werden kann, ob tatsächlich Sicherheitsverletzungen vorgelegen haben und welche Informationen oder sonstigen Betriebsmittel davon betroffen waren.

- Unverfälschbarkeit
  Bei vielen Produkten wird es erforderlich sein sicherzustellen, daß bestimmte Beziehungen zwischen unterschiedlichen Daten korrekt bleiben und daß Daten zwischen einzelnen Prozessen ohne Änderungen übertragen werden.
  Daneben müssen auch Funktionen bereitgestellt werden, die es bei der Übertragung von Daten zwischen einzelnen Prozessen, Benutzern und Objekten ermöglichen, Verluste, Ergänzungen oder Veränderungen zu entdecken bzw. zu verhindern, und die es unmöglich machen, die angebliche oder tatsächliche Herkunft bzw. Bestimmung der Datenübertragung zu ändern.

- Zuverlässigkeit
  Bei vielen Produkten wird es erforderlich sein sicherzustellen, daß zeitkritische Aufgaben genau zu dem Zeitpunkt durchgeführt werden, zu dem es erforderlich ist, also nicht früher oder später, und es wird sicherzustellen sein, daß zeitunkritische Aufgaben nicht in zeitkritische umgewandelt werden können. Desgleichen wird es bei vielen Produkten erforderlich sein sicherzustellen, daß ein Zugriff in dem erforderlichen Moment möglich ist und Betriebsmittel nicht unnötig angefordert oder zurückgehalten werden.

- Übertragungssicherung
  Dieser Begriff umfaßt alle Funktionen, die für den Schutz der Daten während der Übertragung über Kommunikationskanäle vorgesehen sind:

  - Authentisierung
  - Zugriffskontrolle
  - Datenvertraulichkeit
  - Datenintegrität
  - Sende- und Empfangsnachweis

  Einige dieser Funktionen werden mittels kryptographischer Verfahren realisiert. Über die ITSEC hinaus können weitere Sicherheitsanforderungen an Standardsoftware konkretisiert werden.

- Datensicherung
  An die Verfügbarkeit der mit dem Produkt verarbeiteten Daten werden hohe Anforderungen gestellt. Unter diesen Punkt fallen im Produkt integrierte Funktionen, die Datenverlusten vorbeugen sollen wie die automatische Speicherung von Zwischenergebnissen

oder die automatische Erstellung von Sicherungskopien vor der Durchführung größerer Änderungen.

- Verschlüsselung
  Verschlüsselung dient der Wahrung der Vertraulichkeit von Daten. Bei vielen Produkten wird es erforderlich sein, Nutzdaten vor einer Übertragung oder nach der Bearbeitung zu verschlüsseln und sie nach Empfang oder vor der Weiterverarbeitung zu entschlüsseln. Hierzu ist ein anerkanntes Verschlüsselungsverfahren zu verwenden. Es ist sicherzustellen, daß die zur Entschlüsselung benötigten Parameter (z.B. Schlüssel) in der Weise geschützt sind, daß kein Unbefugter Zugang zu diesen Daten besitzt.

- Funktionen zur Wahrung der Datenintegrität
  Für Daten, deren Integritätsverlust zu Schäden führen kann, können Funktionen eingesetzt werden, die Fehler erkennen lassen oder sogar mittels Redundanz korrigieren können. Meist werden Verfahren zur Integritätsprüfung eingesetzt, die absichtliche Manipulationen am Produkt bzw. den damit erstellten Daten sowie ein unbefugtes Wiedereinspielen von Daten zuverlässig aufdecken können. Sie basieren auf kryptographischen Verfahren (siehe M 5.36 - Verschlüsselung unter Unix und M 4.34 - Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen).

- Datenschutzrechtliche Anforderungen
  Wenn mit dem Produkt personenbezogene Daten verarbeitet werden sollen, sind über die genannten Sicherheitsfunktionen hinaus zusätzliche spezielle technische Anforderungen zu stellen, um den Datenschutzbestimmungen genügen zu können.

Stärke der Mechanismen
Sicherheitsfunktionen werden durch Mechanismen umgesetzt. Je nach Einsatzzweck müssen diese Mechanismen eine unterschiedliche Stärke besitzen, mit der sie Angriffe abwehren können. Die erforderliche Stärke der Mechanismen ist im Anforderungskatalog anzugeben. Nach ITSEC unterscheidet man drei verschiedene Mechanismenstärken:

- niedrig: bietet Schutz gegen zufällige unbeabsichtigte Angriffe, z.B. Bedienungsfehler.

- mittel: bietet Schutz gegen Angreifer mit beschränkten Gelegenheiten oder Betriebsmitteln.

- hoch: kann nur von Angreifern überwunden werden, die über sehr gute Fachkenntnisse, Gelegenheiten und Betriebsmitteln verfügen, wobei ein solcher erfolgreicher Angriff als normalerweise nicht durchführbar beurteilt wird.

Bewertungsskala
Um einen Vergleich verschiedener Produkte im Sinne einer Nutzwertanalyse durchführen zu können, müssen Kriterien vorhanden sein, wie die Erfüllung der einzelnen Anforderungen gewertet wird. Dazu ist es erforderlich, vorab die Bedeutung der einzelnen Anforderungen für die

angestrebte IT-gestützte Aufgabenerfüllung quantitativ oder qualitativ zu bewerten.

Diese Bewertung kann beispielsweise in drei Stufen vorgenommen werden. In der ersten Stufe wird festgelegt, welche im Anforderungskatalogs geforderten Eigenschaften notwendig und welche wünschenswert sind. Wenn eine notwendige Eigenschaft nicht erfüllt ist, wird das Produkt abgelehnt (sogenanntes K.O.-Kriterium). Das Fehlen einer wünschenswerten Eigenschaft wird zwar negativ gewertet, dennoch wird aber das Produkt aufgrund dessen nicht zwingend abgelehnt.

Als zweite Stufe wird die Bedeutung der geforderten wünschenswerte Eigenschaft für die Aufgabenerfüllung angegeben. Dies kann z.B. quantitativ mit Werten zwischen 1 für niedrig und 5 für hoch erfolgen. Notwendige Eigenschaften müssen nicht quantitativ bewertet werden. Ist dies aber aus rechnerischen Gründen erforderlich, müssen sie auf jeden Fall höher bewertet werden als jede wünschenswerte Eigenschaft (um die Bedeutung einer notwendigen Eigenschaft hervorzuheben, kann sie z.B. mit 10 bewertet werden).

In der dritten Stufe wird ein Vertrauensanspruch für die Korrektheit Aufgabenerfüllung der geforderten Eigenschaften angegeben (z.B. mit Werten zwischen 1 für niedrig und 5 für hoch). Anhand des Vertrauensanspruchs wird später entschieden, wie eingehend die Eigenschaft getestet wird. Der Vertrauensanspruch der Sicherheitsmechanismen muß entsprechend ihrer Mechanismenstärke bewertet werden, beispielsweise kombiniert man

- Mechanismenstärke niedrig mit Vertrauensanspruch 1
- Mechanismenstärke mittel mit Vertrauensanspruch 3
- Mechanismenstärke hoch mit Vertrauensanspruch 5

Diese Orientierungswerte müssen im Einzelfall verifiziert werden.

M 2.81 Vorauswahl eines geeigneten Standardsoftwareproduktes
Die Vorauswahl eines Standardsoftwareproduktes orientiert sich an dem durch die Fachabteilung und den IT-Bereich aufgestellten Anforderungskatalog. Zunächst sollte die für die Vorauswahl zuständige Stelle eine Marktanalyse durchführen, bei der anhand des Anforderungskatalogs eine tabellarische Marktübersicht erarbeitet werden sollte. In dieser Tabelle sollten für die in Frage kommenden Produkte Aussagen zu den im Anforderungskatalog festgehaltenen Punkten gemacht werden.

Die Marktübersicht sollte vom IT-Bereich erarbeitet werden, sie kann anhand von Produktbeschreibungen, Herstelleraussagen, Fachzeitschriften oder Händlerauskünften erstellt werden. Alternativ ist eine Ausschreibung möglich und teilweise vorgegeben. Der Anforderungskatalog ist Grundlage einer Ausschreibung, so daß anhand der eingehenden Angebote eine vergleichbare Marktübersicht erstellt werden kann.

Anschließend müssen die in der Marktübersicht erfaßten Produkte bzgl. der Vorgaben des Anforderungskatalogs bewertet werden. Hierzu kann die in M 2.80 - Erstellung eines Anforderungskataloges für Standardsoftware erarbeitete Bewertungsskala eingesetzt werden. Anhand der vorliegenden Informationen wird festgestellt, welche der geforderten Eigenschaften des Produktes voranden sind. Fehlen dem Produkt notwendige Eigenschaften, wird es verworfen. Über die Bewertung der Bedeutung der einzelnen Eigenschaften jedes Produktes kann eine Summe ermittelt werden. Anhand dieser Summen kann nun eine Hitliste für die Produkte aus der Vorauswahl erstellt werden.

Die erstellte Hitliste zusammen mit der Marktübersicht sollte dann der Beschaffungsstelle vorgelegt werden, damit dieser überprüfen kann, inwieweit die dort aufgeführten Produkte den internen Regelungen und gesetzlichen Vorgaben entsprechen. Dabei muß ddie Beschaffungsstelle auch darauf achten, daß die anderen Stellen, deren Vorgaben eingehalten werden müssen, wie der Datenschutzbeauftragte, der IT-Sicherheitsbeauftragte oder der Personal- bzw. Betriebsrat, rechtzeitig beteiligt werden.

Es muß entschieden werden, wieviele und welche Kandidaten der Hitliste getestet werden sollen. Sinnvollerweise sollten die ersten zwei oder drei Spitzenkandidaten ausgewählt werden und daraufhin getestet werden, ob sie die wichtigsten Kriterien des Anforderungskatalogs auch tatsächlich erfüllen. Dies ist insbesondere für die notwendigen Anforderungen wichtig. Hierfür sollten Testlizenzen beschafft werden und, wie in M 2.82 -Entwicklung eines Testplans für Standardsoftware und M 2.83 -Testen von Standardsoftware beschrieben, Tests durchgeführt werden.

Neben den Kriterien des Anforderungskatalogs können für die Entscheidung noch die folgenden Punkte berücksichtigt werden:

- Referenzen
  Kann der Hersteller oder Vertreiber für sein Produkt Referenzinstallationen angeben, so können die dort gemachten Erfahrungen hinterfragt und in die Produktbeurteilung einbezogen werden.
  Liegen externe Testergebnisse oder Qualitätsaussagen für das zu testende Softwareprodukt vor (z.B. Testergebnisse in Fachzeitschriften, Konformitätstests nach proprietären Standards, Prüfungen und Zertifikate nach einschlägigen Standards und Normen wie ISO 12119), so sollten auch diese Ergebnisse bei der Vorauswahl berücksichtigt werden.

- Verbreitungsgrad des Produktes
  Bei einem hohen Verbreitungsgrad hat der einzelne Anwender wenig oder keinen Einfluß auf den Hersteller des Produkts, wenn es um die Behebung von Fehlern oder die Implementation bestimmter Funktionalitäten geht. Er kann aber davon ausgehen, daß das Produkt weiterentwickelt wird. Oft gibt es externe Tests, die durch den Hersteller beauftragt oder von Fachzeitschriften durchgeführt wurden. Bei Produkten mit hohem Verbreitungsgrad ist im allgemeinen mehr über Schwachstellen bekannt, so daß der Anwender davon ausgehen kann, daß die wesentlichen Schwachstellen bereits bekannt sind, bzw. daß das Wissen über Schwachstellen schnell verbreitet wird und er nach dem Be-

kanntwerden Abhilfe schaffen kann.
Bei einem niedrigen Verbreitungsgrad kann ein Anwender mehr Einfluß auf den Hersteller nehmen. Externe Tests liegen im allgemeinen nicht vor, da sie für Produkte kleiner Hersteller zu aufwendig und zu teuer sind. Produkte mit niedrigem Verbreitungsgrad enthalten meist nicht mehr oder weniger Schwachstellen als solche mit hohem Verbreitungsgrad. Nachteil ist hier, daß diese evtl. nicht so schnell bekannt werden und damit behoben werden können. Wenn es sich aber um Sicherheitslücken handelt, sind diese aber wahrscheinlich auch potentiellen Angreifer nicht bekannt bzw. keine lohnenden Angriffsziele.

- Wirtschaftlichkeit / Kosten für Kauf, Betrieb, Wartung, Schulung
  Vor der Entscheidung für ein Produkt sollte immer die Frage stehen, ob die Kosten für das Produkt in einem angemessenen Verhältnis zu dem damit erzielbaren Nutzen stehen. In die unmittelbaren Anschaffungskosten sind darüber hinaus alle Folgekosten für Betrieb, Wartung und Schulung einzubeziehen. Dazu muß z.B. geklärt werden, ob die vorhandene Hardware-Plattform aufgerüstet werden muß oder ob für Installation und Betrieb Schulungen erforderlich sind.

Ist dann die Kaufentscheidung für ein Produkt gefallen, sollte der Kauf natürlich beim günstigsten Anbieter getätigt werden. Dieser hat sich evtl. schon bei der Marktsichtung herauskristallisiert.

M 2.82 Entwicklung eines Testplans für Standardsoftware
Die im nachfolgenden beschriebene Vorgehensweise beim Testen orientiert sich an den Standardwerken DIN ISO/IEC 12119 „Software-Erzeugnisse, Qualitätsanforderungen und Prüfbestimmungen“, Vorgehensmodell für die Planung und Durchführung von IT-Vorhaben (V-Modell) und dem Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM), die als weiterführende Literatur empfohlen werden.

Vor der Entscheidung für ein geeignetes Standardsoftwareprodukt müssen die nach der Vorauswahl (siehe M 2.81 - Vorauswahl eines geeigneten Standardsoftwareproduktes) in die engere Wahl gezogenen Produkte als Testlizenz beschafft und ausreichend getestet werden. War es aufgrund zeitlicher Beschränkungen, institutionsinterner Beschaffungsempfehlungen (Einhaltung von Hausstandards) oder anderen Gründen nicht möglich, daß Produkt vor der Beschaffung zu testen, müssen auf jeden Fall Tests vor der endgültigen Inbetriebnahme durchgeführt werden. Die Ergebnisse dieser Tests liefern dann die Grundlage für die Installationsvorschriften und anderer Freigabe-Bedingungen.

Obwohl bereits bei der Vorauswahl eine Überprüfung der notwendigen Anforderungen an das Produkt aufgrund der Herstelleraussagen stattgefunden hat, kann man nicht davon ausgehen, daß diese Anforderungen auch im gewünschten Maße erfüllt werden. Vielmehr muß nun durch systematisches Testen die Eignung und Zuverlässigkeit des Produktes auf Grundlage des Anforderungskataloges überprüft werden, um das geeignetste Produkt auszuwählen.

Dabei bietet es sich an, das Testen in vier Bereiche einzuteilen:

- Eingangsprüfungen (Prüfung auf Computer-Viren, Lauffähigkeit in der gewünschten IT-Einsatzumgebung, ...),
- funktionale Tests (Überprüfung der funktionalen Anforderungen),
- Tests weiterer funktionaler Eigenschaften (Überprüfung von Kompatibilität, Performance, Interoperabilität, Konformität mit Regelungen oder Gesetzen, Benutzerfreundlichkeit, Wartbarkeit, Dokumentation), und
- sicherheitsspezifische Tests (Überprüfung der Sicherheitsanforderungen).

Anhand der bei der Vorauswahl erstellten Hitliste sind diejenigen Produkte auszuwählen, die getestet werden sollen. Anschließend wird ein Testplan entwickelt.
Dieser umfaßt folgende Inhalte:

- Festlegung der Testinhalte anhand des Anforderungskataloges,
- Überprüfung von Referenzen,
- Festlegung des Gesamtprüfaufwandes,
- Zeitplanung einschließlich Prüfaufwand je Testinhalt,
- Festlegung der Testverantwortlichen,
- Testumgebung,
- Inhalt der Testdokumentation,
- Festlegung von Entscheidungskriterien.

Die einzelnen genannten Punkte werden nachfolgend erläutert.

Festlegung der Testinhalte anhand des Anforderungskataloges
Aus dem Anforderungskatalog werden diejenigen Anforderungen ausgewählt, die überprüft werden sollen. Dies sollten insbesondere diejenigen Eigenschaften sein, die eine große Bedeutung oder einen hohen Vertrauensanspruch besitzen.

Überprüfung von Referenzen
Bei der Vorauswahl (siehe M 2.81 - Vorauswahl eines geeigneten Standardsoftwareproduktes) wurden bereits erste Referenzen über die zu testenden Produkte eingeholt. Diese können ersatzweise herangezogen werden, wenn man der jeweiligen externen Testgruppe ausreichendes Vertrauen entgegenbringt.
Wurde für das Produkt ein Zertifikat nach den Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC) vergeben, ist anhand des Zertifizierungsreportes zu prüfen, inwieweit die dort dokumentierten Testergebnisse berücksichtigt werden können.

Gegebenenfalls können dann eigene Test unterbleiben oder in geringerem Umfang stattfinden. Die freiwerdenden Kapazitäten können auf andere Testinhalte verteilt werden.

Festlegung des Gesamtprüfaufwandes
Um den Aufwand für die Tests nicht ausufern zu lassen, sollte vorab der Gesamtprüfaufwand festgelegt werden, z.B. in Personentagen oder durch Fristsetzung.

Zeitplanung einschließlich Prüfaufwand je Testinhalt
Beim Testen mehrerer Produkte empfiehlt es sich, diese vergleichend zu testen. Das heißt, alle Produkte werden von einer Testgruppe bzgl. einer Anforderung des Anforderungskataloges getestet. Der Prüfaufwand ist damit für jede Anforderung des Anforderungskataloges festzulegen und wird damit automatisch gleichmäßig auf alle zu testenden Produkte verteilt. Der Prüfaufwand ergibt sich dabei aus Prüftiefe und Komplexität der Eigenschaft. Die Prüftiefe der jeweiligen Eigenschaften sollte sich zum einen an ihrem Vertrauensanspruch, das heißt an dem Vertrauen orientieren, das der Korrektheit dieser Eigenschaft entgegengebracht werden muß. Zum anderen muß aber auch die Fehleranfälligkeit und Nutzungshäufigkeit der jeweiligen Eigenschaft berücksichtigt werden. Ausführlichere Informationen sind der ISO 12119 zu entnehmen.

Hinweise:

- Für sicherheitsspezifische Anforderungen kann die Prüftiefe entsprechend der geforderten Mechanismenstärke zusätzlich relativiert werden.
- Der Prüfaufwand für die Eingangsprüfungen sollte gemessen an den anderen Tests gering sein.

Abschließend ist der Gesamtprüfaufwand entsprechend dem relativen Prüfaufwand der jeweiligen Eigenschaft auf die einzelnen Testabschnitte zu verteilen.

Festlegung der Testverantwortlichen
Für jeden Testinhalt ist nun festzulegen, welche Aufgaben durchzuführen sind und wer dafür verantwortlich ist. Insbesondere ist zu beachten, daß bei einigen Testinhalten der Personal- bzw. Betriebsrat, der Datenschutzbeauftragte und der IT-Sicherheitsbeauftragte zu beteiligen ist.

Testumgebung
Testen ist immer destruktiv, da vorsätzlich nach Fehlern gesucht wird. Aus diesem Grund muß das Testen immer in einer isolierten Testumgebung erfolgen.

Die Testumgebung sollte nach Möglichkeit ein genaues funktionales Abbild der Produktionsumgebung sein. In der Regel ist es jedoch nicht wirtschaftlich, die Produktionsumgebung in vollem Umfang nachzubilden.

Damit für die ausgewählten Produkte gleiche Randbedingungen gegeben sind, sollte eine Referenztestumgebung definiert werden. Für einzelne Tests kann diese weiter angepaßt oder eingeschränkt werden.

Die für die einzelnen Prüfungen benötigten Ressourcen (Betriebsmittel, IT-Infrastruktur) sind zu spezifizieren. Es sollte im Detail beschrieben werden, wann und in welchem Umfang sie verfügbar sein müssen.

Wichtig ist, daß alle Betriebssysteme in allen im Produktionsbetrieb eingesetzten Versionen (Releases) in der Testumgebung zur Verfügung stehen. Die Intention ist dabei die Ermittlung von systembedingten Schwachstellen von Komponenten der Produktionsumgebung im Zusammenspiel mit dem zu installierenden Standardsoftwareprodukt. In Ausnahmefällen, wenn sich Aspekte verallgemeinern lassen, kann auf einzelne Komponenten verzichtet werden.

Folgende weitere Aspekte sind unbedingt zu beachten und helfen, eine sichere und geeignete Testumgebung aufzubauen:

- Die Computer-Virenfreiheit der Testumgebung ist durch ein aktuelles Virensuchprogramm sicherzustellen.
- Die Testumgebung muß frei sein von Seiteneffekten auf den Echtbetrieb. Um Wechselwirkungen von vornherein zu vermeiden, empfiehlt es sich, dedizierte IT-Systeme zu installieren.
- Die Zugriffsrechte müssen in der Testumgebung derart konfiguriert werden, wie sie dem Produktionsbetrieb entsprechen.
- Der Zutritt und Zugang zur Testumgebung muß geregelt sein.
- Es muß sichergestellt werden, daß das Produkt genau in der Testumgebung ermittelten Konfiguration in den Produktionsbetrieb übernommen wird. Daher ist in der Testumgebung ein geeignetes Verfahren zum Integritätsschutz einzusetzen (digitale Signaturen, Checksummen).
- Die Kosten für den Aufbau der Testumgebung müssen angemessen sein.

Nach Beendigung aller geplanten Tests ist zu entscheiden, ob die Testumgebung abgebaut werden soll. Ggf. sind weitere Tests auch nach der Beschaffung eines Produktes notwendig, so daß es eventuell wirtschaftlich ist, die Testumgebung vorzuhalten. Vor dem Abbau der Testumgebung sind die Testdaten zu löschen, falls sie nicht mehr benötigt werden (z.B. für eine spätere Installation). Druckerzeugnisse sind ordnungsgemäß zu entsorgen, Programme sind zu deinstallieren. Die Testlizenzen der nicht ausgewählten Produkte sind zurückzugeben.

Inhalt der Testdokumentation
Im Testplan ist vorzugeben, wie ausführlich die Testdokumentation zu erstellen ist. Hierbei

sind die Aspekte der Nachvollziehbarkeit, Reproduzierbarkeit und Vollständigkeit zu berücksichtigen.

Die Testdokumentation muß Testpläne, -ziele, -verfahren und -ergebnisse enthalten und die Übereinstimmung zwischen den Tests und den spezifizierten Anforderungen beschreiben. Sämtliche Testaktivitäten sowie die getroffene Testbewertung (inklusive Entscheidungsargumentation) sind schriftlich festzuhalten. Dazu gehören im einzelnen

- Produktbezeichnung und Beschreibung,
- Testbeginn, -ende und -aufwand,
- Testverantwortliche,
- Konfiguration der Testumgebung,
- Beschreibung der Testfälle,
- Entscheidungskriterien, Testergebnisse und Argumentationsketten, und
- nicht erfüllte Anforderungen des Anforderungskataloges.

Der Testgruppe sollte eine Möglichkeit zur übersichtlichen Dokumentation und Protokollierung der Testaktivitäten und -ergebnisse zur Verfügung gestellt werden (z.B. Protokollierungstool, Formblätter o.ä.).

Wird beim Testen ein automatisiertes Werkzeug verwendet, muß die Testdokumentation ausreichende Informationen über dieses Werkzeug und die Art seines Einsatzes enthalten, damit die Entscheidung nachvollzogen werden kann.

Festlegung von Entscheidungskriterien
Bei der Bewertung der jeweiligen Testinhalte kann beispielsweise folgende dreistufige Skala verwendet werden:

Note	Entscheidungskriterien
0	- Anforderungen sind nicht erfüllt. oder - Es wurden nicht tolerierbare Fehler festgestellt, die sich nicht beheben lassen.
1	- Anforderungen sind erfüllt, aber es bestehen Vorbehalte (z.B. Funktion ist nur eingeschränkt geeignet). oder - Es sind geringfügige Fehler festgestellt wurden. Diese spielen nur eine untergeordnete Rolle, da sie tolerierbare Auswirkungen auf den Produktionsbetrieb haben oder da sie nur mit vernachlässigbarer Wahrscheinlichkeit vorkommen können.
2	- Anforderungen sind in vollem Umfang erfüllt. und - Fehler, die ggf. aufgetaucht sind, sind entweder zu beheben oder haben für den Betrieb keinerlei Bedeutung.

Sind Fehler aufgetaucht, die nicht reproduziert werden können, hat der Prüfer zu entscheiden, welcher Kategorie (Note) der Fehler zuzuordnen ist.

Sind Fehler aufgetreten, die während des Tests behoben werden können, ist nach deren Behebung erneut im erforderlichen Umfang zu testen.

Nach Erstellung des Testplans wird für jeden im Testplan spezifizierten Testinhalt ein Tester oder eine Testgruppe mit der Durchführung des ihr zugeteilten Tests beauftragt. Der Testplan ist der Testgruppe zu übergeben und die für die Einzeltests vorgegebenen Zeiten sind mitzuteilen.

M 2.83 Testen von Standardsoftware
Das Testen von Standardsoftware läßt sich in die Abschnitte Vorbereitung, Durchführung und Auswertung unterteilen. In diesen Abschnitten sind folgende Aufgaben wahrzunehmen:

- Testvorbereitung
  - Festlegung der Testmethoden für die Einzeltests (Testarten, -verfahren und -werkzeuge)
  - Generierung von Testdaten und Testfällen
  - Aufbau der benötigten Testumgebung
- Testdurchführung
  - Eingangsprüfungen
  - Funktionale Tests
  - Tests weiterer funktionaler Eigenschaften

  - Sicherheitsspezifische Tests
  - Pilotanwendung
- Testauswertung

Die einzelnen Aufgaben werden nachfolgend beschrieben.

Testvorbereitung
Festlegung der Testmethoden für die Einzeltests (Testarten, -verfahren und -werkzeuge) Methoden zur Durchführung von Tests sind z.B. statistische Analyse, Simulation, Korrektheitsbeweis, symbolische Programmausführung, Review, Inspektion, Versagensanalyse. Hierbei muß beachtet werden, daß einige dieser Testmethoden nur bei Vorliegen des Quellcodes durchführbar sind. In der Vorbereitungsphase muß die geeignete Testmethode ausgewählt und festgelegt werden. Es muß geklärt werden, welche Verfahren und Werkzeuge zum Testen von Programmen und zum Prüfen von Dokumenten eingesetzt werden. Typische Verfahren zum Testen von Programmen sind z.B. Black-Box-Tests, White-Box-Tests oder Penetrationstests. Dokumente können z.B. durch informelle Prüfungen, Reviews oder anhand von Checklisten kontrolliert werden.
Ein Black-Box-Test ist ein Funktionalitätstest ohne Kenntnis der internen Programmabläufe, bei dem z.B. das Pro gramm mit allen Datenarten für alle Testfälle mit Fehlerbehandlung und Plausibilitätskontrollen durchlaufen wird.
Bei einem White-Box-Test handelt es sich um einen Funktionalitätstests unter Offenlegung der internen Programmabläufe, z.B. durch Quellcode-Überprüfung oder Tracing. White-Box-Tests gehen in der Regel über den IT-Grundschutz hinaus und könne n für Standardsoftware in der Regel nicht durchgeführt werden, da der Quellcode vom Hersteller nicht offengelegt wird.
Bei Funktionalitätstests soll der Nachweis erbracht werden soll, daß der Testinhalt der Spezifikation entspricht. Durch Penetrationstests soll festgestellt werden, ob bekannte oder vermutete Schwachstellen im praktischen Betrieb ausgenutzt werden können, beispielsweise durch Manipulationsversuche an den Sicherheitsmechanismen oder durch Umgehung von Sicherheitsmechanismen durch Manipulationen auf Betriebssystemebene.
Weiterhin ist die Art und Weise der Ergebnissicherung und -auswertung festzuschreiben, insbesondere im Hinblick auf die Wiederholbarkeit von Prüfungen. Es muß geklärt werden, welche Daten während und nach der Prüfung festzuhalten sind.

Generierung von Testdaten und Testfällen
Die Vorbereitung von Tests umfaßt auch die Generierung von Testdaten. Methode und Vorgehensweise sind zuvor festzulegen und zu beschrieben.
Für jeden einzelnen Testinhalt muß eine dem Testaufwand angemessene Anzahl von Testfällen generiert werden. Jede der folgenden Kategorien ist dabei zu berücksichtigen:

Standardfälle sind Fälle, mit denen die korrekte Verarbeitung der definierten Funktionalitäten überprüft werden soll. Die eingehenden Daten nennt man Normalwerte oder Grenzwerte. Normalwerte sind Daten innerhalb, Grenzwerte sind Eckdaten des jeweils gültigen Eingabebereichs.

Fehlerfälle sind Fälle, in denen versucht wird, mögliche Fehlermeldungen des Programms zu provozieren. Diejenigen Eingabewerte, auf die das Programm mit vorgegebenen Fehlermeldungen reagieren soll, nennt man Falschwerte.

Ausnahmefälle sind Fälle, bei denen das Programm ausnahmsweise anders reagieren muß als bei Standardfällen. Es muß daher überprüft werden, ob das Programm diese Fälle als solche erkennt und korrekt bearbeitet.
Ist die Generierung von Testdaten zu aufwendig oder schwierig, können auch anonymisierte Echtdaten für den Test eingesetzt werden. Aus Gründen des Vertraulichkeitsschutz müssen Echtdaten unbedingt zuverlässig anonymisiert werden. Zu beachten bleibt, daß die anonymisierten Echtdaten u. U. nicht alle Grenzwerte und Ausnahmefälle abdecken, so daß diese gesondert erzeugt werden müssen.
Über die Testdaten hinaus sollten auch alle Arten möglicher Benutzerfehler betrachtet werden. Problematisch sind insbesondere alle Benutzerreaktionen, die im Programmablauf nicht vorgesehen und dementsprechend nicht korrekt abgewiesen werden.

Aufbau der benötigten Testumgebung
Die im Testplan beschriebene Testumgebung muß aufgebaut und die zu testenden Produkte dort installiert werden. Die eingesetzten Komponenten sind zu identifizieren und deren Konfiguration ist zu beschreiben. Treten bei der Installation des Produktes Abweichungen von der beschriebenen Konfiguration auf, so ist dies zu dokumentieren.

Testdurchführung
Die Durchführung der Tests muß anhand des Testplans erfolgen. Jede Aktion sowie die Testergebnisse müssen ausreichend dokumentiert und bewertet werden. Insbesondere wenn Fehler auftreten, sind diese derart zu dokumentieren, daß sie reproduziert werden können. Die für den späteren Produktionsbetrieb geeigneten Betriebsparameter müssen ermittelt und für die spätere Erstellung einer Installationsanweisung festgehalten werden.
Werden zusätzliche Funktionen beim Produkt erkannt, die nicht im Anforderungskatalog aufgeführt, aber trotzdem von Nutzen sein können, so ist hierfür mindestens ein Kurztest durchzuführen. Zeigt sich, daß diese Funktion von besonderer Bedeutung für den späteren Betrieb sind, sind diese ausführlich zu testen. Für den zusätzlich anfallenden Prüfaufwand ist ggf. eine Fristverlängerungen bei den Verantwortlichen zu beantragen. Die Testergebnisse sind in die Gesamtbewertung mit einzubeziehen.
Zeigt sich bei Bearbeitung einzelner Testinhalte, daß eine oder mehrere Anforderungen des Anforderungskataloges nicht konkret genug waren, sind diese gegebenenfalls zu konkretisieren.
Beispiel: Im Anforderungskatalog wird zum Vertraulichkeitsschutz der zu bearbeitenden Daten Verschlüsselung gefordert. Während des Testens hat sich gezeigt, daß eine Offline-Verschlüsselung für den Einsatzzweck ungeeignet. Daher ist der Anforderungskatalog hinsichtlich einer Online-Verschlüsselung zu ergänzen. (Eine Offline-Verschlüsselung muß vom Anwender angestoßen und die zu verschlüsselnden Elemente jeweils spezifiziert werden; eine Online-Verschlüsselung erfolgt transparent für den Anwender mit voreingestellten Parametern.)

Eingangsprüfungen
Vor allen anderen Tests sind zunächst die folgenden grundlegenden Aspekte zu testen, da ein Mißerfolg bei diesen Eingangsprüfungen zu direkten Aktionen oder dem Testabbruch führt:

- Die Computer-Virenfreiheit des Produktes ist durch ein aktuelles Virensuchprogramm zu überprüfen.
- In einem Installationstest muß festgestellt werden, ob das Produkt für den späteren Einsatzzweck einfach, vollständig und nachvollziehbar zu installieren ist. Ebenfalls muß überprüft werden, wie das Produkt vollständig deinstalliert wird.
- Die Lauffähigkeit des Produktes ist in der geplanten Einsatzumgebung zu überprüfen; dies beinhaltet insbesondere eine Überprüfung der Bildschirmaufbereitung, der Druckerausgabe, der Mausunterstützung, der Netzfähigkeit, etc.
- Die Vollständigkeit des Produktes (Programme und Handbücher) ist zu überprüfen, z.B. durch einen Vergleich mit dem Bestandsverzeichnis, der Produktbeschreibung oder ähnlichem.
- Es sollten Kurztests von Funktionen des Programms durchgeführt werden, die nicht explizit in den Anforderungen erwähnt wurden, im Hinblick auf Funktion, Plausibilität, Fehlerfreiheit, etc.

Funktionale Tests
Die funktionalen Anforderungen, die im Anforderungskatalog an das Produkt gestellt wurden, sind auf folgende Aspekte zu untersuchen:

- Existenz der Funktion durch Aufruf im Programm und Auswertung der Programmdokumentationen.
- Fehlerfreiheit bzw. Korrektheit der Funktion
  Um die Fehlerfreiheit bzw. Korrektheit der Funktion sicherzustellen, sind je nach Prüftiefe bei der Untersuchung unterschiedliche Testverfahren wie Black-Box-Tests, White-Box-Tests oder simulierter Produktionsbetrieb anzuwenden.
  Die in der Vorbereitungsphase erstellten Testdaten und Testfälle werden im Funktionalitätstest eingesetzt. Bei den Funktionalitätstests ist es notwendig, die Testergebnisse mit den vorgegebenen Anforderungen zu vergleichen. Außerdem ist zu überprüfen, wie das Programm bei fehlerhaften Eingabeparametern oder fehlerhafter Bedienung reagiert. Die Funktion ist auch mit den Grenzwerten der Intervalle von Eingabeparametern sowie mit Ausnahmefällen zu testen. Diese müssen entsprechend erkannt und korrekt behandelt werden.
- Eignung der Funktion
  Die Eignung einer Funktion zeichnet sich dadurch aus, daß die Funktion
  - tatsächlich die Aufgabe im geforderten Umfang und effizient erfüllt und

  - sich leicht in die üblichen Arbeitsabläufe integrieren läßt.

  Ist die Eignung der Funktion nicht offensichtlich, bietet es sich an, dies in einem simulierten Produktionsbetrieb, aber immer noch in der Testumgebung zu testen.

- Widerspruchsfreiheit
  Die Widerspruchsfreiheit der einzelnen Funktionen ist zu überprüfen und zwar jeweils zwischen Anforderungskatalog, Dokumentation und Programm. Eventuelle Widersprüche sind zu dokumentieren. Abweichungen zwischen Dokumentation und Programm sind so zu festzuhalten, daß sie bei einem späteren Einsatz des Produktes in den Ergänzungen zur Dokumentation aufgenommen werden können.

Tests weiterer funktionaler Eigenschaften
Die im Anforderungskatalog neben den funktionalen und den sicherheitsspezifischen Anforderungen spezifizierten weiteren funktionalen Eigenschaften sind ebenfalls zu überprüfen:

- Performance
  Das Laufzeitverhalten sollte für alle geplanten Konfigurationen des Produktes ermittelt werden. Um die Performance ausreichend zu testen, sind in der Regel Tests, in denen der Produktionsbetrieb simuliert wird oder auch Pilotanwendung bei ausgewählten Anwendern sinnvoll. Es muß festgestellt werden, ob die gestellten Performanceanforderungen erfüllt sind.

- Zuverlässigkeit
  Das Verhalten bei zufälligen oder mutwillig herbeigeführten Systemabstürzen („Crashtest“) ist zu analysieren und es ist festzustellen, welche Schäden dabei entstehen. Es ist festzuhalten, ob nach Systemabstürzen ein ordnungsgemäßer und korrekter Wiederanlauf des Produktes möglich ist. Es ist ebenfalls zu überprüfen, ob ein direkter Zugriff auf Datenbestände unabhängig von der regulären Programmfunktion erfolgen kann. In vielen Fällen kann ein solcher Zugriff zu Datenverlusten führen und sollte dann vom Produkt verhindert werden. Ebenfalls sollte festgehalten werden, ob das Programm Möglichkeiten unterstützt, „kritische Aktionen“ (z.B. Löschen, Formatieren) rückgängig zu machen.

- Benutzerfreundlichkeit
  Ob das Produkt benutzerfreundlich ist, ist in besonderem Maße vom subjektiven Empfinden der Testperson abhängig. Jedoch können bei der Beurteilung folgende Aspekte Anhaltspunkte liefern:

  - Technik der Menüoberflächen (Pull-Down-Menüs, Scrolling, Drag & Drop, etc.),
  - Design der Menüoberflächen (z.B. Einheitlichkeit, Verständlichkeit, Menüführung),
  - Tastaturbelegung,
  - Fehlermeldungen,
  - problemloses Ansprechen von Schnittstellen (Batchbetrieb, Kommunikation, etc.),

  - Lesbarkeit der Benutzerdokumentation,
  - Hilfefunktionen.

  Die Analyse der Benutzerfreundlichkeit muß mögliche Betriebsarten des Produktes beschreiben, einschließlich des Betriebes nach Bedien- oder Betriebsfehlern, und ihre Konsequenzen und Folgerungen für die Aufrechterhaltung eines sicheren Betriebes.

- Wartbarkeit
  Der personelle und finanzielle Aufwand für die Wartung und Pflege des Produktes sollte während des Testens ermittelt werden. Dieser kann z. B. anhand von Referenzen wie anderen Referenzinstallationen oder Tests in Fachzeitschriften oder anhand des während des Testens ermittelten Installationsaufwandes geschätzt werden. Hierfür muß dokumentiert werden, wieviele manuelle Eingriffe während der Installation notwendig waren, um die angestrebte Konfiguration zu erreichen. Sind bereits Erfahrungen mit Vorgängerversionen des getesteten Produktes gesammelt worden, sollte hinterfragt werden, wie aufwendig deren Wartung war.
  Es sollte nachgefragt werden, inwieweit Support durch den Hersteller oder Vertreiber angeboten wird und zu welchen Konditionen. Wird vom Hersteller oder Vertreiber eine Hotline angeboten, sollte auch deren Erreichbarkeit und Güte betrachtet werden.

- Dokumentation
  Die vorliegende Dokumentation muß daraufhin überprüft werden, ob sie vollständig, korrekt und widerspruchsfrei ist. Darüber hinaus sollte sie verständlich, eindeutig, fehlerfrei und übersichtlich sein.
  Es muß weiterhin kontrolliert werden, ob sie für eine sichere Verwendung und Konfiguration ausreicht. Alle sicherheitsspezifischen Funktionen müssen beschrieben sein.

Darüber hinaus sind als weitere Punkte des Anforderungskatalogs zu testen:

- Kompatibilitätsanforderungen
- Interoperabilität
- Konformität zu Standards
- Einhaltung von internen Regelungen und gesetzlichen Vorschriften
- Softwarequalität

Sicherheitsspezifische Tests
Wurden sicherheitsspezifische Anforderungen an das Produkt gestellt, so sind zusätzlich zu den vorgenannten Untersuchungen auch folgende Aspekte zu untersuchen:

- Wirksamkeit und Korrektheit der Sicherheitsfunktionen,
- Stärke der Sicherheitsmechanismen und

- Unumgänglichkeit und Zwangsläufigkeit der Sicherheitsmechanismen.

Als Grundlage für eine Sicherheitsuntersuchung könnte beispielsweise das Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM) herangezogen werden, in dem viele der nachfolgend aufgezeigten Vorgehensweise beschrieben sind. Die weiteren Ausführungen dienen zur Orientierung und zur Einführung in die Thematik.
Zu Beginn muß durch funktionale Tests zunächst nachgewiesen werden, daß das Produkt die erforderlichen Sicherheitsfunktionen bereitstellt.
Anschließend ist zu überprüfen, ob alle erforderlichen Sicherheitsmechanismen im Anforderungskatalog genannt wurden, ggf. ist dieser zu ergänzen. Um die Mindeststärke der Mechanismen zu bestätigen oder zu verwerfen sind Penetrationstests durchzuführen. Penetrationstests sind nach allen anderen Tests durchzuführen, da sich aus diesen Tests Hinweise auf potentielle Schwachstellen ergeben können.
Durch Penetrationstests kann das Testobjekt oder die Testumgebung beschädigt oder beeinträchtigt werden. Damit solche Schäden keine Auswirkungen haben, sollten vor der Durchführung von Penetrationstests Datensicherungen gemacht werden.
Penetrationstests können durch Verwendung von Sicherheitskonfigurations- und Protokollierungstools unterstützt werden. Diese Tools untersuchen eine Systemkonfiguration und suchen nach gemeinsamen Schwachstellen wie etwa allgemein lesbaren Dateien und fehlenden Paßwörtern.
Mit Penetrationstests soll das Produkt auf Konstruktionsschwachstellen untersucht werden, indem dieselben Methoden angewandt werden, die auch ein potentieller Angreifer zur Ausnutzung von Schwachstellen benutzen würde, wie z.B.

- Ändern der vordefinierten Befehlsabfolge,
- Ausführen einer zusätzlichen Funktion,
- Direktes oder indirektes Lesen, Schreiben oder Modifizieren interner Daten,
- Ausführen von Daten, deren Ausführung nicht vorgesehen ist,
- Verwenden einer Funktion in einem unerwarteten Kontext oder für einen unerwarteten Zweck,
- Aktivieren der Fehlerüberbrückung,
- Nutzen der Verzögerung zwischen dem Zeitpunkt der Überprüfung und dem Zeitpunkt der Verwendung,
- Unterbrechen der Abfolge durch Interrupts, oder
- Erzeugen einer unerwarteten Eingabe für eine Funktion.

Die Mechanismenstärken werden anhand der Begriffe Fachkenntnisse, Gelegenheiten und Betriebsmittel definiert, in der ITSEM werden diese näher erläutert. Beispielsweise können zur Bestimmung der Mechanismenstärke folgende Regeln angewandt werden:

- Kann der Mechanismus innerhalb von Minuten von einem Laien allein überwunden werden, dann kann er nicht einmal als niedrig eingestuft werden.
- Kann ein erfolgreicher Angriff von jedem bis auf einen Laien innerhalb von Minuten durchgeführt werden, dann ist der Mechanismus als niedrig einzustufen.
- Wenn für einen erfolgreichen Angriff ein Experte benötigt wird, der mit der vorhandenen Ausstattung Tage braucht, dann ist der Mechanismus als mittel einzustufen.
- Kann der Mechanismus nur von einem Experten mit Sonderausstattung überwunden werden, der dafür Monate braucht und eine geheime Absprache mit einem Systemverwalter treffen muß, dann ist er als hoch einzustufen.

Es muß sichergestellt werden, daß die durchgeführten Tests alle sicherheitsspezifischen Funktionen umfassen. Wichtig ist zu beachten, daß durch Testen immer nur Fehler oder Abweichungen von den Spezifikationen festgestellt werden können, niemals jedoch die Abwesenheit von Fehlern.

An einigen Beispielen sollen typische Untersuchungsaspekte aufgezeigt werden:

Paßwortschutz:

- Gibt es vom Hersteller voreingestellte Paßwörter? Typische Beispiele für solche Paßwörter sind der Produktname, der Herstellername, „SUPERVISOR“, „ADMINISTRATOR“, „USER“, „GUEST“.
- Welche Datei ändert sich, wenn ein Paßwort geändert wurde? Kann diese Datei durch eine alte Version aus einer Datensicherung ersetzt werden, um alte Paßwörter zu aktivieren? Werden die Paßwörter verschlüsselt gespeichert oder sind sie im Klartext auslesbar? Ist es möglich, in dieser Datei Änderungen vorzunehmen, um neue Paßwörter zu aktivieren?
- Wird der Zugang tatsächlich nach mehreren fehlerhaften Paßworteingaben gesperrt?
- Werden in Zeitschriften oder Mailboxen Programme angeboten, die die Paßwörter des untersuchten Produkts ermitteln können? Für einige Standardapplikationen sind solche Programme erhältlich.
- Wenn Dateien mit Paßwörtern geschützt werden, kann durch einen Vergleich einer Datei vor und nach der Paßwortänderung die Stelle ermittelt werden, an der das Paßwort gespeichert wird. Ist es möglich, an dieser Stelle Änderungen oder alte Werte einzugeben, um bekannte Paßwörter zu aktivieren? Werden die Paßwörter verschlüsselt gespeichert? Wie ist die Stelle belegt, wenn der Paßwortschutz deaktiviert ist?
- Kann die Paßwort-Prüfroutine unterbrochen werden? Gibt es Tastenkombinationen, mit denen die Paßworteingabe umgangen werden kann?

Zugriffsrechte:

- In welchen Dateien werden Zugriffsrechte gespeichert und wie werden sie geschützt?
- Können Zugriffsrechte von Unberechtigten geändert werden?
- Können Dateien mit alten Zugriffsrechten zurückgespielt werden und welche Rechte benötigt man dazu?
- Können die Rechte des Administrators so eingeschränkt werden, daß er keinen Zugriff auf die Nutz- oder Protokolldaten erhält?

Datensicherung:

- Können erstellte Datensicherungen problemlos rekonstruiert werden?
- Können Datensicherungen durch ein Paßwort geschützt werden? Wenn ja, können die oben dargestellten Untersuchungsansätze für Paßwörter eingesetzt werden.

Verschlüsselung:

- Bietet das Produkt an, Dateien oder Datensicherungen zu verschlüsseln?
- Werden mehrere verschiedene Verschlüsselungsalgorithmen angeboten? Hierbei ist im allgemeinen folgende Faustregel zu beachten: „Je schneller ein in Software realisierter Verschlüsselungsalgorithmus ist, um so unsicherer ist er."
- Wo werden die zur Ver- oder Entschlüsselung genutzten Schlüssel gespeichert? Bei einer lokalen Speicherung ist zu untersuchen, ob diese Schlüssel paßwortgeschützt oder mit einem weiteren Schlüssel überschlüsselt geschützt werden. Bei einem Paßwortschutz sind die obigen Punkte zu berücksichtigen. Bei einer Überschlüsselung ist zu betrachten, wie der zugehörige Schlüssel geschützt wird.
  Dazu können folgende Punkte betrachtet werden: Welche Datei ändert sich, wenn ein Schlüssel geändert wurde? Durch den Vergleich dieser Datei vor und nach der Schlüsseländerung kann die Stelle ermittelt werden, an der dieser Schlüssel gespeichert wird. Ist es möglich, an dieser Stelle Änderungen vorzunehmen, um neue Schlüssel zu aktivieren, die dann vom Anwender genutzt werden, ohne daß dieser die Kompromittierung bemerkt?
- Gibt es vom Hersteller voreingestellte Schlüssel, die vor der erstmaligen Benutzung des Programms geändert werden müssen?
- Was passiert, wenn bei der Entschlüsselung ein falscher Schlüssel eingegeben wird?
- Wird nach der Verschlüsselung einer Datei die unverschlüsselte Variante gelöscht? Wenn ja, wird sie zuverlässig überschrieben? Wird vor der Löschung überprüft, ob die Verschlüsselung erfolgreich war?

Protokollierung:

- Wird der Zugriff auf Protokolldaten für Unbefugte verwehrt?

- Werden die zu protokollierenden Aktivitäten lückenlos aufgezeichnet?
- Hat der Administrator die Möglichkeit aufgrund seiner privilegierten Rechte, sich unberechtigt und unbemerkt Zugriff auf Protokolldaten zu verschaffen oder kann er die Protokollierung unbemerkt deaktivieren?
- Wie reagiert das Programm, wenn der Protokollierungsspeicher überläuft?

Darüber hinaus muß festgestellt werden, ob durch das neue Produkt Sicherheitseigenschaften an anderer Stelle unterlaufen werden.

Pilotanwendung
Nach Abschluß aller anderen Tests kann noch eine Pilotanwendung, also ein Einsatz unter Echtbedingungen, für notwendig gehalten werden.
Erfolgt der Test in der Produktionsumgebung mit Echtdaten, muß vorab durch eine ausreichende Anzahl von Tests die korrekte und fehlerfreie Funktionsweise des Programms bestätigt worden sein, um die Verfügbarkeit und Integrität der Produktionsumgebung nicht zu gefährden. Dabei kann das Produkt beispielsweise bei ausgewählten Benutzern installiert werden, die es dann für einen gewissen Zeitraum im echten Produktionsbetrieb einsetzen.

Testauswertung
Anhand der festgelegten Entscheidungskriterien sind die Testergebnisse zu bewerten, alle Ergebnisse zusammenzuführen und mit der Testdokumentation der Beschaffungsstelle bzw. Testverantwortlichen vorzulegen.
Anhand der Testergebnisse sollte ein abschließendes Urteil für ein zu beschaffendes Produkt gefällt werden. Hat kein Produkt den Test bestanden, muß überlegt werden, ob eine neue Marktsichtung vorgenommen werden soll, ob die gestellten Anforderungen zu hoch waren und geändert werden müssen oder ob von einer Beschaffung zu diesem Zeitpunkt abgesehen werden muß.

M 2.84 Entscheidung und Entwicklung der Installationsanweisung für Standardsoftware

Nach Abschluß aller Test müssen die Testergebnisse der Beschaffungsstelle vorgelegt werden. Die Entscheidung für ein Produkt hat jetzt die Beschaffungsstelle unter Beteiligung der Leiter der Fachabteilung und des IT-Bereichs aufgrund der Testergebnisse und des daraus resultierenden Preis-/Leistungsverhältnisses zu treffen. Hierbei ist insbesondere der Erfüllungsgrad der einzelnen Produkte gegenüber dem Anforderungskatalog in Relation zum Kaufpreis zu stellen. Auch sollten zusätzliche Funktionen der Produkte, die nicht im Anforderungskatalog aufgeführt wurden, aber dennoch für den Einsatz sinnvoll sind, bei der Entscheidung berücksichtigt werden.

Erstellen einer Installationsanweisung
Nach der Entscheidung für ein Produkt muß anschließend für das ausgewählte Produkt eine Installationsanweisung erstellt werden. Während des Testens wurde diejenige Konfiguration des Produktes ermittelt, die einen sicheren und effizienten Produktionsbetrieb erlaubt. Damit

soll Benutzerfreundlichkeit, Ordnungsmäßigkeit und Sicherheit am Arbeitsplatz sichergestellt werden.

Um die geeignete Konfiguration des Produktes im Wirkbetrieb sicherzustellen, müssen bestimmte Parameter vorgegeben werden. Teilweise muß dies durch organisatorische Regelungen begleitet werden.

M 2.85 Freigabe von Standardsoftware
Vor der Übernahme der Standardsoftware in den Wirkbetrieb steht die formelle Freigabe. Verantwortlich für die Freigabe eines Produktes ist die Behörden- bzw. Unternehmensleitung, sie kann dies aber an die Leitung der Fachabteilung oder die Leitung des IT-Bereichs delegieren. Die Fachabteilung kann die durch Behörden- bzw. Unternehmensleitung vorgegebene Freigaberegelung durch eigene Restriktionen weiter einschränken. Der Einsatz nicht freigegebener Software ist zu untersagen (siehe M 2.9 - Nutzungsverbot nicht freigegebener Software).

Der Freigabe geht immer der erfolgreiche Abschluß aller notwendigen Tests voraus (siehe M 2.83 - Testen von Standardsoftware). Eine Freigabe darf nicht erfolgen, wenn während der Tests nicht tolerierbare Fehler, z.B. erhebliche Sicherheitsmängel, festgestellt wurden.

Für die Freigabe sind Installations- bzw. Konfigurationsvorschriften zu erarbeiten, deren Detaillierungsgrad davon abhängig ist, ob die Installation durch die Systemadministration oder den Benutzer vorgenommen werden soll. Die Installations- bzw. Konfigurationsvorschriften sind Ergebnisse der im Rahmen der Beschaffung durchgeführten Tests (siehe M 2.83 - Testen von Standardsoftware). Wenn unterschiedliche Konfigurationen zulässig sind, muß die Auswirkung der einzelnen Konfigurationen auf die Sicherheit dargelegt werden. Insbesondere muß festgelegt werden, ob für alle oder nur einige Benutzer Einschränkungen der Produktfunktionalität oder der Zugriffsrechte vorzunehmen sind. Für die Festlegung dieser Randbedingungen sind der Personal- bzw. Betriebsrat, der Datenschutzbeauftragter sowie der IT-Sicherheitsbeauftragte rechtzeitig zu beteiligen.

Die Freigabe sollte in Form einer schriftlichen Freigabeerklärung erfolgen. In der Freigabeerklärung sollten Aussagen gemacht werden zu den folgenden Punkten:

- Programmname und Versionsnummer,
- Bezeichnung des IT-Verfahrens, in dem das Produkt eingesetzt werden soll,
- Bestätigung, daß die eingesetzten IT-Komponenten den fachlichen Anforderungen entsprechen,
- Datum der Freigabe, Unterschrift des Freigabe-Verantwortlichen,
- Unbedenklichkeitserklärung seitens IT-Sicherheitsbeauftragter, Datenschutzbeauftragter, Personal- bzw. Betriebsrat,

- vorgesehener Zeitpunkt des Einsatzes im Wirkbetrieb,
- für welche Benutzer das Produkt freigegeben wird,
- Installationsanweisung, insbesondere an welchen Arbeitsplätzen es mit welcher Konfiguration installiert wird,
- wer berechtigt ist, es zu installieren,
- wer Zugriff auf die Installationsdatenträger hat und
- welche Schulungen vor Nutzung des Produktes vorzunehmen sind.

Die Freigabeerklärung muß allen Beteiligten zur Kenntnis gegeben werden, insbesondere sollten bei der Freigabeinstanz, dem IT-Bereich, der Fachabteilung und ggf. beim IT-Anwender Kopien vorhanden sein.

Darüber hinaus ist organisatorisch zu regeln, daß die Freigabe und ggf. die notwendigen Tests wiederholt werden, wenn sich durch Versionswechsel oder Patches grundlegende Eigenschaften, insbesondere im Bereich der Sicherheitsfunktionen, geändert haben. Änderungen der genannten Art sind dem für die Freigabe des Produktes Verantwortlichen mitzuteilen.

Weiterhin kann festgelegt werden, welche Standardsoftware-Produkte, abhängig vom Einsatzort und -zweck, generell freigegeben werden. Voraussetzung ist, daß sie zumindest auf Computer-Viren geprüft, daß die Lizenzfragen geklärt und daß sie registriert sind.

M 2.86 Sicherstellen der Integrität von Standardsoftware
Es ist sicherzustellen, daß die freigegebene Standardsoftware nur unverändert installiert werden kann. Damit soll verhindert werden, daß zwischenzeitlich gewollte oder ungewollte Veränderungen vorgenommen werden können, z.B. durch Computer-Viren, Bit-Fehler aufgrund technischer Fehler oder Manipulationen in Konfigurationsdateien.

Die Installation darf daher ausschließlich von Originaldatenträgern bzw. von numerierten Kopien der Originaldatenträger erfolgen. Eine Alternative zur lokalen Installation von Datenträgern ist die Installation über ein lokales Netz von einer dafür freigegebenen Version. Dabei sollte sichergestellt sein, daß nur berechtigte Personen darauf Zugriff haben.

Von den Originaldatenträgern sollten, falls der Datenumfang (z.B. CD-ROM) es zuläßt, Sicherungskopien angefertigt werden. Originaldatenträger und alle Kopien müssen vor unberechtigtem Zugriff geschützt aufbewahrt werden (siehe M 6.21 - Sicherungskopie der eingesetzten Software). Die angefertigten Kopien sollten numeriert und in Bestandsverzeichnisse aufgenommen werden. Kopien, die nicht mehr benötigt werden, sind zu löschen. Vor der Installation muß eine Computer-Virenprüfung durchgeführt werden.

Optional kann über die Originaldatenträger oder über eine während des Tests installierte Referenzversion eine Checksumme (vgl. M 4.34 - Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen) gebildet werden, anhand derer vor der Installation die Integrität der dafür eingesetzten Datenträger bzw. der in lokalen Netzen hinterlegten Versionen oder anhand derer die korrekte Installation überprüft werden kann. Darüber hinaus können installierten Programme zusätzlich zum Schutz vor unberechtigten Veränderungen der freigegebenen Konfiguration mit Checksummen versehen werden. Auf diese Weise können auch Infektionen mit bisher unbekannten Computer-Viren erkannt werden. Damit kann auch festgestellt werden, ob eine Vireninfektion vor oder nach der Installation stattgefunden hat.

M 2.87 Installation und Konfiguration von Standardsoftware
Die freigegebene Software wird entsprechend der Installationsanweisung auf den dafür vorgesehenen IT-Systemen installiert. Die Installationsanweisung beinhaltet neben den zu installierenden Programmen auch Konfigurationsparameter und die Einrichtung der Hardware- und Softwareumgebung.

Abweichungen von der Installationsanweisung bedürfen der Zustimmung der Freigabeinstanz.

Wenn die Benutzer die Software selbst installieren sollen, muß ihnen eine Installationsanweisung zur Verfügung gestellt werden, die eine selbständige Installation ermöglicht. Mindestens die Pilot-Installation durch einen ausgewählten typischen Benutzer sollte durch die IT-Abteilung begleitet werden, um die Verständlichkeit der Installationsanweisung zu überprüfen.

Da Standardsoftware für eine Vielzahl von Einsatzfelder entwickelt wird, enthält sie meist mehr Funktionen, als für die Erfüllung der Fachaufgabe benötigt werden. Damit es zu weniger Problemen und Fehlern bei der Arbeit mit der Software kommt, sollten nur die tatsächlich benötigten Funktionalitäten installiert werden. Funktionalitäten, die zu Sicherheitsproblemen führen können, dürfen nicht freigegeben werden.

Sowohl vor als auch nach der Installation von Software sollte eine vollständige Datensicherung durchgeführt werden. Die erste Datensicherung kann bei nachfolgenden Problemen während der Installation zur Wiederherstellung eines konsolidierten Aufsetzpunktes verwendet werden. Nach der erfolgreichen Installation sollte erneut eine vollständige Datensicherung durchgeführt werden, damit bei späteren Problemen wieder auf den Zustand nach der erfolgreichen Installation des Produktes aufgesetzt werden kann.

Die erfolgreiche Installation wird schriftlich an die für die Aufnahme des Wirkbetriebes zuständige Stelle gemeldet. Optional kann die Installation durch den Einsatz eines sog. „Delta-Tools“ begleitet werden, das alle Veränderungen in einer IT-Umgebung zwischen zwei bestimmbaren Zeitpunkten dokumentiert. Diese Dokumentation von Veränderungen ist insbesondere bei der Deinstallation der Software hilfreich.
Beim Einsatz eines neuen Produktes müssen evtl. Datenbestände übernommen werden, die mit einem Vorgängerprodukt erzeugt wurden. Hat sich bei den Tests gezeigt, daß es dabei

zu Schwierigkeiten kommen kann, sind Hilfestellungen für die Benutzer zu erarbeiten oder die Übernahme von alten Datenbeständen ist zentral durch geschultes Personal durchzuführen.

M 2.88 Lizenzverwaltung und Versionskontrolle von Standardsoftware
Ohne eine geeignete Versionskontrolle und Lizenzkontrolle kommt es erfahrungsgemäß schnell zur Verwendung verschiedenster Versionen auf einem IT-System oder innerhalb einer Organisationseinheit, von denen evtl. einige ohne Lizenz benutzt werden. Auf allen IT-Systemen einer Institution darf ausschließlich lizenzierte Software eingesetzt werden. Diese Regelung muß allen Mitarbeitern bekanntgemacht werden, die Administratoren der verschiedenen IT-Systeme müssen sicherstellen, daß nur lizenzierte Software eingesetzt wird. Dafür müssen sie mit geeigneten Werkzeugen zur Lizenzkontrolle ausgestattet werden.

Häufig werden in einer Institution verschiedene Versionen einer Standardsoftware eingesetzt. Im Rahmen der Lizenzkontrolle muß es auch möglich sein, einen Überblick über alle eingesetzten Versionen zu erhalten. Damit kann gewährleistet werden, daß alte Versionen durch neuere ersetzt werden, sobald dies notwendig ist, und daß bei der Rückgabe von Lizenzen alle Versionen gelöscht werden.

Darüber hinaus sind die verschiedenen Konfigurationen der installierten Software zu dokumentieren. Damit muß es möglich sein, sich einen Überblick zu verschaffen, an welchem IT-System welche sicherheitsrelevanten Einstellungen eines Standardsoftwareproduktes durch die Freigabe vorgegeben und welche tatsächlich installiert wurden. Damit kann z.B. schnell geklärt werden, an welchen Rechnern beim Produkt XYZ die Makro-Programmierung installiert worden ist und an welchen nicht.

M 2.89 Deinstallation von Standardsoftware
Bei der Deinstallation von Software müssen alle Dateien entfernt werden, die für den Betrieb der Software auf dem IT-System angelegt worden sind, und alle Einträge in Systemdateien, die bezüglich des Produktes vorgenommen wurden, gelöscht werden. Bei vielen Softwareprodukten werden während der Installation in diversen Verzeichnissen auf dem IT-System Dateien angelegt oder bestehende Dateien verändert. Häufig wird der Benutzer nicht einmal über alle bei der Installation durchgeführten Veränderungen am IT-System informiert.

Um eine vollständige Deinstallation durchführen zu können, ist es daher hilfreich, die bei der Installation durchgeführten Systemänderungen nachzuhalten, entweder manuell oder mit Hilfe von speziellen Tools. Wird dies nicht vorgenommen, kommt es erfahrungsgemäß dazu, daß eine Deinstallation nur rudimentär stattfindet oder daß sie unterlassen wird aus Furcht, wichtige Dateien bei der Deinstallation zu löschen.

M 2.90 Überprüfung der Lieferung
Nach Eingang einer Lieferung ist anhand der vorhandenen Unterlagen zu überprüfen,

- ob die Lieferung bestellt wurde,

- für wen sie bestimmt ist,
- ob Transportschäden zu erkennen sind,
- ob sie vollständig ist, d.h. ob einerseits alle bestellten Komponenten und andererseits alle gemäß Produktbeschreibung zum Lieferumfang des Produktes gehörenden Komponenten vorhanden sind.

Die Ergebnisse dieser Prüfungen sind in einem Wareneingangsverzeichnis zu dokumentieren, zusammen mit:

- Produktname und Version,
- Produktart, z.B. Textverarbeitung,
- Lieferumfang, also Beschreibung der einzelnen Komponenten inklusive Anzahl und Lieferform (Buch, Diskette, CD-ROM, ...),
- Lieferdatum,
- Lieferart,
- wer es in Empfang genommen hat,
- Aufbewahrungsort und
- an wen es weitergegeben wurde.

Für die Durchführung der funktionalen Tests, sowie die anschließende formelle Freigabe, die Installation und Konfiguration müssen die gelieferten Produkte an die IT-Abteilung weitergegeben werden.
Werden die Produkte nur vorübergehend eingesetzt oder zur Verfügung gestellt, z.B. im Rahmen von Tests, müssen zumindest die Seriennummer und andere produktspezifische Identifizierungsmerkmale in entsprechende Bestandsverzeichnissen vermerkt werden. Wenn die gelieferten Produkte für den dauerhaften Verbleib vorgesehen sind, sind sie mit eindeutigen Identifizierungsmerkmalen (z.B. gruppierte fortlaufende Inventarnummern) zu kennzeichnen. Anschließend müssen sie in ein Bestandsverzeichnis aufgenommen werden. Dieses muß Auskunft geben können über:

- Identifizierungsmerkmale,
- Beschaffungsquellen, Lieferzeiten,
- Verbleib,
- Freigabedatum,
- Installationsdatum und Konfigurationsbesonderheiten und

- Wartungsverträge, Wartungsintervalle.

M 2.91 Festlegung einer Sicherheitsstrategie für das Windows NT Client-Server-Netz

Bevor mit der eigentlichen Konfiguration und Installation von Windows NT in einem Client-Server-Netz begonnen werden kann, müssen zuerst zwei grundlegende Überlegungen angestellt werden:
Zunächst muß geklärt werden, welche Dienstleistung das Betriebssystem erbringen und in welchem Rahmen es diesbezüglich eingesetzt werden soll.
Dies soll anhand einiger Beispiele veranschaulicht werden:

- Das System wird in einem servergestützten PC-Netz als Server für eine größere Arbeitsgruppe eingesetzt, in der unterschiedliche Rechte vergeben werden können. Ggf. sollen aufgrund konkreter Anforderungen zusätzlich Peer-to-Peer-Funktionalitäten in eingeschränkter Form realisiert werden. Beispielsweise sollen einzelne Drucker über Peer-to-Peer-Funktionalität gemeinsam benutzt werden können.

- Das System wird als Client in einem servergestützten PC-Netz mit Windows NT Servern eingesetzt, bei dem auf die Peer-to-Peer-Funktionalität zum Austausch von Daten verzichtet werden kann.

- Das System wird als Client in einem servergestützten PC-Netz mit Novell NetWare Servern eingesetzt.

- Das System wird als Server in einem PC-Netz mit MS-DOS-, MS-Windows-, WfW- oder Windows 95-Clients eingesetzt.

- Das System wird als Server in einem Netz eingesetzt, in dem ausschließlich Windows NT-Clients vorhanden sind.

Durch die Verwendung von Peer-to-Peer-Funktionalitäten innerhalb eines Windows NT Netzes können zusätzliche Sicherheitsprobleme entstehen (siehe dazu auch Kapitel 6.3 - Peer-to-Peer-Netz). Deshalb sollte auf die Verwendung von Peer-to-Peer-Funktionalitäten innerhalb von Windows NT Netzen verzichtet werden. Peer-to-Peer-Funktionalitäten sollten höchstens als Übergangslösung eingeschränkt zugelassen werden, wenn z.B. WfW-Rechner oder nichtnetzfähige Drucker in das Windows NT-Netz eingebunden werden sollen.
Anschließend müssen diese Überlegungen in eine Sicherheitsstrategie übersetzt werden.
Dabei zeigt sich, daß je nach bereits vorhandener Systemumgebung und Organisationsstruktur sowie der ggf. vorzusehenden Restriktionen an eventuelle Peer-to-Peer-Funktionalitäten ein mehr oder weniger großer Aufwand bei der Entwicklung einer dazu passenden Sicherheitsstrategie notwendig ist.
Es wird nachfolgend eine methodische Vorgehensweise aufgezeigt, mittels derer eine umfassende Sicherheitsstrategie für ein Client-Server-Netz entwickelt werden kann. Da jedoch Windows NT

in verschiedenen Konfigurationen eingesetzt werden kann, ist für die jeweilige Ausprägung individuell zu entscheiden, welche der beschriebenen Schritte anzuwenden sind.

Festlegung einer Sicherheitsstrategie für ein Client-Server-Netz

In der Sicherheitsstrategie muß aufgezeigt werden, wie ein Client-Server-Netz für die jeweilige Organisation sicher aufgebaut, administriert und betrieben wird. Nachfolgend werden die einzelnen Entwicklungsschritte einer solchen Strategie vorgestellt:

1. Definition der Client-Server-Netzstruktur
   Im ersten Schritt sind die logische Struktur des Client-Server-Netzes, insbesondere die Zuordnung der Server und der Netz-Domänen festzulegen (siehe M 2.93 - Planung des Windows NT Netzes). Nach Möglichkeit sollte auf die Verwendung von Peer-to-Peer-Funktionalitäten verzichtet werden, da diese die Sicherheit des Client-Server-Netzes beeinträchtigen können. Sofern sich dies jedoch nicht vermeiden läßt, sind verbindliche Regelungen für die Nutzung von Peer-to-Peer-Funktionalitäten zu treffen (siehe M 2.67 - Festlegung einer Sicherheitsstrategie für das Peer-to-Peer-Netz).

2. Regelung der Verantwortlichkeiten
   Ein Client-Server-Netz sollte von einem geschulten Netzadministrator nebst Stellvertreter sicher betrieben werden. Diese allein dürfen Sicherheitsparameter im Netz verändern. Sie sind z.B. dafür zuständig, auf den Servern den entsprechenden Verantwortlichen Administrationsrechte und -werkzeuge zur Verfügung zu stellen, damit diese die Vergabe von Datei- und Verzeichnisberechtigungen, die Freigabe der von anderen benötigten Verzeichnissen bzw. Anwendungen, den Aufbau von Benutzergruppen und -konten sowie die Einstellung der Systemrichtlinien für Benutzer, Zugriffskontrolle und Überwachung vornehmen können.
   Die Verantwortlichkeiten der einzelnen Benutzer im Client-Server-Netz sind unter Schritt 11 dargestellt.

3. Festlegung von Namenskonventionen
   Um die Verwaltung des Client-Server-Netzes zu erleichtern, sollten eindeutige Namen für die Rechner, Benutzergruppen und die Benutzer verwendet werden.
   Zusätzlich sollten Namenskonventionen für die Freigabenamen von Verzeichnissen oder Druckern eingeführt werden (siehe M 2.67 - Festlegung einer Sicherheitsstrategie für das Peer-to-Peer-Netz). Sollen keine Rückschlüsse auf den Inhalt eines freigegebenen Verzeichnisses möglich sein, sind entsprechende Pseudonyme zu verwenden. Soll eine freigegebene Ressource nicht als solche erkennbar sein, ist dem Freigabenamen das Zeichen „$“ anzuhängen. Letzteres empfiehlt sich immer dann, wenn Verzeichnisse nur zum bilateralen Austausch von Informationen zwischen zwei Anwendern oder zum Zugriff auf Ressourcen, die nur einzelnen Benutzern bekannt sein sollen, freigegeben werden.

4. Festlegung der Regeln für Benutzerkonten
   Vor der Einrichtung von Benutzerkonten sollten die Restriktionen, die für alle bzw. für be-

stimmte dieser Konten gelten sollen, festgelegt werden. Dies betrifft insbesondere die Regelungen für Paßwörter und für die Reaktion des Systems auf fehlerhafte Login-Vorgänge. Die festgelegten Regelungen können mit Hilfe der Option „Richtlinien“ des Benutzer-Managers umgesetzt werden (siehe M 4.48 - Paßwortschutz unter Windows NT).

5. Einrichtung von Gruppen
   Zur Vereinfachung der Administration sollten Benutzerkonten, für die die gleichen Anforderungen gelten, zu Gruppen zusammengefaßt werden. Benutzerrechte sowie Datei-, Verzeichnis- und Freigabeberechtigungen und ggf. weitere vordefinierte Funktionen werden dann den Gruppen und nicht einzelnen Benutzerkonten zugeordnet. Die Benutzerkonten erben die Rechte und Berechtigungen der Gruppen, denen sie angehören. So ist es z.B. denkbar, alle Mitarbeiter einer Abteilung in einer Gruppe zusammenzufassen. Eine Zuweisung von Benutzerrechten und -berechtigungen an einzelne Benutzer sollte nur erfolgen, wenn dies ausnahmsweise unumgänglich ist.

6. Festlegung der Benutzerrechte
   Rechte gestatten einem Benutzer die Ausführung bestimmter Aktionen auf dem System. Sie beziehen sich auf das gesamte System, sind keinem speziellen Objekt zugeordnet und können die Berechtigungen für ein Objekt außer Kraft setzen, da ein Recht Vorrang vor allen Datei- und Verzeichnisberechtigungen hat. Wenn sich ein Benutzer bei einem Konto anmeldet, dem die gewünschten Rechte entweder direkt oder über die Gruppenmitgliedschaft erteilt wurden, kann er die entsprechenden Aktionen ausführen. Besitzt ein Benutzer nicht die geeigneten Rechte, so verhindert Windows NT jeden Versuch, die betreffenden Aktionen auszuführen.
   Wie schon zuvor dargestellt, sollten Benutzerrechte möglichst nur Gruppen und nicht einzelnen Benutzern zugeordnet werden.
   Windows NT legt bei der Installation Voreinstellungen fest, die in der Regel für einen sicheren und effizienten Betrieb ausreichend sind. Empfehlenswert erscheint jedoch, der Gruppe „Jeder“ das Recht „System herunterfahren“ und der Gruppe „Jeder“ und ggf. der Gruppe „Gäste“ das Recht „Lokale Anmeldung“ zu entziehen (siehe M 4.50 - Strukturierte Systemverwaltung unter Windows NT).

7. Festlegung der Vorgaben für Protokollierung
   Windows NT stellt sehr ausführliche Möglichkeiten der Protokollierung sicherheitsrelevanter Ereignisse zur Verfügung, die bei vollständiger Nutzung in der Lage sind, das System weitgehend mit Auditing zu beschäftigen und dabei große Mengen an Plattenplatz zu verbrauchen. Dabei kann ein Spektrum von Ereignisarten aufgezeichnet werden, das sich von systemweiten Ereignissen, wie zum Beispiel dem Anmelden eines Benutzers bis hin zum Versuch eines Benutzers, eine bestimmte Datei zu lesen, erstreckt. Sowohl die erfolgreichen als auch die fehlgeschlagenen Versuche, eine Aktion durchzuführen, lassen sich aufzeichnen. Bei der Konfiguration der Protokollierung ist jedoch zu beachten, daß ein Mehr an Protokollierung nicht unbedingt auch die Sicherheit des überwachten Systems erhöht. Protokolldateien, die nicht ausgewertet werden oder die aufgrund ihres Umfangs nur mit großem Aufwand auswertbar sind, führen nicht zu einer besseren Kontrolle der

Systemabläufe, sondern sind letztlich nutzlos. Aus diesen Gründen sollte die Protokollierung so eingestellt werden, daß sie im Normalfall nur die wirklich bedeutsamen Ereignisse aufzeichnet (siehe M 4.54 - Protokollierung unter Windows NT).

8. Regelungen zur Datenspeicherung
   Es ist festzulegen, wo Benutzerdaten gespeichert werden (siehe M 2.138 - Strukturierte Datenhaltung). So ist denkbar, daß Benutzerdaten nur auf einem Server abgelegt werden. Eine Datenspeicherung auf der lokalen Festplatte ist bei diesem Modell nicht erlaubt. Möglich ist aber auch, bestimmte Benutzerdaten nur auf der lokalen Festplatte abzulegen. Nach welcher Strategie verfahren werden soll, muß an den konketen Umständen des Einzelfalles festgelegt werden. Eine generelle Empfehlung auszusprechen, ist nicht möglich.

9. Einrichtung von Projektverzeichnissen
   Um eine saubere Trennung von Benutzer- und projektspezifischen Daten untereinander sowie von den Programmen und Daten des Betriebssystems durchzusetzen, sollte eine geeignete Verzeichnisstruktur festgelegt werden, mit der eine projekt- und benutzerbezogene Dateiablage unterstützt wird. So können beispielsweise zwei Hauptverzeichnisse \Projekte und \Benutzer angelegt werden, unter denen dann die Dateien und Verzeichnisse der Projekte bzw. Benutzer in jeweils eigenen Unterverzeichnissen abgelegt werden.

10. Vergabe der Zugriffsrechte
    Für die Server ist festzulegen, welche Verzeichnisse und bei Nutzung von NTFS-Partitionen welche Dateien für den Betrieb freizugeben und welche Zugriffsrechte ihnen zuzuweisen sind (siehe M 4.53 - Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnissen unter Windows NT). Zusätzlich ist bei Nutzung von Peer-to-Peer-Funktionalitäten auf der Ebene der Clients zu entscheiden, welche Verzeichnisse für Netzzugriff freizugeben sind (siehe M 2.94 - Freigabe von Verzeichnissen unter Windows NT).
    Das zuvor gesagte gilt analog für die Freigabe von Druckern.

11. Verantwortlichkeiten für Administratoren und Benutzer im Client-Server-Netz
    Neben der Wahrnehmung der Netzmanagementaufgaben (siehe Nr. 2) müssen weitere Verantwortlichkeiten festgelegt werden. Es ist festzulegen, welche Verantwortung die einzelnen Administratoren im Client-Server-Netz übernehmen müssen. Dies können zum Beispiel Verantwortlichkeiten sein für

    - die Auswertung der Protokolldateien auf den einzelnen Servern oder Clients,
    - die Vergabe von Zugriffsrechten,
    - das Hinterlegen und den Wechsel von Paßwörtern und
    - die Durchführung von Datensicherungen.

    Auch die Endbenutzer müssen in einem Client-Server-Netz bestimmte Verantwortlichkeiten übernehmen, sofern ihnen Rechte zur Ausführung administrativer Funktionen gegeben werden. In der Regel beschränken sich diese Verantwortlichkeiten jedoch auf die Vergabe

von Zugriffsrechten auf die eigenen Dateien, sofern diese explizit festgelegt und nicht von Voreinstellungen des übergeordneten Verzeichnisses übernommen werden.

12. Schulung
    Abschließend muß festgelegt werden, welche Benutzer zu welchen Punkten geschult werden müssen. Erst nach ausreichender Schulung kann der Wirkbetrieb aufgenommen werden. Insbesondere die Administratoren sind hinsichtlich der Verwaltung und der Sicherheit von Windows NT gründlich zu schulen.

Die so entwickelte Sicherheitsstrategie ist zu dokumentieren und im erforderlichen Umfang den Benutzern des Client-Server-Netzes mitzuteilen.

M 2.92 Durchführung von Sicherheitskontrollen im Windows NT Client-Server-Netz

Die folgenden Punkte sollten auf der Ebene der Server in einem Windows NT Client-Server-Netz regelmäßig auf Einhaltung und Effektivität kontrolliert werden (siehe auch M 4.54 - Protokollierung unter Windows NT):

- System-Sicherheits-Einstellungen
  Die korrekte Einstellung der sicherheitsrelevanten Einträge in der Registrierung, d.h. im wesentlichen die Einträge im Bereich HKEY_LOCAL_MACHINE, ist regelmäßig zu kontrollieren, indem die Einträge des Sicherheitsprotokolle, die sich auf die Registrierung beziehen, überprüft werden.

- Benutzung von privilegierten Benutzerkonten
  Die Benutzung privilegierter Benutzerkonten, also von Konten mit erweiterten Rechten und Berechtigungen wie etwa Administratoren, ist regelmäßig durch Überprüfung der Einträge im Sicherheitsprotokoll zu überprüfen. Ebenso ist das Protokoll auf Anmeldeversuche auf das Gastbenutzerkonto zu überprüfen.

- Fehlgeschlagene Zugriffsversuche (Berechtigungsverstöße)
  Sofern Zugriffe auf Dateien und/oder die Registrierung aufgezeichnet werden, ist das Sicherheitsprotokoll wöchentlich, bei Bedarf auch öfter, auf das Vorliegen fehlgeschlagener Zugriffsversuche zu überprüfen. Werden Berechtigungsverstöße festgestellt, ist die Ursache zu ermitteln.

- Systemintegrität
  Die Systemintegrität ist regelmäßig zu überprüfen; insbesondere sind die Daten der letzten Veränderung sowie die Zugriffsrechte auf die wichtigen Systemdateien zu überprüfen und mit den Werten, die unmittelbar nach der Installation des Systems sowie bei der jeweils vorherigen Überprüfung gegeben waren, zu vergleichen. Da diese Kontrolle mit Hilfe der von Windows NT gebotenen Möglichkeiten relativ aufwendig ist, sollten hier geeignete Zusatzwerkzeuge eingesetzt werden, beispielsweise das Shareware-Programm DumpACL oder das mit der Technischen Referenz (dem „Resource Kit“) zu Windows NT ausgelieferte Dienstprogramm WinDiff, mit dem sich Inhalte von Verzeichnissen und Dateien vergleichen lassen.

- Unbenutzte Benutzerkonten
  Es ist sicherzustellen, daß die Konten ehemaliger Beschäftigter sofort deaktiviert und nach einer geeigneten Übergangszeit (ca. 1/2 Jahr) vom System gelöscht werden. Da die Zeit des letzten Anmeldens am System nicht angezeigt wird, sind zu diesem Zweck nach Möglichkeit alle Benutzerkonten mit einem Verfallsdatum einzurichten, das in gewissen Zeitabständen (z.B. jährlich) auf Antrag des Benutzers aktualisiert werden muß. Inaktive, d.h. abgelaufene, Benutzerkonten sind zu löschen. Die Eigentümer sind vorab zu informieren. Die Liste der definierten Benutzer ist regelmäßig zu überprüfen, um sicherzustellen, daß nur aktive Beschäftigte auf dem System arbeiten.

- Gruppenzugehörigkeit
  Eine strukturierte Systemadministration setzt voraus, daß Systemrechte und Objektberechtigungen möglichst nicht an einzelne Benutzer, sondern an Benutzergruppen vergeben werden. Es ist sicherzustellen, daß bei Änderungen in den Beschäftigungsverhältnissen die Mitgliedschaft der einzelnen Benutzer in den Benutzergruppen den organisatorischen Vorgaben angepaßt wird. Daher ist regelmäßig zu prüfen, ob die Mitgliedschaften der Benutzer in den verschiedenen Benutzergruppen noch dem aktuellen Stand entspricht. Weiterhin ist bei der Veränderung der Gruppenmitgliedschaft eines Benutzers zu prüfen, ob dies zu einer Anhäufung von Benutzerrechten führt. Insbesondere ist in regelmäßigen Abständen zu überprüfen, ob die Zuweisung von Sonderrechten an Gruppen oder einzelne Benutzer noch den aktuellen organisatorischen Vorgaben entsprechen.

- Berechtigungskontrolle
  Es ist sicherzustellen, daß die Eigentümer von Dateien und Verzeichnissen ihre Verpflichtung verstehen, anderen Benutzern nur dann Zugriff zu gewähren, wenn dies erforderlich ist. Mit dem Datei-Manager bzw. Explorer ist regelmäßig zu überprüfen, daß auf sensitive Daten nicht zu weitgehende Berechtigungen vergeben wurden. Kritisch sind insbesondere Berechtigungen für die Gruppen „Jeder“ und „Gäste“ bzw. „Domänen-Gäste“. Sofern temporäre Berechtigungen zum Einsatz kommen, ist sicherzustellen, daß dies nur dann geschieht, wenn es erforderlich ist, und daß diese Berechtigungen sorgfältig überwacht werden.

Es sind Prozeduren bzw. Verfahren zu entwickeln für den Fall, daß Abweichungen von den festgelegten Einstellungen auftreten.
Diese Prozeduren müssen folgende Punkte enthalten:

- wer wird wann informiert,

- Begründung für die eventuelle Wahl abweichender Einstellungen und Angabe, ob hierdurch möglicherweise ein Sicherheitslücke entsteht,

- Schritte zur Behebung der Sicherheitslücke,

- Schritte zur Identifizierung der Ursache der Sicherheitslücke.

Die Durchführung der hier beschriebenen Kontrollen auf der Ebene von Clients sollte nur dann durchgeführt werden, wenn sichergestellt ist, daß damit keine unzulässigen Leistungskontrollen der Benutzer dieser Clients verbunden sind und wenn die datenschutzrechtlich korrekte Behandlung der Protokoll-Informationen gewährleistet werden kann.

M 2.93 Planung des Windows NT Netzes
Windows NT kann in einem Netz in verschiedenen Konfigurationen eingesetzt werden. Um die Vor- und Nachteile der einzelnen Einsatzarten abschätzen und nachvollziehen zu können, muß zunächst kurz auf das Sicherheitssystem von Windows NT eingegangen werden. Grundsätzlich behält das Betriebssystem die Kontrolle über alle Ressourcen. Ein Benutzer kann nur dann auf Ressourcen zugreifen, wenn er die dazu notwendigen Rechte und Berechtigungen hat. Der Zugang zum System ist nur über ein gültiges Benutzerkonto möglich, das mittels Paßwort geschützt werden kann. Durch die Sicherheitskontenverwaltung (SAM - Security Account Manager) werden die Informationen über Benutzer- und Gruppenkonten in der Security Account Database, die häufig auch als SAM-Datenbank bezeichnet wird, verwaltet. Das Betriebssystem generiert bei der Anmeldung eines Benutzers für diesen unter Berücksichtigung der Eintragungen in der SAM-Datenbank ein Access-Token. Der Sicherheitskontrollmonitor (Security Reference Monitor) überprüft anhand dieses Tokens, ob der Benutzer die Berechtigung hat, auf bestimmte Objekte zuzugreifen und ob er das Recht hat, die angeforderten Aktionen durchzuführen (beispielsweise eine Datei löschen oder das System herunterfahren).

Windows NT unterstützt die Arbeit im Netz mit folgenden Konzepten:

1. Arbeitsgruppen
   Rechner können zu Arbeitsgruppen zusammengefaßt werden und im Rahmen des Peer-to-Peer Konzeptes über das Netz Ressourcen gemeinsam nutzen (siehe dazu auch Kapitel 6.3 - Peer-to-Peer-Netz in [BSI1998]).
   Jeder Rechner in einem solchen Netz kann gleichzeitig sowohl als Server als auch als Workstation benutzt werden. Realisiert wird dies durch Freigabe von Ressourcen auf den einzelnen Rechnern. Jede Windows NT Workstation, die in einer Arbeitsgruppe eingesetzt wird, verwaltet ihre eigene SAM-Datenbank und damit auch eigene Benutzer- und Gruppenkonten. Die Eintragungen in dieser Datenbank können von keinem anderen Rechner der Arbeitsgruppe benutzt werden. Dies hat zur Folge, daß eine zentrale Administration nicht möglich ist. Für den Zugriff auf freigegebene Ressourcen wird in der Regel ein Paßwort benötigt.
   Besonders nachteilig wirkt sich bei diesem Konzept aus, daß keine ausreichende Kontrolle über die Rechte der einzelnen Benutzer möglich ist. Die Einrichtung von Arbeitsgruppen sollte daher möglichst vermieden werden.

2. Netz mit dediziertem Server Hierbei handelt es sich um ein Netz mit Client-Server-Struktur. Es wird dabei festgelegt, welche Rechner als Server und welche Rechner als Clients fungieren. Server können Verzeichnisse und/oder Drucker freigeben bzw. Anwendungen wie z.B. Mail, Schedule+, Fax global zur Verfügung stellen. Clients können hingegen nur die von Servern zur Verfügung gestellten Ressourcen nutzen.

Ein NT-Rechner kann mit dem Betriebssystem „Windows NT Server“ oder „Windows NT Workstation“ betrieben werden. In kleinen Netzen kann auch eine Lizenzversion „Windows NT Workstation“ als Server betrieben werden. Zu beachten ist aber, daß sich aufgrund der lizenzrechtlichen Einschränkung nicht mehr als 10 Benutzer gleichzeitig über das Netz auf diesem Rechner anmelden dürfen. Reicht dies nicht aus, muß Windows NT Server installiert werden. Auf Servern unter dem Betriebssystem Windows NT sollten generell keine normalen Benutzer arbeiten. Die Clients müssen nicht zwingend unter Windows NT betrieben werden.
Der Vorteil dieses Konzeptes liegt in der Zentralisierung der Datenhaltung und -verwaltung. Sofern in einem solchen Netz nur ein Server zum Einsatz kommt, ist für die Arbeit im Netz auch nur auf diesem Rechner je Benutzer ein Konto anzulegen. Für die Benutzung von Ressourcen oder Diensten des Servers über das Netz ist lediglich die Anmeldung des Benutzers an diesem einem Rechner notwendig. Für kleinere Netze kann der Einsatz dieses Konzeptes durchaus wirtschaftlich sinnvoll sein.
Sofern jedoch die Kapazität eines Servers nicht mehr ausreicht, um den jeweiligen Anforderungen hinsichtlich Geschwindigkeit und Plattenspeicherplatz zu genügen, nimmt der Verwaltungsaufwand erheblich zu, wenn ein oder mehrere Server dem Netz hinzugefügt werden. Sollen alle Benutzer das Recht erhalten, auf alle Server über das Netz zuzugreifen, müssen die Benutzerkonten auf jedem einzelnen Server eingerichtet und gepflegt werden.

3. Domänen-Konzept
   Eine Domäne unter Windows NT ist eine Gruppe von Rechnern, die über eine gemeinsame Sicherheits- und Benutzerkontendatenbank (SAM-Datenbank) verfügt. Für den Benutzer bedeutet dies, daß er sich nur einmal an der Domäne anmelden muß. Danach stehen ihm sämtliche für ihn freigegebene Ressourcen zur Verfügung, unabhängig davon, auf welchem Server sich diese befinden.
   Ein Server der Domäne unter dem Betriebssystem Windows NT Server dient als primärer Domänencontroller (PDC). Daneben kann die Domäne einen oder mehrere Backup Domänencontroller (BDC), Mitgliedsserver, d.h. Server ohne Domänencontrollerfunktionalität (siehe auch weiter unten) und Windows NT Workstations enthalten. Außerdem können zu einer Domäne Arbeitsstationen mit anderen Betriebssystemen wie z.B. Windows für Workgroups, Windows 95 oder MS-DOS gehören. Die Entscheidung, ob ein Server als primärer Domänenkontroller, als Backup Domänenkontroller oder als Mitgliedsserver fungieren soll, muß vor der Installation getroffen werden, da später eine Änderung ohne Neuinstallation nicht mehr möglich ist. Zum besseren Verständnis soll zunächst näher auf die verschiedenen Serverarten einer Domäne eingegangen werden:

   (a) Primärer Domänencontroller (PDC)
       Ein Server einer Windows NT Domäne muß zwingend als primärer Domänenkontroller eingerichtet werden. Der Einsatz des Betriebssystems Windows NT Server ist zwingend, da die Workstation-Version diese Funktionalität nicht enthält. Auf dem PDC wird die zentrale Benutzerkontendatenbank (SAM-Datenbank) für die Domäne verwaltet. Alle Änderungen können nur an dieser Datenbank mit Hilfe

des Benutzermanagers für Domänen durchgeführt werden. Außerdem werden die Benutzeranmeldungen vom primären Domänenkontroller bearbeitet.

(b) Backup Domänencontroller (BDC)
Andere Server der Domäne können als Backup Domänencontroller eingerichtet werden. Auch hier ist der Einsatz des Betriebssystems Windows NT Server zwingend. Auf jeden Backup Domänencontroller wird automatisch eine Read-only-Kopie der Benutzerdatenbank der Domäne repliziert. Die Synchronisation erfolgt regelmäßig. Auch Backup Domänenkontroller können Benutzeranmeldungen für die Domäne bearbeiten. Dadurch ist es gerade bei einer großen Anzahl von Benutzern möglich, die durch die Benutzeranmeldungen entstehende Last auf mehrere Server zu verteilen. Jede Domäne sollte möglichst über mindestens einen Backup Domänencontroller verfügen, um die Verwaltung der Domäne bei Ausfall des primären Domänencontrollers sicherzustellen. In einem solchen Fall ist es möglich, den Backup Domänencontroller zum primären Domänencontroller hochzustufen. Sofern kein Backup Domänencontroller eingerichtet wurde, kann einer Domäne durch Neuinstallation kein neuer primärer Domänenkontroller hinzugefügt werden.
Wenn die Server der Domäne auf verschiedene über WAN-Verbindungen zusammengeschaltete Liegenschaften verteilt sind, sollte in jeder Liegenschaft wenigstens ein Backup Domänencontroller installiert sein.

(c) Mitgliedsserver (Memberserver)
Hierbei handelt es sich um Server, die weder als primärer noch als Backup Domänencontroller eingerichtet wurden. Diese Server verfügen über keine Kopien der Benutzerkontendatenbank der Domäne. Die Benutzeranmeldung für die Domäne kann von einem solchen Server daher nicht bearbeitet werden.
Folgende Gründe sprechen dafür, einen Server als Mitgliedsserver in die Domäne einzufügen:

- Ein Server hat zeitkritische Aufgaben durchzuführen oder es müssen auf diesem Rechner umfangreiche Applikationen ausgeführt werden, so daß der Aufwand von Benutzeranmeldungen nicht akzeptabel ist.
- Ein Server soll in naher Zukunft in eine andere Domäne eingefügt werden. Dies ist dann einfacher möglich, als wenn er als Backup Domänencontroller konfiguriert wäre.

Wesentlicher Ansatz des Domänenkonzeptes ist es, daß alle Benutzerkonten für jede Domäne nur einmal definiert werden müssen. Die Verwaltung erfolgt in der zentralen Benutzerdatenbank auf dem primären Domänenkontroller. Für die Benutzer bedeutet dies, daß sie sich bei der Benutzeranmeldung nur gegenüber dieser Datenbank authentisieren müssen. Danach können sie auf alle Objekte und Ressourcen der Domäne zugreifen, sofern sie die entsprechenden Berechtigungen besitzen. Dabei spielt keine Rolle, auf welchem Server sich diese Objekte und Ressourcen befinden. Arbeitet der Benutzer auf einem Rechner unter dem Betriebssytem Windows NT Workstation, genügt die Benutzeranmeldung gegenüber der zentralen Benutzerdatenbank, um auch auf diesen Rechner Zugang zu erhalten.

Organisation von Domänen
Innerhalb eines Netzes können mehrere Domänen eingerichtet werden; jede muß dabei aber über einen eindeutigen Namen verfügen. Jede Domäne verwaltet ihre eigene zentrale SAM-Datenbank. Die jeweiligen Benutzer- und Gruppenkonten sind daher auch nur in der Domäne gültig, in der sie definiert wurden.
Es kann aber innerhalb eines Netzes die Notwendigkeit bestehen, daß Benutzer einer Domäne auf Ressourcen einer anderen Domäne zugreifen müssen. Hierzu gibt es den Mechanismus der Vertrauensbeziehungen zwischen Domänen.
Dabei unterscheidet man zwischen vertrauten Domänen (Trusted Domain) und vertrauenden Domänen (Trusting Domain). Den Benutzerkonten und globalen Gruppen der vertrauten Domäne können in der vertrauenden Domäne Rechte und Berechtigungen zugewiesen werden, wodurch auch der Zugriff auf freigegebene Ressourcen möglich wird.
Es sind folgende Domänen-Modelle möglich:

1. Single-Domänen-Modell
   Dies ist das einfachste Domänen-Modell, da in einem Netz hierbei nur eine einzige Domäne existiert. Daher besteht nicht die Notwendigkeit, Vertrauensbeziehungen zu verwalten. Im gesamten Netz existiert hierbei nur eine einzige SAM-Datenbank, über die die Verwaltung erfolgt. Eine Abwandlung dieses Modells liegt vor, wenn in einem Netz mehrere Einzeldomänen eingerichtet wurden, zwischen denen keine Vertrauensbeziehungen definiert wurden. Hierbei verwaltet jede Domäne ihre eigene SAM-Datenbank und ihre eigenen Benutzer- und Gruppenkonten. Das Single-Domänen-Modell eignet sich besonders gut für Netze mit wenigen Benutzern (ca. 200 bis 300) und wenigen Computerkonten. Nachteilig ist bei diesem Modell, daß die Performance bei steigender Benutzer und Gruppenanzahl abnimmt. Außerdem ist eine Gruppierung der Ressourcen nach Organisationseinheiten in dem Sinne, daß ein Server z.B. für eine Abteilung reserviert ist, nicht möglich.

2. Master-Domänen-Modell
   Kennzeichen dieses Modells ist, daß ein Netz in mehrere Domänen eingeteilt wird, wobei eine Domäne zentral alle Benutzer- und Gruppenkonten verwaltet. Diese Domäne wird Master-Domäne genannt. In den anderen Domänen werden die Ressourcen zusammengefaßt. Die Ressourcen-Domänen vertrauen dabei der Domäne mit den Benutzerkonten.
   Dieses Domänen-Modell läßt sich nach Angaben von Microsoft bis zu einer Zahl von ca. 15.000 Benutzern einsetzen. Besonders geeignet ist dieses Modell, wenn eine Organisation aus mehreren Abteilungen besteht und alle Abteilungen ihre eigenen Ressourcen verwalten sollen, wobei die Benutzeradministration zentral erfolgt. Es ist bei diesem Domänen-Modell möglich, für die Administration der Ressourcen-Domänen jeweils einen eigenen Administrator zu benennen. Außerdem ist ein zentrales Sicherheitsmanagement möglich.

3. Multiple-Master-Domänen Dieses Modell besteht aus mehreren Master-Domänen, die sich gegenseitig vertrauen. Die Benutzer- und Gruppenkonten werden in diesen Master-Domänen geführt. Darüberhinaus existieren Ressourcen-Domänen, die einseitig allen

Master-Domänen vertrauen.
Die explizite Vertrauensbeziehung zwischen Domäne 1 und Domäne 3 ist nötig, da Vertrauensstellungen nicht transitiv sind; d.h. vertrauen sich Domäne 1 und Domäne 2 sowie Domäne 2 und Domäne 3 gegenseitig, folgt nicht daraus, daß sich auch Domäne 1 und 3 gegenseitig vertrauen.
Das Master-Domänen-Konzept kommt häufig zum Einsatz, wenn die Benutzerzahl größer als 15.000 ist. Außerdem läßt es dieses Konzept zu, ein Netz nach Hauptabteilungen aufzuteilen und die Ressourcen durch die einzelnen Abteilungen verwalten zu lassen. Dazu wird je Hauptabteilung eine Master-Domäne eingerichtet. Die Benutzer einer Hauptabteilung erhalten ihre Benutzerkonten in der Master-Domäne. Die Ressourcen werden durch die Abteilungen in den Ressourcen-Domänen verwaltet. Auch ist es möglich, ein Netz nach Standorten zu organisieren. Hierbei wird für jeden Standort eine Master-Domäne und für jede Abteilung eine Ressourcen-Domäne eingerichtet. Dieses Domänenmodell ist skalierbar, wobei die Größe einer Organisation keine Grenze setzt. Es besteht die Möglichkeit eines zentralen Sicherheitsmanagement und globale Gruppen und Benutzerkonten brauchen organisationsweit nur einmal eingerichtet zu werden.
Es sei abschließend darauf hingewiesen, daß dieses Modell große Disziplin bei der Administration und sorgfältige Planung benötigt. Besondere Sorgfalt ist auf die Definition der Vertrauensbeziehungen zu legen. Außerdem muß zwingend verhindert werden, daß in den Ressourcen-Domänen Benutzerkonten eingerichtet werden.

4. Complete-Trust-Modell (Vertrauensverbund) Bei diesem Modell bestehen gegenseitige Vertrauensbeziehungen zwischen allen Domänen eines Netzes. In jeder Domäne werden sowohl Ressourcen als auch Benutzer- und Gruppenkonten verwaltet.
Bei diesem Modell ist es möglich, den Abteilungen einer Organisation sowohl die Verwaltung der Benutzerkonten als auch die Verwaltung der Ressourcen zu überlassen. Es wird keine zentrale Abteilung zur Verwaltung benötigt. Das Modell ist mit jeder Anzahl von Benutzern skalierbar. Dieses Modell hat aber auch erhebliche Nachteile. So ist die Kontrolle, ob die Sicherheitspolitik eingehalten wird, schwierig. Dies erschwert es, ein zentrales Sicherheitsmanagement aufzubauen. Außerdem ist es schwierig, die Tätigkeit der einzelnen Administratoren zu koordinieren. Wenn ein Netz sehr viele Domänen umfaßt, sind sehr viele Vertrauensbeziehungen zu verwalten, was letztlich unübersichtlich ist.

Es können keine globalen Aussagen dazu gemacht werden, welches der beschriebenen Domänen-Modelle in einer Organisation Anwendung finden sollte. Dies kann nur in Abhängigkeit von der physischen und logischen Netzstruktur sowie der Verteilung von Daten, Anwendungen und Benutzern im Netz spezifisch festgelegt werden. Die Bestimmung der optimalen Domänenstruktur bedarf daher einer detaillierten Analyse, die für umfangreiche Netze aufwendig werden kann und ggf. durch Planungssoftware zu unterstützen ist.

M 2.94 Freigabe von Verzeichnissen unter Windows NT

Durch die Möglichkeit der Freigabe von Verzeichnissen können Administratoren unter Windows NT den Benutzern den netzweiten Zugriff auf diese Verzeichnisse eröffnen. Normalerwei-

se erfolgt diese Freigabe nur auf Verzeichnissen auf Servern, doch können in Einzelfällen auch durch Freigaben auf Clients im Netz Peer-to-Peer Funktionalitäten bereitgestellt werden.

Für freigegebene Verzeichnisse können Mitglieder der Gruppe „Administratoren“ oder „Hauptbenutzer“ Berechtigungen festlegen. Dabei spielt es keine Rolle, ob sich diese Verzeichnisse auf Laufwerken befinden, das für das NTFS-, das FAT- oder das HPFS-Dateisystem formatiert wurden. Diese Berechtigungen gelten jedoch nur für Zugriffe über das Netz und in einheitlicher Form für alle Dateien und Unterverzeichnisse in den freigegebenen Verzeichnissen.

Berechtigungen, die für ein freigegebenes Verzeichnis festgelegt werden, das sich auf einem NTFS-Datenträger befindet, sind zusätzlich zu NTFS-Berechtigungen wirksam, die für das Verzeichnis selbst festgelegt wurden. Mit Berechtigungen freigegebener Verzeichnisse wird das maximal erlaubte Zugriffsrecht definiert. Besitzt ein Benutzer beispielsweise die Berechtigung „Lesen“ für das freigegebene Verzeichnis, andererseits aber nur die NTFS-Berechtigung „Anzeigen“ für das Verzeichnis selbst, so ist sein Zugriffsrecht auf „Anzeigen“ beschränkt.

Von der Möglichkeit der Freigabe einzelner Laufwerke oder Verzeichnisse auf den Clients sollte kein Gebrauch gemacht werden, da dies zu unüberschaubaren Rechtestrukturen und ggf. sogar zum Unterlaufen allgemeinen Sicherheitsvorgaben führen kann.

Weiterhin ist zu beachten, daß Windows NT grundsätzlich die Wurzelverzeichnisse aller Platten sowie das Windows-Verzeichnis %SystemRoot% (in der Regel C:\WINNT) für administrative Zugriffe freigibt. Die Zugriffsrechte auf diese speziellen Freigaben sind nicht veränderbar und auf die Benutzergruppe „Administratoren“ eingeschränkt. Diese Freigaben sind nicht direkt sichtbar, da sie Freigabenamen der Form „Plattenname$“, also z.B. „C$“ bzw. den Namen „ADMIN$“ haben.
Dadurch besteht die Gefahr, daß

- jemand Administratorkennung und Paßwort ausprobieren kann, oder
- ein Administrator jederzeit unbemerkt auf Benutzerrechner zugreifen kann.

Falls diese Eigenschaft zur Erleichterung der Workstation-Betreuung gewünscht ist, ist zu überlegen, ob ein Adminstrator für alle von ihm betreuten Workstations dasselbe Administrator-Paßwort verwenden soll. Dies läßt sich zwar leichter merken, führt aber dazu, daß ein Angreifer auf alle Workstations zugreifen kann, wenn er dieses eine Paßwort herausgefunden hat.

Falls diese Zugriffsmöglichkeit nicht gewünscht sind, z.B. weil der Administrator nicht auf lokale Benutzerdaten zugreifen können soll, sollte über den Benutzer-Manager, unter Richtlinien - Benutzerrechte das Recht „Zugriff auf diesen Computer vom Netz“ für Administratoren gesperrt werden.

M 2.95 Beschaffung geeigneter Schutzschränke
Schutzschränke können ihren Inhalt gegen die Einwirkung von Feuer bzw. gegen unbefugten

Zugriff schützen. Je nach angestrebter Schutzwirkung sind bei der Auswahl geeigneter Schutzschränke folgende Hinweise zu beachten:

- Schutz gegen Feuereinwirkung:
  Bei Schutzschränken unterscheidet man bezüglich Schutz gegen Feuereinwirkung die Güteklassen S60 und S120 nach VDMA 24991 Teil 1. In diesen Güteklassen werden die Schutzschränke darauf geprüft, ob in ihnen bis zu einer Beflammungszeit von 60 bzw. 120 Minuten während eines normierten Testes für die geschützten Datenträger verträgliche Temperaturen erhalten bleiben. Durch Zusätze in der Klassifizierung werden die zu schützenden Datenträger bezeichnet. Die Kürzel bedeuten im einzelnen:
  P = Papier aller Art
  D = Datenträger (z.B. Magnetbänder, Filme)
  DIS = Disketten, Magnetbandkassetten einschließlich aller anderen Datenträger.
  Die Unterschiede zwischen den Klassen liegen in der Isolationsleistung, die bei DIS-Schränken am höchsten ist.
  Für den IT-Grundschutz sollten bei Schutz gegen Feuer Schutzschränke der Güteklasse aS60 ausreichend sein. Zu beachten bleibt, daß Serverschränke damit ein Schutz gegen Feuer für einen gewissen Zeitraum bieten, so daß Datenträger nicht zerstört werden, jedoch ist im Brandfall davon auszugehen, daß der Betrieb des Servers nicht aufrechterhalten werden kann.
  Bei Schutzschränken, die zum Schutz vor Feuer und Rauch dienen, sollte eine Vorrichtung zum automatischen Schließen der Türen im Brandfall vorgesehen werden. Die Schließung sollte lokal durch Rauchgasmelder und/oder extern durch ein Signal einer Brandmeldeanlage (soweit vorhanden) ausgelöst werden können.

- Schutz gegen unbefugten Zugriff:
  Der Schutzwert gegen unbefugten Zugriff wird neben der mechanischen Festigkeit des Schutzschrankes entscheidend durch die Güte des Schlosses beeinflußt. Für den IT-Grundschutz sollten Wertschränke nach RAL-RG 627 geeignet sein.
  Sind Zugriffsschutz und Brandschutz in Kombination erforderlich, so können Datensicherungsschränke nach RAL-RG 626/9 verwendet werden.

Weitere relevante Normen und Informationen sind VDMA 24992 für Stahlschränke und RAL-RG 627 für Wertschränke. Hilfestellung bei der Bewertung des Widerstandswertes verschiedener Schutzschränke gibt das VDMA-Einheitsblatt 24990, in dem Sicherheitsmerkmale von Schutzschränken kurz beschrieben werden.

Bei der Auswahl von Schutzschränken ist auch die zulässige Deckenbelastung am Aufstellungsort zu berücksichtigen. Nach diesen Auswahlkriterien für den Schutzwert des Schutzschrankes ist als nächstes die Ausstattung des Schrankes bedarfsgerecht festzulegen. Dazu sollte vor der Beschaffung eines Schutzschrankes festgelegt werden, welche Geräte bzw. welche Arten von Datenträgern in ihm aufbewahrt werden sollen. Die Innenausstattung des Schutzschrankes ist dieser Festlegung angemessen auszuwählen. Nachrüstungen sind in der Regel schwierig, da der Schutzwert des Schrankes und seine spezifische Zulassung beeinträchtigt werden können. Es

sollte auch Raum für zukünftige Erweiterungen mit eingeplant werden.

In Serverschränken sollte außer für den Server und eine Tastatur auch Platz für einen Bildschirm und weitere Peripheriegeräte wie z.B. Bandlaufwerke vorgesehen werden, damit Administrationsarbeiten vor Ort durchgeführt werden können. Dazu ist zu beachten, daß die Ausstattung ergonomisch gewählt ist, damit Administrationsarbeiten am Server ungehindert durchgeführt werden können. So ist zum Beispiel ein ausziehbarer Boden für die Tastatur wünschenswert, der in einer Höhe angebracht wird, daß der Administrator seine Arbeiten sitzend durchführen kann. Je nach Nutzung des Schrankes können auch eine Klimatisierung und/oder eine USV-Versorgung erforderlich sein. Die entsprechenden Geräte sollten dann im Schrank mit untergebracht werden. Andernfalls muß zumindest eine Lüftung vorhanden sein. Die Ausstattung des Schrankes mit einem lokal arbeitenden Brandfrüherkennungssystem, das im Brandfall die Stromzufuhr der Geräte unterbricht (auf der Eingangs- und der Ausgangsseite der USV, sofern diese vorhanden ist), ist empfehlenswert.

Nicht im gleichen Schrank untergebracht werden sollten Backup-Datenträger und Protokolldrucker. Backup-Datenträger würden im Falle einer Beschädigung des Servers vermutlich ebenfalls beschädigt. Die Protokollierung der Aktionen am Server dient auch zur Kontrolle des Administrators. Es ist also nicht sinnvoll, ihm, ggf. sogar als Einzigem, Zugriff auf die Protokollausdrucke zu gewähren.

M 2.96 Verschluß von Schutzschränken
Generell sind Schutzschränke bei Nichtbenutzung zu verschließen. Werden Arbeiten, die ein Öffnen des Schutzschrankes erfordern, unterbrochen, so ist auch bei kurzfristigem Verlassen des Raumes der Schutzschrank zu verschließen. Bei Verwendung von Codeschlössern sind diese jedesmal zu verwerfen.

M 2.97 Korrekter Umgang mit Codeschlössern
Werden Schutzschränke mit mechanischen oder elektronischen Codeschlössern verwendet, so muß der Code für diese Schlösser geändert werden:

- nach der Beschaffung,
- bei Wechsel des Benutzers,
- nach Öffnung in Abwesenheit des Benutzers,
- wenn der Verdacht besteht, daß der Code einem Unbefugten bekannt wurde und
- mindestens einmal alle zwölf Monate.

Der Code darf nicht aus leicht zu ermittelnden Zahlen (z.B. persönliche Daten, arithmetische Reihen) bestehen. Die jeweils gültigen Codes von Codeschlössern sind aufzuzeichnen und gesichert zu hinterlegen (vgl. M 2.22 - Hinterlegen des Paßwortes in analoger Anwendung). Zu

beachten ist, daß eine Hinterlegung im zugehörigen Schutzschrank sinnlos ist.

Wenn der Schutzschrank neben einem Codeschloß ein weiteres Schloß besitzt, so ist abzuwägen, ob Code und Schlüssel gemeinsam hinterlegt werden, was im Notfall einen schnelleren Zugriff erlauben würde, oder getrennt hinterlegt werden, so daß es für einen Angreifer schwieriger ist, sich Zugriff zu verschaffen.

M 2.103 Einrichten von Benutzerprofilen unter Windows 95

Unter Windows 95 besteht die Möglichkeit, durch Einrichten von Benutzerprofilen eine Benutzertrennung durchzuführen. Diese Trennung dient jedoch (wenn nicht durch Systemrichtlinien eine Einschränkung erfolgt, vgl. M 2.104 - Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95) ausschließlich dazu, benutzerspezifische Einstellungen zu konservieren und damit für den jeweiligen Benutzer eine individuelle Arbeitsumgebung zu erhalten, die er nach seinen Bedürfnissen und Erfordernissen anpassen kann. Ein Windows 95-Anmeldepaßwort wird erst nach Aktivieren der Benutzerprofile obligatorisch. Für dieses Paßwort gelten im übrigen dieselben Überlegungen wie für WfW-Anmeldepaßwörter (vgl. M 4.46 - Nutzung des Anmeldepaßwortes unter WfW und Windows 95).
Die den Benutzer betreffenden Einstellungen werden in einem Verzeichnis
C:\WINDOWS\PROFILES\Benutzername gespeichert.
Benutzerprofile sollten auf einem nicht vernetzten Windows 95-Rechner immer dann aktiviert werden, wenn unerfahrenen Benutzern das Navigieren unter Windows 95 erleichtert werden soll. Dies ist ebenfalls sinnvoll, wenn eine Benutzertrennung, wenn auch nicht unter Sicherheitsgesichtspunkten, so doch aus organisatorischen oder prinzipiellen Gründen gewünscht wird.
Dazu öffnet man die Programmgruppe SYSTEMSTEUERUNG, dann die Schaltfläche Kennwörter und kann anschließend die Benutzerprofile aktivieren bzw. deaktivieren.

Hinweis: In Novell Netware- oder Windows NT-Netzen können verpflichtende Benutzerprofile angelegt werden, indem das entsprechende Profil in einem dem Benutzer zugeordneten Netzverzeichnis zugriffsgeschützt gespeichert wird. Dieses Profil hat den Namen USER.MAN und wird bei jeder Anmeldung am Server automatisch geladen (vgl. M 4.51 - Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT).

M 2.104 Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95

Soll unerfahrenen Benutzern das Navigieren unter Windows 95 erleichtert werden oder ist aus betrieblicher Sicht die Einschränkung bestimmter Ressourcen notwendig, so kann unter Windows 95 mit sogenannten Systemrichtlinien die Benutzerumgebung benutzerspezifisch mit bestimmten Restriktionen versehen werden. Jedoch sollte berücksichtigt werden, daß Benutzer gegenüber dem IT-System möglicherweise eine abweisende Haltung einnehmen, wenn Einschränkungen nicht unmittelbar einsichtig sind. Eine Einschränkung sollte also nur dann erfolgen, wenn sie tatsächlich notwendig ist oder wenn sie vom Benutzer nicht bemerkt wird. Sobald Systemrichtlinien aktiviert sind, wird beim Starten von Windows 95 überprüft, ob benutzerspezifische Einschränkungen für den aktuellen Benutzer eingerichtet wurden. Ist dies der Fall, werden diese geladen. Ist dies nicht der Fall, werden die Einschränkungen für den Standardbenutzer

herangezogen. Im folgenden werden zunächst die prinzipiellen Einschränkungen beschrieben, die mit den Systemrichtlinien eingestellt werden können. Anschließend wird aufgezeigt, wie diese mittels des Systemrichtlinieneditors (POLEDIT.EXE) angelegt und aktiviert werden können.

Die wesentlichen mit Systemrichtlinien einzustellenden Restriktionen für einen nicht vernetzten Windows 95-Rechner sind:

- Der Zugriff auf die Systemsteuerung kann bezüglich der Optionen Anzeige, Netzwerk, Kennwörter, Druckereinstellungen und System eingeschränkt werden. Die jeweiligen Optionen können zum Teil vollständig deaktiviert oder auf einzelne Registerkarten beschränkt werden.
  Wesentlich bei diesen Optionen sind folgende Punkte:
  - Es können Vorgaben für Bildschirmfarben unter Ergonomiegesichtspunkten gemacht werden.
  - Es kann vorgesehen werden, eigene Kennwörter durch den Benutzer ändern zu lassen.
  - Druckerkonfiguration und Hardware-Einstellungen lassen sich fest vorgeben.
- Der Zugriff auf einzelne Funktionen der Benutzeroberfläche kann eingeschränkt werden. Beispielsweise können die Befehle Ausführen, Suchen und Beenden entfernt werden. Damit wird zum Beispiel verhindert, daß Benutzer nach sicherheitsrelevanten Dateien oder Programmen suchen und diese dann ggf. ausführen. Die Laufwerke lassen sich aus dem Arbeitsplatz und für den Explorer (dem früheren Dateimanager) ausblenden. Partitionen (Laufwerke) können dann ggf. nur noch aus Anwendungen heraus gewechselt werden, da standardmäßig nur die Start-Partition (z.B. C:\) zur Verfügung steht.
- Der Programmstart von ausführbaren Dateien kann eingeschränkt und die DOS-Eingabeaufforderung deaktiviert werden. Die für den einzelnen Benutzer erlaubten Anwendungen lassen sich explizit vorgeben (z.B. Winword.exe, Excel.exe und Explorer.exe) Zusätzlich kann für den Rechner gefordert werden, daß die Windows 95-Anmeldekennwörter sowohl aus Buchstaben als auch aus Sonderzeichen oder Zahlen bestehen müssen und welche Mindestlänge sie aufweisen sollen. Programme, die beim Systemstart ausgeführt werden sollen, lassen sich ebenfalls vorgeben.

Im folgenden wird in einzelnen Schritten gezeigt, wie Systemrichtlinien angelegt und aktiviert werden können und welche Restriktionen für einen nicht vernetzten Windows 95-Rechner Sicherheit bieten:

1. Anlegen einer Systemrichtliniendatei
   Mit Hilfe des Systemrichtlinieneditors wird eine Systemrichtliniendatei erzeugt. Ihr Name ist zwar beliebig, jedoch wird an dieser Stelle der Einfachheit halber der Name CONFIG.POL gewählt. Dazu wird das Programm POLEDIT.EXE aufgerufen, eine neue Datei angelegt und diese unter dem Namen CONFIG.POL abgespeichert. Diese Datei enthält automatisch Einträge für den Standardbenutzer und den Standardcomputer, die im nächsten Schritt ggf. einzuschränken sind. Für den Administrator sind ebenfalls Einträge für

den Computer und den Benutzer anzulegen (im Menü Bearbeiten mit Benutzer hinzufügen und Computer hinzufügen), die im dritten Schritt zu spezifizieren sind.

2. Definition einer Richtlinie für den Standardbenutzer und Standardcomputer
Öffnet man mit dem Systemrichtlinieneditor die Einstellungen für den Standardbenutzer, so kann man menügeführt die entsprechenden sicherheitsrelevanten Einträge vornehmen.

Für einen Standardbenutzer sollten folgende Restriktionen eingestellt werden:
SYSTEMSTEUERUNG

- Der Zugriff auf die Registerkarte Bildschirmschoner sollte dann deaktiviert werden, wenn der Benutzer die Bildschirmsperre nicht deaktivieren können soll. In diesem Fall ist ihm allerdings die Möglichkeit zu geben, das Bildschirmpaßwort zu ändern. Dazu darf die Systemsteuerung (s.u.) nicht vollständig und bei der Option Kennwörter die Registerkarte Kennwort ändern nicht deaktiviert sein.
- Damit der Benutzer die Systemrichtlinien nicht deaktivieren kann, ist zwingend die Registerkarte Benutzerprofile für die Systemsteuerungsoption Kennwörter auszublenden.
- Die Einstellungen für die Hardware-Konfiguration sind vorzunehmen und der Zugriff auf die Register und Schaltflächen für die Systemsteuerungsoption System maximal zu beschränken, damit fehlerhafte Konfigurationen durch den Benutzer vermieden werden, die die Verfügbarkeit oder Leistungsfähigkeit des Rechners einschränken können.

SHELL-ZUGRIFFSBESCHRÄNKUNGEN

- Der Befehl Ausführen sollte deaktiviert werden, wenn verhindert werden soll, daß bestimmte Programme unter Angaben von Optionen gestartet werden können.
- Die System- und Druckersteuerung kann vollständig deaktiviert werden, wenn man die Option Ordner unter „Einstellungen“ im Menü „Start“ entfernen aktiviert. Dies ist immer dann notwendig, wenn dem Benutzer jegliche Möglichkeit genommen werden soll, System- oder Druckereinstellungen zu ändern. Damit der Benutzer sein Bildschirmpaßwort ändern kann, ist unter der Systemsteuerungsoption Anzeige die Registerkarte Bildschirmschoner (s.o.) freizugeben. Der Benutzer kann dann durch Klicken mit der rechten Maustaste auf den Desktop über Eigenschaften auf die Bildschirmsperre zugreifen.
- Soll die Benutzung des Explorers nicht erlaubt sein, so ist die Option Laufwerke im Fenster „Arbeitsplatz“ ausblenden zu aktivieren, da der Explorer über den Arbeitsplatz gestartet werden kann, selbst wenn die Nutzung explizit verboten wurde.

SYSTEM-ZUGRIFFSBESCHRÄNKUNGEN

- Die Option Programme zum Bearbeiten der Registrierung deaktivieren ist zu wählen. Hinweis: Diese Option betrifft nur den Registrierungseditor (REGEDIT.EXE). Mit

dem Systemrichtlinien-Editor (POLEDIT.EXE) läßt sich die lokale Registrierung nach wie vor bearbeiten. Dieses Programm sollte daher von der Festplatte gelöscht werden.

- Es sollten nur zugelassene Anwendungen ausführbar sein.
  Es sind diejenigen Anwendungen, wie etwa WINWORD.EXE, ACCESS.EXE, EXPLORER.EXE, einzutragen, die der Benutzer ausführen können soll.
- Die MS-DOS-Eingabeaufforderung ist zu deaktivieren.
- Ggf. sind Single-Mode-Anwendungen für MS-DOS zu deaktivieren.
  Falls einige DOS-Anwendungen unter Windows 95 aufgerufen werden sollen, der Benutzer aber nicht auf die DOS-Ebene gelangen soll, ist die DOS-Eingabeaufforderung zu aktivieren, jedoch sind bei den zugelassene Anwendungen für Windows nur diejenigen zu nennen, die benötigt werden. Die command.com darf dann dort nicht genannt werden.

Für einen Standardcomputer sollten folgende Restriktionen eingestellt werden:

NETZWERK

- Unter Kennwörter ist ein alphanumerisches Windows-Anmeldekennwort und eine Mindestlänge von sechs Zeichen zu fordern.
- Unter Update ist Remote-Update nicht zu deaktivieren, da sonst die Systemrichtlininen nicht geladen werden.

SYSTEM

- Die Benutzerprofile sind zu aktivieren.

3. Definition einer Richtlinie für den Administrator In einer Richtlinie für den Administrator sollten keine der obigen Restriktionen gesetzt werden. Hierfür ist ein eigener Benutzer unter Windows 95 sowie ein Benutzer und Computer mittels Systemrichtlinien einzurichten, da sonst für ihn die über den Standardbenutzer eingestellten Einschränkungen gelten. Das dazugehörige Paßwort darf nur dem Administrator und seinem Vertreter bekannt sein.
   Diese Richtlinie ist ebenfalls in der Datei CONFIG.POL abzulegen.

4. Definition von Richtlinien für einzelne Benutzer basierend auf dem Standardbenutzer und Standardcomputer Werden weitere Benutzer benötigt, deren Restriktionen sich von den unter 1. spezifizierten unterscheiden sollen, so sind analog zu 1. diese Richtlinien zusätzlich in der Datei CONFIG.POL einzurichten. Dazu kopiert man das Standardprofil, gibt diesem den Namen des betreffenden Benutzers und stellt die Restriktionen wie unter 1. für diesen Benutzer ein.

5. Aktivieren der Richtlinien Beim Einrichten der Systemrichtlinien durch den Administrator ist besondere Vorsicht und Aufmerksamkeit geboten, da sehr leicht inkonsistente Systemzustände eingestellt werden können, die ein Arbeiten mit dem Rechner verhindern. Das Betriebssystem wäre neu zu installieren. Die Systemrichtlinien sollten also nur dann aktiviert werden, wenn die Richtlinien mit äußerster Sorgfalt definiert wurden.
   Dazu öffnet der Administrator mit dem Systemrichtlinieneditor (POLEDIT.EXE) die lokale Registrierung und setzt dort für den Lokalen Computer unter der Option Netzwerk-Update den Schalter Remote-Update. Als Update-Modus muß Interaktiv gewählt werden. Der Pfad für die oben definierte CONFIG.POL ist ebenfalls anzugeben.
   Die notwendigen Einstellungen können von besonders erfahrenen Administratoren auch mit dem Registrierungseditor (Programm REGEDIT.EXE) vorgenommen werden.
   Darüber hinaus sind in der Programmgruppe Systemsteuerung mit der Schaltfläche Kennwörter die Benutzerprofile zu aktivieren.

M 2.105 Beschaffung von TK-Anlagen
Bei der Beschaffung neuer TK-Anlagen besteht die Möglichkeit, diese von vornherein so auszugestalten, daß im späteren Betrieb mit geringem personellen und organisatorischen Zusatzaufwand ein hohes Maß an Sicherheit erreicht werden kann. Hierfür muß in erster Linie auf

- das Vorhandensein geeigneter Funktionalitäten für die Anlagenadministration,
- ausreichende Protokollmechanismen und Auswerte-Tools sowie
- die Revisionsfähigkeit der TK-Anlage

geachtet werden. Für den Bereich der Bundesbehörden wurden entsprechende Anforderungen vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in Zusammenarbeit mit dem Zentralverband der Elektrotechnik- und Elektronikindustrie (ZVEI) erarbeitet und in der Broschüre

Sicherheitsanforderungen an TK-Anlagen - Empfehlungen für den Bereich der Bundesbehörden -

zusammengefaßt. Diese Empfehlungen sind aus Sicht des BSI auch auf andere Bereich der Verwaltung und der Privatwirtschaft übertragbar.

Die Broschüre befindet sich auf der CD-ROM zum IT-Grundschutzhandbuch: GSHB_98\HILFSM\TK.DO

M 2.106 Auswahl geeigneter ISDN-Karten in der Beschaffung
Bei der Beschaffung von ISDN-Karten besteht die Möglichkeit, diese von vornherein so auszuwählen, daß im späteren Betrieb Sicherheitsfunktionalitäten nicht teuer hinzugekauft werden müssen. Erforderliche Sicherheitsfunktionalitäten sollten bereits auf der Karte vorhanden sein oder durch mitgelieferte Kommunikationssoftware und Treiberprogramme realisiert werden können.

Mögliche Kriterien für die Auswahl geeigneter ISDN-Karten sind:

- Fähigkeit zur Durchführung einer Authentisierung über PAP und CHAP (Password Authentikation Protocol und Challenge Handshake Authentication Protocol, RFC 1994),
- Vorhandensein eines Verschlüsselungsverfahrens (symmetrisch/asymmetrisch) in Hard- oder Software,
- Möglichkeit der Auswertung von CLIP-Rufnummern (Calling Line Identification Presentation) zur Authentisierung,
- Möglichkeit des Führens einer Rufnummerntabelle für das Durchführen eines Callbacks,
- Möglichkeit der Protokollierung nicht erfolgreicher Verbindungsaufbauten (Ablehnung aufgrund falscher Rufnummern- oder PAP/CHAP-Authentisierung).

Außerdem sind die ISDN-Karten auf Funktionalitäten hin zu untersuchen, die für einen sicheren Betrieb nicht vorhanden sein dürfen, oder falls sie dennoch vorhanden sind, zumindest durch Konfiguration eine Deaktivierung herbeigeführt werden kann. Hierzu zählt z.B. die „Remote-Control"-Funktionalität, die einen direkten Kommunikationsaufbau zum IT-System aus dem öffentlichen Netz zuläßt.

Beachtet werden sollte, daß sowohl im Bereich der IT-Systeme, die mit ISDN-Karten ausgestattet werden sollen, als auch im Bereich der Netzkoppelelemente (z.B. ISDN-Router) ISDN-Karten mit möglichst gleichen Sicherheitsfunktionalitäten eingesetzt werden. Ist dies nicht gewährleistet, entfalten Sicherheitsfunktionalitäten, die auf beiden Seiten erforderlich sind, nicht die gewünschte Wirkung.

M 2.107 Dokumentation der ISDN-Karten-Konfiguration
Je nach Einsatzgebiet ergeben sich für eine ISDN-Karte nahezu beliebig komplexe Konfigurationseinstellungen. Für das Sicherstellen eines geordneten Wiederanlaufs (z.B. nach Austausch einer ISDN-Karte oder deren Kommunikationssoftware) wird empfohlen, mindestens die folgenden Einstellungen zu dokumentieren:

- Typenbezeichnung der eingesetzten Karte und Seriennummer,
- Rufnummer(n) für den Kommunikationsaufbau und eine evtl. durchzuführende Authentisierung,
- Verwendetes D-Kanal-Protokoll (1TR6, EDSS-1 etc.),
- Verwendetes B-Kanal-Protokoll (X.25, PPP, TCP/IP, Bittransparent etc.),
- Stand der verwendeten CAPI-Version,
- Stand der verwendeten Treiber-Software,
- Art der Datenkompression, wenn verwendet,
- Art der Authentisierung (z.B. PAP/CHAP), wenn verwendet.

Beim Einsatz von Authentisierungsverfahren, die auf dem Besitz eines gemeinsamen Geheimnisses (z.B. Paßwort) beruhen, kann auch dieses Geheimnis dokumentiert werden. Beachtet werden muß dann allerdings, daß die erstellte Dokumentation nur einem eingeschränkten Personenkreis zugänglich gemacht werden darf, um das Bekanntwerden des Geheimnisses zu verhindern.

M 2.108 Verzicht auf Fernwartung der ISDN-Netzkoppelelemente

Der Verzicht auf Fernwartung ist eine wirkungsvolle Maßnahme, um Externe an Manipulationen an ISDN-Routern und IT-Systemen mit ISDN-Karten zu hindern.

Bei IT-Systemen mit ISDN-Karte sollte überprüft werden, ob die verwendete Kommunikationssoftware „Remote-Control"-Funktionalitäten bietet. Hierdurch kann das betreffende IT-System über das öffentliche ISDN angerufen werden, die ISDN-Karte nimmt den Anruf entgegen und der Anrufende bedient das IT-System so, als ob es „vor Ort" wäre. Diese Funktionalität ist zu deaktivieren.

Bei ISDN-Routern sollte die Fernwartung über reservierte Bandbreiten (oder reservierte ISDN-Rufnummern) deaktiviert werden, da hier i.d.R. eine nur über ein Paßwort geschützte Verbindung zur Management Information Base des Routers hergestellt wird, in der nahezu alle Konfigurationseinstellungen vorgenommen werden können.

M 2.109 Rechtevergabe für den Fernzugriff

Der externe Zugriff auf ein Unternehmensnetz muß hinsichtlich der eingeräumten Rechte auf das erforderlich Maß eingeschränkt werden. Über die in M 2.8 - Vergabe von Zugriffsrechten beschriebenen Anforderungen ist weiterhin zu berücksichtigen, daß die Rechtevergabe für den Fernzugriff noch restriktiver zu handhaben ist.

Beispielsweise müssen für einen Telearbeitsplatz nicht zwingend Zugriffsrechte auf Verzeichnisse mit Software bestehen (siehe G 5.62 - Mißbrauch von Ressourcen über abgesetzte IT-Systeme).

M 2.110 Datenschutzaspekte bei der Protokollierung

Unter Protokollierung beim Betrieb von IT-Systemen ist im datenschutzrechtlichen Sinn die Erstellung von manuellen oder automatisierten Aufzeichnungen zu verstehen, aus denen sich die Fragen beantworten lassen: „Wer hat wann mit welchen Mitteln was veranlaßt bzw. worauf zugegriffen?" Außerdem müssen sich Systemzustände ableiten lassen: „Wer hatte von wann bis wann welche Zugriffsrechte?"

Art und Umfang von Protokollierungen hängen vom allgemeinen Datenschutzrecht und auch von bereichsspezifischen Regelungen ab.

Die Protokollierung der Administrationsaktivitäten entspricht einer Systemüberwachung, während die Protokollierung der Benutzeraktivitäten im wesentlichen der Verfahrensüberwachung dient. Dementsprechend finden sich die Anforderungen an die Art und den Umfang der systemorientierten Protokollierung überwiegend im allgemeinen Datenschutzrecht, während die verfahrensorientierte Protokollierung oft durch bereichsspezifische Regelungen definiert wird. Beispiele für verfahrensorientierte Protokollierung sind u.a. Meldegesetze, Polizeigesetze, Verfassungsschutzgesetze.

Mindestanforderungen an die Protokollierung
Bei der Administration von IT-Systemen sind die folgenden Aktivitäten vollständig zu protokollieren:

- Systemgenerierung und Modifikation von Systemparametern
  Da auf dieser Ebene in der Regel keine systemgesteuerten Protokolle erzeugt werden, bedarf es entsprechender detaillierter manueller Aufzeichnungen, die mit der Systemdokumentation korrespondieren sollten.

- Einrichten von Benutzern
  Wem von wann bis wann durch wen das Recht eingeräumt worden ist, das betreffende IT-System zu benutzen, ist vollständig zu protokollieren. Für diese Protokolle sollten längerfristige Aufbewahrungszeiträume vorgesehen werden, da sie Grundlage praktisch jeder Revisionsmaßnahme sind.

- Erstellung von Rechteprofilen
  Im Rahmen der Protokollierung der Benutzerverwaltung kommt es insbesondere auch darauf an aufzuzeichnen, wer die Anweisung zur Einrichtung bestimmter Benutzerrechte erteilt hat (siehe auch M 2.31 - Dokumentation der zugelassenen Benutzer und Rechteprofile)

- Einspielen und Änderung von Anwendungssoftware
  Die Protokolle repräsentieren das Ergebnis der Programm- und Verfahrensfreigaben.

- Änderungen an der Dateiorganisation
  Im Hinblick auf die vielfältigen Manipulationsmöglichkeiten, die sich bereits bei Benutzung der „Standard-Dateiverwaltungssysteme“ ergeben, kommt einer vollständigen Protokollierung eine besondere Bedeutung zu (vgl. z.B. Datenbankmanagement).

- Durchführung von Datensicherungsmaßnahmen
  Da derartige Maßnahmen (Backup, Restore) mit der Anfertigung von Kopien bzw. dem Überschreiben von Datenbeständen verbunden sind und häufig in „Ausnahmesituationen“ durchgeführt werden, besteht eine erhöhte Notwendigkeit zur Protokollierung.

- Sonstiger Aufruf von Administrations-Tools
  Die Benutzung aller Administrations-Tools ist zu dokumentieren, um feststellen zu können, ob Unbefugte sich Systemadministrator-Rechte erschlichen haben.

- Versuche unbefugten Einloggens und Überschreitung von Befugnissen
  Geht man von einer wirksamen Authentisierungsprozedur und sachgerechten Befugniszuweisungen aus, kommt der vollständigen Protokollierung aller „auffälligen Abnormalitäten“ beim Einloggen und der Benutzung von Hard- und Softwarekomponenten eine zentrale Bedeutung zu. Benutzer in diesem Sinne ist auch der Systemadministrator.

Bei der Verarbeitung von personenbezogenen Daten sind folgende Benutzeraktivitäten in Abhängigkeit von der Sensibilität der Verfahren bzw. Daten vollständig bzw. selektiv zu protokollieren:

- Eingabe von Daten
  Die sogenannte Eingabekontrolle erfolgt grundsätzlich verfahrensorientiert (z.B. Protokollierung in Akten, soweit vorhanden, Protokollierung direkt im Datenbestand, sofern keine Akten geführt werden). Auch wenn man davon ausgeht, daß Befugnisüberschreitungen anderweitig protokolliert werden, dürfte eine vollständige Protokollierung von Dateneingaben als Regelfall angesehen werden müssen.

- Datenübermittlungen
  Nur soweit nicht gesetzlich eine vollständige Protokollierung vorgeschrieben ist, kann eine selektive Protokollierung als ausreichend angesehen werden.

- Benutzung von automatisierten Abrufverfahren
  In der Regel dürfte eine vollständige Protokollierung der Abrufe und der Gründe der Abrufe (Vorgang, Aktenzeichen etc.) erforderlich sein, um unbefugte Kenntnisnahme im Rahmen der grundsätzlich eingeräumten Zugriffsrechte aufdecken zu können.

- Löschung von Daten
  Die Durchführung der Löschung ist zu protokollieren.

- Aufruf von Programmen
  Dies kann erforderlich sein bei besonders „sensiblen“ Programmen, die z.B. nur zu bestimmten Zeiten oder Anlässen benutzt werden dürfen. Deshalb ist in diesen Fällen eine vollständige Protokollierung angezeigt. Die Protokollierung dient auch der Entlastung der befugten Benutzer (Nachweis des ausschließlich befugten Aufrufs der Programme).

Zweckbindung bei der Nutzung von Protokolldaten
Protokolldaten unterliegen aufgrund der nahezu übereinstimmenden Regelungen im Datenschutzrecht des Bundes und der Länder einer besonderen engen Zweckbindung (z.B. § 14 Abs. 4 und § 31 BDSG, § 13 Abs. 5 HDSG). Sie dürfen nur zu den Zwecken genutzt werden, die Anlaß für ihre Speicherung waren. Dies sind in der Regel die in einem Sicherheitskonzept festgelegten allgemeinen Kontrollen, die in den meisten Datenschutzgesetzen geforderte "Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme, mit denen personenbezogene Daten verarbeitet werden"(vgl. z.B. § 18 Abs. 2 BDSG, § 8 Abs. 3 LDSG-SH) und die Kontrollen durch interne oder externe Datenschutzbeauftragte. Nur in Ausnahmefällen lassen die bereichsspezifischen Regelungen die Nutzung dieser Daten für andere Zwecke, z.B. zur Strafverfolgung, zu.

Aufbewahrungsdauer
Soweit nicht bereichsspezifische Regelungen etwas anderes vorsehen, richtet sich die Aufbewahrungsdauer der Protokolle nach den allgemeinen Löschungsregeln der Datenschutzgesetze. Maßstab ist die „Erforderlichkeit zur Aufgabenerfüllung“. Gibt es keinen zwingenden Grund für das weitere Vorhalten von Protokolldateien, besteht eine Löschungspflicht (vgl. z. B. § 20 Abs. 2 BDSG).
Als Anhaltspunkte können dienen:

- die Wahrscheinlichkeit, daß Unregelmäßigkeiten (noch) offenbar werden können und
- die Möglichkeit, die Gründe von Unregelmäßigkeiten anhand der Protokolle und anderer Unterlagen aufdecken zu können.

Erfahrungsgemäß sollte eine Frist von einem Jahr nicht überschritten werden.
Soweit Protokolle zum Zwecke gezielter Kontrollen angefertigt werden, kommen kürzere Speicherungsfristen in Betracht. In der Regel reicht eine Aufbewahrung bis zur tatsächlichen Kontrolle aus. Auch hier sind die bereichsspezifischen Vorschriften zu beachten.

Technische und organisatorische Rahmenbedingungen
Die Effektivität der Protokollierung und ihre Auswertung im Rahmen von Kontrollen hängt im entscheidenden Maße von den technischen und organisatorischen Rahmenbedingungen ab. In diesem Zusammenhang sollten folgende Aspekte Berücksichtigung finden:

- Es sollte ein Revisionskonzept erstellt werden, das den Zweck der Protokolle und deren Kontrollen sowie Schutzmechanismen für die Rechte der Mitarbeiter und der sonstigen betroffenen Personen klar definiert.
- Die Zwangsläufigkeit und damit die Vollständigkeit der Protokolle muß ebenso gewährleistet werden wie die Manipulationssicherheit der Einträge in Protokolldateien.
- Entsprechend der Zweckbindung der Datenbestände müssen wirksame Zugriffsbeschränkungen realisiert werden.
- Die Protokolle müssen so gestaltet sein, daß eine effektive Überprüfung möglich ist. Dazu gehört auch eine IT-Unterstützung der Auswertung.
- Die Auswertungsmöglichkeiten sollten vorab abgestimmt und festgelegt sein.
- Kontrollen sollten so zeitnah durchgeführt werden, daß bei aufgedeckten Verstößen noch Schäden abgewendet sowie Konsequenzen gezogen werden können. Kontrollen müssen rechtzeitig vor dem Ablauf von Löschungsfristen von Protokolldateien stattfinden.
- Kontrollen sollten nach dem 4-Augen-Prinzip erfolgen.
- Es sollte vorab definiert werden, welche Konsequenzen sich aus Verstößen ergeben, die durch die Kontrolle von Protokollen aufgedeckt werden.
- Die Mitarbeiter sollten darüber informiert sein, daß Kontrollen durchgeführt werden, ggf. auch unangekündigt.
- Für Routinekontrollen sollten automatisierte Verfahren (z.B. watch dogs) verwendet werden.
- Personal- bzw. Betriebsräte sollten bei der Erarbeitung des Revisionskonzeptes und bei der Festlegung der Auswertungsmöglichkeiten der Protokolle beteiligt werden.

M 2.111 Bereithalten von Handbüchern
Bei der Beschaffung von Informationstechnik, egal ob es sich um Hardware oder Software handelt, müssen die zugehörigen Handbücher und technischen Referenzen in ausreichender Anzahl mitbeschafft werden.
Im Lieferumfang von IT-Produkten ist zunehmend keine weiterführende Dokumentation mehr enthalten, sondern es werden neben Online-Hilfen nur noch Installationshilfen und einführende Texte mitgeliefert. Dieser eingeschränkte Umfang an Dokumentationshilfen ist insbesondere bei auftretenden Fehlern unzureichend. Es ist daher darauf zu achten, daß die erforderlichen Handbücher, technische Referenzen und Fehlerkataloge zusätzlich beschafft werden. Hierbei muß nicht ausschließlich auf die vom Hersteller angebotene Literatur zurückgegriffen werden.
Alle Handbücher zu einem IT-Produkt müssen jederzeit in der Anwendungsumgebung verfügbar sein. Beispielweise müssen die Handbücher zu einem Server-Betriebssystem bei diesem Server aufbewahrt werden, und nicht in einer evtl. geschlossenen Bibliothek. Bei der Notfallplanung ist der Zugriff auf diese Literatur einzuplanen (siehe M 6.3 - Erstellung eines Notfall-Handbuches).

M 2.112 Regelung des Akten- und Datenträgertransports zwischen häuslichem Arbeitsplatz und Institution
Damit der Austausch von Akten und Datenträgern zwischen häuslichem Arbeitsplatz und Institution sicher vollzogen werden kann, ist eine Regelung über Art und Weise des Austauschs aufzustellen. Darin sollten zumindest folgende Punkte betrachtet bzw. geregelt werden:

- welche Akten/Datenträger über welchen Transportweg (Postweg, Kurier, Paketdienst, ...) ausgetauscht werden dürfen (vgl. M 5.23 - Auswahl einer geeigneten Versandart),
- welche Schutzmaßnahmen sind beim Transport zu beachten. Beispiele dazu sind:
  - geschlossener Behälter,
  - Versandtasche,
  - Einschreiben,
  - Wertbrief,
  - Begleitschreiben und
  - Versiegelung.
- welche Akten/Datenträger nur persönlich transportiert werden dürfen.

Da Schriftstücke, Dokumente und Akten oftmals Unikate sind, muß bei der Auswahl eines geeigneten Aktenaustauschverfahrens beachtet werden, welchen Schaden der Verlust bedeuten würde. Hingegen kann beim Datenträgeraustausch vorab eine Datensicherung erfolgen.

M 2.118 Festlegung einer Sicherheitspolitik für E-Mail-Nutzung
Bevor E-Mail-Systeme für die Nutzung freigeben werden, sollte festgelegt werden, für welchen Einsatzzweck E-Mail vorgesehen ist. Abhängig davon, wofür E-Mail eingesetzt werden soll, differieren auch die Ansprüche an Vertraulichkeit, Verfügbarkeit, Integrität und Verbindlichkeit der zu übertragenden Daten sowie des eingesetzten E-Mail-Programms. Es muß geklärt werden, ob über E-Mail ausschließlich unverbindliche oder informelle Informationen weitergegeben

werden sollen oder ob einige oder sogar alle der bisher schriftlich bearbeiteten Geschäftsvorfälle nun per E-Mail durchgeführt werden sollen. Bei letzterem ist zu klären, wie Anmerkungen an Vorgängen wie Verfügungen, Abzeichnungen oder Schlußzeichnungen, die bisher handschriftlich angebracht wurden, elektronisch abgebildet werden sollen.

Die Institution muß eine Sicherheitspolitik festlegen, in der folgende Punkte beschrieben sind:

- wer einen E-Mail-Anschluß erhält,
- die Regelungen, die von den Mail-Administratoren und den E-Mail-Benutzern zu beachten sind,
- bis zu welchem Vertraulichkeits- bzw. Integritätsanspruch Informationen per E-Mail versandt werden dürfen,
- welche Handbücher beschafft werden,
- wie die Benutzer geschult werden und
- wie jederzeit technische Hilfestellung für die Benutzer gewährleistet wird.

Durch organisatorische Regelungen oder durch die technische Umsetzung sind dabei insbesondere die folgenden Punkte zum ordnungsgemäßen Dateitransfer zu gewährleisten:

- Die E-Mail-Progamme der Benutzer müssen durch den Administrator so vorkonfiguriert sein, daß ohne weiteres Zutun der Benutzer maximale Sicherheit erreicht werden kann (siehe auch M 5.57 - Sichere Konfiguration der Mailclients).
- Die Übermittlung von Daten darf erst nach erfolgreicher Identifizierung und Authentisierung des Senders beim Übertragungssystem möglich sein.
- Die Benutzer müssen vor erstmaliger Nutzung von E-Mail in die Handhabung der relevanten Applikationen eingewiesen werden. Die organisationsinternen Benutzerregelungen zu Dateiübermittlung muß ihnen bekannt sein.
- Zur Beschreibung des Absenders werden bei E-Mails sogenannte Signatures (Absenderangaben) an das Ende der E-Mail angefügt. Der Inhalt einer Signature sollte dem eines Briefkopfs ähneln, also Name, Organisationsbezeichnung und Telefonnummer u.ä. enthalten. Eine Signature sollte nicht zu umfangreich sein, da dies nur unnötig Übertragungszeit und Speicherplatz kostet. Die Behörde bzw. das Unternehmen sollte einen Standard für die einheitliche Gestaltung von Signatures festlegen.
- Von den eingesetzten Sicherheitsmechanismen hängt es ab, bis zu welchem Vertraulichkeits- bzw. Integritätsanspruch Dateien per E-Mail versandt werden dürfen. Es sollte geregelt werden, ob und wann übertragene Dateien verschlüsselt bzw. digital signiert werden müssen (siehe auch M 4.34 - Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen). Es ist zentral festzulegen, welche Applikationen für die Verschlüsselung

bzw. den Einsatz von Digitalen Signaturen von den Benutzern zu verwenden sind. Diese müssen den Benutzern zur Verfügung gestellt werden, die wiederum in deren Anwendung unterwiesen werden müssen.

- Es sollte vor der Einführung elektronischer Kommunikationssysteme festgelegt werden, unter welchen Bedingungen ein- oder ausgehende E-Mails zusätzlich ausgedruckt werden müssen.
- Die Dateiübertragung kann (optional) dokumentiert werden. Für jede stattgefundene Übermittlung ist dann in einem Protokoll festzuhalten, wer wann welche Informationen erhalten hat. Bei der Übertragung personenbezogener Daten sind die gesetzlichen Vorgaben zur Protokollierung zu beachten.

E-Mails, die intern versandt werden, dürfen das interne Netz nicht verlassen. Dies ist durch die entsprechenden administrativen Maßnahmen sicherzustellen. Beispielsweise sollte die Übertragung von E-Mails zwischen verschiedenen Liegenschaften einer Organisation über eigene Standleitungen und nicht über das Internet erfolgen.
Grundsätzlich sollten Nachrichten, die an interne Adressen verschickt wurden, nicht an externe Adressen weitergeleitet werden. Sollen hiervon Ausnahmen gemacht werden, sind alle Mitarbeiter darüber zu informieren. Beispielsweise kann für Außendienstmitarbeiter oder andere Mitarbeiter, die viel unterwegs sind, die E-Mails an externe Zugriffspunkte weitergeleitet werden.

M 2.119 Regelung für den Einsatz von E-Mail
Sollen zwischen zwei oder mehreren Kommunikationspartnern Daten elektronisch ausgetauscht werden, so müssen diese zum ordnungsgemäßen Austausch folgende Punkte beachten:

- Die Adressierung von E-Mail muß eindeutig erfolgen, um eine fehlerhafte Zustellung zu vermeiden. Innerhalb einer Organisation sollten Adressbücher und Verteilerlisten gepflegt werden, um die Korrektheit der gebräuchlichsten Adressen sicherzustellen. Durch den Versand von Testnachrichten an neue E-Mail-Adressen ist die korrekte Zustellung von Nachrichten zu prüfen.
- Für alle nach außen gehenden E-Mails ist eine Signature zu verwenden.
- Die Betreffangabe (Subject) des Kommunikationssystems sollte immer ausgefüllt werden, z.B. entsprechend der Betreffangabe in einem Anschreiben.
- Die Korrektheit der durchgeführten Datenübertragung sollte überprüft werden. Die Empfängerseite sollte den korrekten Empfang überprüfen und der Senderseite bestätigen.
- Verwendung residenter Virenscanner für ein- bzw. ausgehende Dateien. Vor dem Absenden bzw. vor der Dateiübermittlung sind die ausgehenden Dateien explizit auf Computer-Viren zu überprüfen.
- Erfolgt über die E-Mail noch eine Dateiübertragung, so sollten die folgenden Informationen an den Empfänger zusätzlich übermittelt werden:

- Art der Datei (z.B. Word Perfect 5.0),
- Kurzbeschreibung für den Inhalt der Datei,
- Hinweis, daß Dateien auf Computer-Viren überprüft sind,
- ggf. Art des verwendeten Packprogramms (z.B. PKZIP)
- ggf. Art der eingesetzten Software für Verschlüsselung bzw. Digitale Signatur.

Jedoch sollte nicht vermerkt werden,

- welches Paßwort für die eventuell geschützten Informationen vergeben wurde,
- welche Schlüssel ggf. für eine Verschlüsselung der Informationen verwendet wurde.

Bei den meisten E-Mail-Systemen werden die Informationen unverschlüsselt über offene Leitungen transportiert und können auf diversen Zwischenrechnern gespeichert werden, bis sie schließlich ihren Empfänger erreichen. Auf diesem Weg können Informationen leicht manipuliert werden. Aber auch der Versender einer E-Mail hat meistens die Möglichkeit, seine Absenderadresse (From) beliebig einzutragen, so daß man sich nur nach Rückfrage oder bei Benutzung von Digitalen Signaturen der Authentizität des Absenders sicher sein kann. In Zweifelsfällen sollte daher die Echtheit des Absenders durch Rückfrage oder - besser noch - durch den Einsatz von Verschlüsselung und/oder Digitalen Signaturen überprüft werden. Grundsätzlich gilt, daß man sich nicht auf die Echtheit der Absenderangabe verlassen kann.

Beim Anschluß an E-Mail-Systeme ist mehrfach täglich zu überprüfen, ob neue E-Mails eingegangen sind. Bei längerer Abwesenheit sollte eine Vertretungsregelung getroffen werden, beispielsweise können eingehende E-Mails an einen Vertreter weitergeleitet werden.

Da in vielen Fällen nicht vorhergesagt werden kann, welchen Mail-Client ein Mail-Empfänger benutzt und welche Software und Betriebssysteme auf dem Transportweg eingesetzt werden, müssen die Benutzer darüber informiert sein, daß sie sowohl für den Nachrichtentext (Mailbody) als auch für Attachments eine 7-Bit-ASCII-Darstellung verwenden sollten. Für den Nachrichtentext sollte daher auf nationale Sonderzeichen wie Umlaute und „ß “ verzichtet werden. Attachments sollten im Zweifelsfall in 7-Bit-ASCII-Darstellung umgewandelt werden, z.B. mit uuencode.

Alle Regelungen und Bedienungshinweise zum Einsatz von E-Mail sind schriftlich zu fixieren und sollten den Mitarbeitern jederzeit zur Verfügung stehen. Ein entsprechendes Muster ist der dem IT-Grundschutzhandbuch beiliegenden CD-ROM zu entnehmen. Die Benutzer müssen vor dem Einsatz von Kommunikationsdiensten wie E-Mail geschult werden, um Fehlbedienungen zu vermeiden und die Einhaltung der organisationsinternen Richtlinien zu gewährleisten. Insbesondere müssen sie hinsichtlich möglicher Gefährdungen und einzuhaltender Sicherheitsmaßnahmen beim Versenden bzw. Empfangen von E-Mail sensibilisiert werden.

Zur Vermeidung von Überlastung durch E-Mail sind die Mitarbeiter über potentielles Fehlverhalten zu belehren. Sie sollten dabei ebenso vor der Teilnahme an E-Mail-Kettenbriefen wie

vor der Abonnierung umfangreicher Mailinglisten gewarnt werden. Benutzer müssen darüber informiert werden, daß Dateien, deren Inhalt Anstoß erregen könnte, weder verschickt noch auf Informationsservern eingestellt werden noch nachgefragt werden sollten. Außerdem sollten Benutzer darauf verpflichtet werden, daß bei der Nutzung von Kommunikationsdiensten

- die fahrlässige oder gar vorsätzliche Unterbrechung des laufenden Betriebes unter allen Umständen vermieden werden muß. Zu unterlassen sind insbesondere Versuche, ohne Autorisierung Zugang zu Netzdiensten - welcher Art auch immer - zu erhalten, Informationen, die über die Netze verfügbar sind, zu verändern, in die individuelle Arbeitsumgebung eines Netznutzers einzugreifen oder unabsichtlich erhaltene Angaben über Rechner und Personen weiterzugeben.

- die Verbreitung von für die Allgemeinheit irrelevanten Informationen unterlassen werden muß. Die Belastung der Netze durch ungezielte und übermäßige Verbreitung von Informationen sollte vermieden werden.

- die Verbreitung von redundanten Informationen vermieden werden sollte.

M 2.120 Einrichtung einer Poststelle
Zum reibungslosen Ablauf des E-Mail-Dienstes muß ein Postmaster benannt werden, der folgende Aufgaben wahrnimmt:

- Bereitstellen der Maildienste auf lokaler Ebene,

- Pflege der Adreßtabellen,

- Überprüfung, ob die externen Kommunikationsverbindungen funktionieren,

- Anlaufstelle bei Mailproblemen für Endbenutzer sowie für die Betreiber von Gateway- und Relaydiensten.

Alle unzustellbaren E-Mails und alle Fehlermeldungen müssen an den Postmaster weitergeleitet werden, der versuchen sollte die Fehlerquellen zu beheben. E-Mail, die unzustellbar bleibt, muß nach Ablauf einer vordefinierten Frist an den Absender mit einer entsprechenden Fehlermeldung zurückgeschickt werden.

Daneben müssen je nach Organisationsstruktur und -größe ein oder mehrere Verantwortliche für die Pflege der angebotenen Kommunikationsdienste benannt werden. Neben dem Serverbetrieb wie Mail-, News- oder FTP-Server müssen auch die von den Benutzer eingesetzten Kommunikationsclients betreut werden.

Alle Betreuer bzw. deren Vertreter sollten jederzeit von den Benutzern telefonisch erreicht werden könnten.

M 2.121 Regelmäßiges Löschen von E-Mails
E-Mails sollten nicht unnötig lange im Posteingang gespeichert werden. Sie sollten entweder nach dem Lesen gelöscht werden oder in Benutzerverzeichnissen gespeichert werden, wenn sie erhalten bleiben sollen. Wenn im Posteingang zu viele E-Mails archiviert werden, kann es passieren, daß das IT-System, das diesen verwaltet (der Mailserver bzw. Mailclient), aus Speicherplatzmangel neu ankommende E-Mails abweist.

Benutzer müssen andererseits darüber informiert sein, daß eine E-Mail, die sie selber über ihre Mailanwendung gelöscht haben, dadurch meistens nicht unwiederbringlich gelöscht ist. Viele Mailprogramme löschen E-Mails nicht sofort, sondern transferieren sie in spezielle Ordner. Benutzer müssen darauf hingewiesen werden, wie sie E-Mails auf ihren Clients vollständig löschen können. Daneben können E-Mails nach dem Löschen auf den Clients trotzdem noch auf Mail-Servern vorhanden sein. Viele Internetprovider und Administratoren archivieren die ein- und ausgehenden E-Mails. Viele Mailanwendungen löschen E-Mails nicht, sondern verschieben sie in einen „Papierkorb"-Bereich, der dann ebenfalls gelöscht werden muß.

Die Benutzer müssen wissen, daß die Vertraulichkeit einer E-Mail nur durch Verschlüsselung gewährleistet werden kann, und daß sie sich nicht auf „schnelles Löschen" nach dem Empfang verlassen können.

M 2.122 Einheitliche E-Mail-Adressen
E-Mail-Adressen sollten aufgrund von klaren Regelungen vergeben werden. Dabei ist es sinnvoll, Namenskonventionen für die personenbezogenen E-Mail-Adressen festzulegen, die an die Benutzernamen auf den verwendeten IT-Systeme angelehnt sind (z.B. E-Mail-Adresse = die ersten 8 Zeichen des Nachnamens). Die Benutzernamen auf IT-Systemen, die von außerhalb des geschützten Netzes erreicht werden können, sollten nicht aus den E-Mail-Adressen unmittelbar ableitbar sein, um mögliche Angriffe auf Benutzer-Accounts zu erschweren. Wichtig ist, daß die Adressen nicht häufig geändert werden und daß sie weder zu lang noch zu kompliziert aufgebaut sind. Insbesondere ist darauf zu achten, daß keine Nicht-ASCII-Zeichen wie Umlaute innerhalb von E-Mail-Adressen verwendet werden.

Um Angriffe zu erschweren, Werbe-E-Mail zu vermeiden bzw. um möglichst wenig Information nach außen weiterzugeben, kann es sinnvoll sein, statt benutzer- und organisationsbezogenen E-Mail-Adressen wie nachname@organisation.de schwer erratbare E-Mail-Adressen zu verwenden. Dies macht aber auch die Adreßweitergabe unbequemer und kann die Kommunikation mit Externen erschweren.

Wenn E-Mail-Adressen geändert werden oder wegfallen, ist darauf zu achten, daß zumindest für eine Übergangszeit E-Mail, die noch an diese Adressen gerichtet ist, an die jetzt aktuellen Adressen weitergeleitet wird.

Neben personenbezogenen E-Mail-Adressen können auch organisations- bzw. funktionsbezogene E-Mail-Adressen eingerichtet werden, um unabhängig von Personen die Zustellung zur

richtigen Organisationseinheit zu garantieren. Dies ist insbesondere bei zentralen Anlaufstellen wichtig.

M 2.123 Auswahl eines Mailproviders
Vor der Auswahl eines Mailproviders sollten sich die Verantwortlichen über die beim Provider geltenden Regelungen informieren, beispielsweise ob er Obergrenzen für den Umfang von E-Mails beim Empfang oder Versand gesetzt hat, ob E-Mails gefiltert werden, und wenn ja, nach welchen Regeln.

Man sollte sich vom Mailprovider dokumentieren lassen, daß deren Mailserver sicher betrieben wird, also die in M 5.56 - Sicherer Betrieb eines Mailservers beschriebenen Anforderungen erfüllt sind.

Beim Mailprovider sind Daten über die Benutzer für Abrechnungszwecke gespeichert (Name, Adresse, Benutzer-Kennung, Bankverbindung) ebenso wie Verbindungsdaten und für eine je nach Provider kürzere oder längere Zeitspanne auch die übertragenen Inhalte.

Die Anwender sollten sich bei ihrem Mailprovider erkundigen, welche Daten wie lange über sie gespeichert werden. Bei der Auswahl von Providern sollte berücksichtigt werden, daß deutsche Betreiber den einschlägigen datenschutzrechtlichen Regelungen für die Verarbeitung dieser Daten unterliegen.

Die Benutzer können durch den Einsatz von Verschlüsselung verhindern, daß der Provider die Inhalte der übertragenen Informationen mitlesen kann.

Große Provider mit großem eigenem Netz haben den Vorteil, daß E-Mail, die nur innerhalb dieses Netzes ausgetauscht wird, sicherer vor Manipulationen ist als bei Weiterleitung über das Internet.

Bei Providern, die ihren Hauptsitz im Ausland haben, wird häufig auch alle E-Mail über dieses Land geroutet. Beispielsweise werden bei AOL und Compuserve alle E-Mails über die USA weitergeleitet. Dieser Punkt sollte berücksichtigt werden, wenn man sich Gedanken darüber macht, über wie viele Gateways die E-Mail weiterverteilt wird, also wer sie beispielsweise mitlesen kann.

M 2.124 Geeignete Auswahl einer Datenbank-Software
Bei der Beschaffung neuer Datenbank-Software besteht die Möglichkeit, diese von vornherein so auszuwählen, daß im späteren Betrieb mit nur geringem personellen und organisatorischen Zusatzaufwand ein hohes Maß an Sicherheit erreicht werden kann. Zu Beginn muß der Einsatzbereich und Verwendungszweck des Datenbanksystems geklärt werden, um die Anforderungen bezüglich der Verfügbarkeit, der Integrität und der Vertraulichkeit formulieren zu können. Weiterhin sind die Anforderungen hinsichtlich der zu verarbeitenden Datenmengen, der Verarbeitungsgeschwindigkeit und des Durchsatzes zu quantifizieren. Daraus leiten sich die zu erfüllenden Eigenschaften für die zu beschaffende Datenbank-Software ab, wie z.B. Verfügbar-

keit für bestimmte Hardware-Plattformen bzw. Betriebssysteme oder Umfang von notwendigen Sicherheitsmechanismen. In diesem Planungsstadium kann bereits erkannt werden, ob und in welchem Maße für den späteren Betrieb des Datenbanksystems Hardware nach- bzw. umgerüstet werden muß. Anhand der Verfügbarkeitsanforderungen sind auch die benötigten Überwachungsmöglichkeiten zu definieren, d.h. es muß festgelegt werden, welche Datenbankzustände in welcher Form erkennbar sein sollen (z.B. durch eine Protokollierung in einer Datei), sowie die Art der Benachrichtigung verantwortlicher Personen bzw. Personengruppen über kritische Zustände der Datenbank (z.B. durch eine Meldung an der Konsole).

Für die Beschaffung einer Datenbank-Software sollten insbesondere die folgenden Punkte berücksichtigt werden:

- Die Datenbank-Software muß über eigene geeignete Mechanismen zur Identifikation und Authentisierung der Benutzer verfügen (siehe M 2.128 - Zugangskontrolle einer Datenbank).
- Die Datenbank-Software muß über geeignete Mechanismen zur Ressourcenbeschränkung verfügen (siehe M 4.73 - Festlegung von Obergrenzen).
- Falls in der Datenbank vertrauliche Daten verwaltet werden sollen, so muß einem unberechtigten Zugriff vorgebeugt werden können. Die zu beschaffende Datenbank-Software muß in diesem Fall entsprechende Zugriffskontrollmechanismen zur Verfügung stellen (siehe M 2.129 - Zugriffskontrolle einer Datenbank).
  Es sollte auch die Zusammenfassung mehrerer Benutzer mit gleichen Zugriffsrechten zu Gruppen möglich sein. Eine Unterscheidung zwischen der Gruppe der Administratoren und der Gruppe der Benutzer ist dabei obligatorisch. Weiterhin sollte eine Trennung von verschiedenen Administrator-Rollen unterstützt werden (siehe M 2.131 - Aufteilung von Administrationstätigkeiten bei Datenbanksystemen).
- Es gibt Datenbanken mit unterschiedlich starken Zugriffsschutzmechanismen. Ähnliche Sicherheitsmechanismen können dabei auch in unterschiedlicher Granularität angeboten werden. Im Vorfeld ist zu klären, welcher Zugriffsschutz erforderlich ist und welche Datenbank-Software den definierten Sicherheitsanforderungen entspricht. Maßgeblich hierfür sind die Möglichkeiten, Zugriffsrechte auf Datenbankobjekte und die Daten selbst einzuschränken.
- Einige Hersteller bieten sowohl die Möglichkeit der Definition von Gruppen als auch die von Rollen an. Dadurch kann eine differenziertere Zugriffskontrolle auf die Datenbankobjekte realisiert werden. Im Vorfeld sind die diesbezüglichen Anforderungen zu klären und mit den zur Auswahl stehenden Datenbank-Softwareprodukten abzugleichen.
- Die Datenbank-Software muß ebenfalls hinsichtlich ihrer Überwachungs- und Kontrollmechanismen überprüft werden. Die diesbezüglichen Anforderungen müssen definiert und mit den Leistungsprofilen der Produkte abgeglichen werden (Beispiele siehe M 2.133 - Kontrolle der Protokolldateien eines Datenbanksystems bzw. M 2.126 - Erstellung eines Datenbanksicherheitskonzeptes).

- Es muß geprüft werden, ob die Datenbank-Software eine Rollentrennung zwischen Administrator und Revisor unterstützt. Es muß möglich sein, die Rolle eines Revisors einzurichten, der als einziger in der Lage ist, die Protokolldateien auszuwerten und zu löschen. Dies verhindert potentielle Manipulationen durch den Datenbank-Administrator.

- Zum Schutz der Datenbankintegrität muß die Datenbank-Software über ein vollständiges Transaktionssystem verfügen, welches dem ACID-Prinzip genügt. Diese Anforderung wird heutzutage von allen wesentlichen relationalen DBMSen erfüllt.

- Es müssen Mechanismen zur Datensicherung der Datenbank vorhanden sein (siehe M 6.49 - Datensicherung einer Datenbank).
  Im Vorfeld muß in diesem Zusammenhang geklärt werden, welche Möglichkeiten hinsichtlich der Datensicherung die Datenbank-Software zur Verfügung stellen muß. So wird beispielsweise eine partielle Datenbanksicherung nicht für alle am Markt erhältlichen Produkte angeboten. Im konkreten Fall gilt es also zu prüfen, ob das erstellte Datensicherungskonzept mit den zur Verfügung stehenden Mechanismen auch umgesetzt werden kann.

Anhand dieser Kriterien müssen die zur Auswahl stehenden Datenbanksysteme geprüft und bewertet werden. Es ist dann diejenige Software auszuwählen, die die spezifischen Anforderungen am besten erfüllt. Weitergehende Anforderungen müssen entweder durch Zusatzprodukte oder durch Eigenentwicklung abgedeckt werden. Es sollte jedoch schon vor der Beschaffung abgeklärt werden, zu welcher Datenbank-Software welche Zusatzprodukte verfügbar sind, um nicht auf teure Eigenentwicklungen zurückgreifen zu müssen.

Von den meisten Datenbankmanagementsystemen sind in der Regel mehrere unterschiedliche Versionen auf dem Markt erhältlich. Dabei unterscheiden sich auch die einzelnen Versionen desselben DBMS in ihrer Funktionalität, u.a. auch in sicherheitsrelevanten Bereichen. Der starke Wettbewerb führt dazu, daß einige Hersteller auch noch nicht vollausgereifte Software ausliefern, bei der dann mit Fehlern und eingeschränkter Funktionalität gerechnet werden muß.

In einer Testphase sollte deshalb überprüft werden, ob die ausgewählte Datenbank-Software die erforderlichen Funktionen in der vorgegebenen Einsatzumgebung auch erfüllt. Dies gilt insbesondere für die Anforderungen an die Performance und die benötigten Mechanismen zur Notfallvorsorge.

Vor der Beschaffung sollten auch Erfahrungen aus vergleichbaren Installationen herangezogen werden.

M 2.125 Installation und Konfiguration einer Datenbank
Grundsätzlich muß zwischen der Erstinstallation einer Datenbank-Software und der Installation auf bestehenden Datenbanksystemen unterschieden werden.

Da bei der erstmaligen Installation einer Datenbank-Software noch keine Benutzer auf die Datenbank zugreifen wollen und auch noch keine Altdaten vorhanden sind (es sei denn in anderen Datenbanksystemen), gestaltet sich dies relativ unproblematisch und stört den normalen IT-Betrieb kaum.

Für Installationen auf bestehenden Systemen sollten dagegen die Arbeiten wenn möglich außerhalb der regulären Arbeitszeiten erfolgen, um Behinderungen des normalen IT-Betriebs weitestgehend zu minimieren. In jedem Fall sollten die Benutzer über bevorstehende Arbeiten informiert werden, um sie auf eventuell mögliche Störungen oder längere Antwortzeiten hinzuweisen.

Die Installation und Konfiguration einer Datenbank gliedert sich in die folgenden Aktivitäten:

- Installation der Datenbank-Software
  Vor der Installation der Datenbank-Software ist zu überprüfen, ob das IT-System entsprechend der Planung vorbereitet wurde, z.B. genügend Speicherplatz zur Verfügung steht und die notwendigen Betriebssystemeinstellungen vorgenommen wurden.
  Bei der Installation der Datenbank-Software sind die Installationsanweisungen des Herstellers zu befolgen. Wenn möglich, sollten die vom Hersteller vorgeschlagenen Default-Einstellungen übernommen werden. Dies gilt vor allem für technische Parameter, die z.B. die Größe verschiedener interner Tabellen des DBMS steuern. Für Parameter, die sich auf sicherheitsrelevante Eigenschaften beziehen, muß u.U. von den vorgegebenen Werten abgewichen werden.
  Die Installation der Datenbank-Software ist geeignet zu dokumentieren. Dies gilt insbesondere für Abweichungen von den vomHersteller vorgeschlagenen Default-Einstellungen, die ausführlich zu begründen sind.
  Sollen vom Hersteller angebotene optionale Funktionalitäten genutzt werden, so ist während der Installation darauf zu achten, daß sie auch entsprechend eingerichtet werden.
  Alle Tätigkeiten in diesem Schritt werden vom fachlich übergreifenden Administrator durchgeführt.

- Erstellen der Datenbank
  Bereits bei der Erstellung der Datenbank sind Parameter anzugeben, die später während des Betriebs des Datenbanksystems nicht mehr geändert werden können. Die Bedeutung dieser Parameter und die geeignete Auswahl ihrer Werte werden in den Installationsunterlagen und Handbüchern des Herstellers ausführlich erläutert und sind dort entsprechend nachzulesen.
  Dem Installationshandbuch bzw. Administrationshandbuch sind außerdem Hinweise über eventuell erforderliche Nacharbeiten nach der Erstellung der Datenbank zu entnehmen.
  Auch dieser Vorgang ist im Rahmen einer Dokumentation festzuhalten.
  Alle Tätigkeiten in diesem Schritt werden vom fachlich übergreifenden Administrator durchgeführt, wobei ihm die anwendungsspezifischen Administratoren beratend zur Seite stehen müssen (z.B. um die Größe der Datenbank festlegen zu können).

- Konfiguration der Datenbank
  Im dritten Schritt ist das Benutzer- und Gruppenkonzept sowie das ggf. zum Einsatz kommende Rollenkonzept umzusetzen. Dazu erstellt der fachlich übergreifende Administrator die einzelnen Berechtigungsprofile und legt alle Gruppen sowie die administrativen Benutzerkennungen (für die anwendungsspezifischen Administratoren) an. Dabei sind die in M 2.132 - Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen festgelegten Regelungen anzuwenden und zu überprüfen. Hängen die entsprechenden Zugriffsberechtigungen von einzelnen Datenbankobjekten ab, können diese natürlich erst dann definiert werden, wenn die Datenbankobjekte auch existieren (siehe Schritt 4).
  Falls die Datenbank-Software eine Verteilung der Daten auf mehrere Dateien oder Festplatten unterstützt, sind zusätzliche Parametereinstellungen vorzunehmen, die das Anlegen dieser Dateien respektive der zugehörigen Speicherbereiche festlegen. Alle vorgenommenen Einstellungen sind detailliert zu dokumentieren (siehe M 2.25 - Dokumentation der Systemkonfiguration). Alle Tätigkeiten in diesem Schritt werden vom fachlich übergreifenden Administrator durchgeführt.

- Erstellen und Konfigurieren von Datenbankobjekten Gemäß des Datenbanksicherheitskonzeptes (siehe M 2.126 - Erstellung eines Datenbanksicherheitskonzeptes) werden im letzten Schritt die Datenbankobjekte der einzelnen Anwendungen angelegt. Dieser Vorgang sollte wenn möglich durch den Einsatz von Skripten automatisiert und protokolliert werden. Nach Anlage der Datenbankobjekte sind die notwendigen Zugriffsberechtigungen für Rollen, Gruppen und Benutzer zu ergänzen. Ebenso können jetzt die konkreten Benutzer anhand der existierenden Berechtigungsprofile erstellt werden.
  Alle Tätigkeiten in diesem Schritt werden von den anwendungsspezifischen Administratoren durchgeführt.

M 2.126 Erstellung eines Datenbanksicherheitskonzeptes

Da eine zentrale Datenhaltung über einen längeren Zeitraum hinweg einen zentralen und kritischen Aspekt des Informationsmanagements einer Behörde bzw. eines Unternehmens darstellt, kommt der Erstellung eines Datenbankkonzeptes eine besondere Bedeutung zu. Ein Datenbankkonzept beschäftigt sich mit den notwendigen Vorarbeiten zum eigentlichen Betrieb der Datenbank und sollte deshalb immer ein Datenbanksicherheitskonzept enthalten, welches auch den laufenden Betrieb untersucht. Werden die Daten nicht ausreichend geschützt, kann es zu einem Verlust der Vertraulichkeit, Verfügbarkeit oder der Integrität kommen. Um diesem vorzubeugen, ist es unumgänglich, ein schlüssiges Datenbanksicherheitskonzept zu erstellen.

Um die Sicherheit einer Datenbank zu gewährleisten, muß ein geeignetes Datenbankmanagementsystem (DBMS) eingesetzt werden. Damit ein DBMS effektiven Schutz bieten kann, müssen folgende grundlegende Bedingungen erfüllt sein. Das DBMS muß

- auf einer umfassenden Sicherheitspolitik aufsetzen,

- im IT-Sicherheitskonzept der Organisation eingebettet sein,

- korrekt installiert und
- korrekt administriert werden.

Direkte Zugriffe auf die Datenbank (z.B. über SQL-Interpreter wie SQL*Plus) dürfen nur für administrative Nutzer zugelassen werden, um Manipulationen an den Daten bzw. Datenbankobjekten (z.B. Tabellen und Indizes) zu verhindern. Datenbankobjekte dürfen ausschließlich über spezielle Kennungen kontrolliert modifiziert werden. Dementsprechend muß das DBMS über ein geeignetes Zugriffs- und Zugangskonzept verfügen (siehe M 2.129 - Zugriffskontrolle einer Datenbank und M 2.128 - Zugangskontrolle einer Datenbank). Benutzer-Kennungen, die nur über eine Anwendung Datenmodifikationen durchführen können, dürfen keinen direkten Zugang zur Datenbank erhalten, während Kennungen zur Verwaltung der Datenbankobjekte der kontrollierte direkte Zugriff erlaubt sein muß.

Weiterhin müssen folgende wichtige Aspekte in einem Datenbanksicherheitskonzept geregelt werden:

- Die physische Speicherung bzw. Spiegelung der Datenbankdateien (z.B. der DBMS-Software, der Datenbank an sich oder der Protokolldateien) sowie deren Verteilung ist festzulegen, um z.B. die Verfügbarkeit und Ausfallsicherheit zu erhöhen. Aus Sicherheitsgründen sollten gespiegelte Kontrolldateien beispielsweise auf verschiedenen Festplatten abgelegt sein. Der Ausfall einer Platte bedeutet dann nicht gleichzeitig den Verlust aller Kontrolldateien. Falls die Datenbankobjekte einer Anwendung in eigenen Datendateien abgelegt werden, so sollte man bei der Verteilung der Datendateien darauf achten, daß bei einem Ausfall einer Festplatte nicht alle Anwendungen betroffen sind.
- Es muß eine regelmäßige Prüfung des tatsächlich anfallenden Datenvolumens bzw. des Zuwachses des Datenvolumens im späteren laufenden Betrieb durchgeführt werden, um den benötigten Speicherplatz auch für zukünftige Bedürfnisse geeignet dimensionieren zu können.
- Geeignete Mechanismen zur Datensicherung müssen angewendet werden (siehe M 6.49 - Datensicherung einer Datenbank).
- Der Einsatz von Überwachungs- und Kontrollmechanismen ist festzulegen, d.h. ob und in welchem Umfang Datenbankaktivitäten protokolliert werden sollen. Hier stellt sich u.a. die Frage, ob beispielsweise nur der Zeitpunkt einer Datenmodifikation festgehalten wird, oder ob auch die Modifikation selbst protokolliert werden soll (siehe M 2.133 - Kontrolle der Protokolldateien eines Datenbanksystems).

Für die Konzeption und den Betrieb eines Datenbanksystems muß geeignetes Personal zur Verfügung stehen. Der zeitliche Aufwand für den Betrieb eines Datenbanksystems darf nicht unterschätzt werden. Alleine die Auswertung der angefallenen Protokolldaten nimmt erfahrungsgemäß viel Zeit in Anspruch. Ein Datenbank-Administrator muß fundierte Kenntnisse über die eingesetzte DBMS-Software besitzen und auch entsprechend geschult werden.

M 2.127 Inferenzprävention
Zum Schutz personenbezogener und anderer vertraulicher Daten eines Datenbanksystems ist grundsätzlich jedem Benutzer nur der Zugriff auf diejenigen Daten zu gestatten, die für seine Tätigkeiten notwendig sind. Alle anderen Informationen, die sich zusätzlich in der Datenbank befinden, sind vor ihm zu verbergen.

Zu diesem Zweck müssen die Zugriffsberechtigungen auf Tabellen bis hin zu deren Feldern definiert werden können. Dies kann mittels Verwendung von Views und Grants durchgeführt werden (vgl. M 2.129 - Zugriffskontrolle einer Datenbank). Damit ist es einem Benutzer nur möglich, die für ihn bestimmten Daten einzusehen und zu verarbeiten. Stellt er Datenbankabfragen, die auf andere Informationen zugreifen wollen, werden diese vom DBMS zurückgewiesen.

Im Zusammenhang mit statistischen Datenbanken, die Daten über Personengruppen, Bevölkerungsschichten oder ähnliches enthalten, treten dagegen andere Schutzanforderungen auf. In einer statistischen Datenbank unterliegen die einzelnen, personenbezogenen Einträge dem Datenschutz, statistische Informationen sind jedoch allen Benutzern zugänglich.

Hier gilt es zu verhindern, daß aus Kenntnissen über die Daten einer Gruppe auf die Daten eines individuellen Mitglieds dieser Gruppe geschlossen werden kann. Es muß außerdem verhindert werden, daß durch das Wissen der in der Datenbank gespeicherten Informationen bzw. der Ablagestrukturen der Daten in der Datenbank die Anonymität dieser Daten durch entsprechend formulierte Datenbankabfragen umgangen werden kann (z.B. wenn die Ergebnismenge einer Datenbankabfrage nur einen Datensatz beinhaltet). Diese Problematik wird Inferenzproblem, der Schutz vor solchen Techniken Inferenzprävention genannt.

Auch wenn die Daten einer statistischen Datenbank anonymisiert sind, kann durch Inferenztechniken der Personenbezug zu bestimmten Datensätzen wiederhergestellt werden. Eine Zurückweisung bestimmter Anfragen (z.B. Anfragen mit nur einem oder wenigen Ergebnistupeln) reicht im allgemeinen nicht aus, da auch die Verweigerung einer Antwort durch das DBMS Informationen beinhalten kann.

Durch das Erstellen verschiedener Statistiken kann die Anonymität der Daten ebenfalls verloren gehen. Ein solcher indirekter Angriff zielt darauf ab, aus mehreren Statistiken Rückschlüsse auf die persönlichen Daten eines einzelnen Individuums ziehen zu können. Eine Schutzmaßnahme ist in diesem Fall, die Freigabe von sogenannten sensitiven Statistiken nicht zu erlauben, was als unterdrückte Inferenzprävention bezeichnet wird. Eine weitere Möglichkeit ist die Verzerrung solcher Statistiken durch kontrolliertes Runden (gleiche Statistiken sind gleich zu runden) oder die Beschränkung auf statistisch relevante Teilmengen mit der Auflage, daß gleiche Anfragen immer Bezug auf die gleichen Teilmengen nehmen. Dieses Verfahren wird als verzerrende Inferenzprävention bezeichnet.

Werden weitergehende Anforderungen an die Vertraulichkeit der Daten gestellt, ist deren Verschlüsselung erforderlich (vergleiche M 4.72 - Datenbank-Verschlüsselung).

M 2.128 Zugangskontrolle einer Datenbank

Die Datenbank-Software muß über geeignete Mechanismen zur Identifikation und Authentisierung der Benutzer verfügen, um eine wirkungsvolle Zugangskontrolle zu gewährleisten (siehe M 2.132 - Regelung für die Einrichtung von Datenbankbenutzern/ -benutzergruppen).
Generell sollte man für normale Benutzer den Zugang zu einer Produktionsdatenbank über einen interaktiven SQL-Interpreter unterbinden. Auf solche Datenbanken sollte ausschließlich ein indirekter Zugang über die entsprechenden Anwendungen möglich sein. Die einzige Ausnahme bilden hier Datenbankkennungen zu Administrationszwecken.
Remote-Zugänge zu Datenbanken sollten äußerst restriktiv gehandhabt werden. Ist diese Art des Zugangs nicht zwingend erforderlich, so sind diese zu unterbinden. Ansonsten sollte nur denjenigen Benutzern ein Remote-Zugang ermöglicht werden, die diesen auch tatsächlich benötigen. Andere Benutzer dürfen nicht in der Lage sein, sich selbst einen Remote-Zugang zu verschaffen. Keinesfalls darf ein Remote-Zugang ohne Angabe einer gültigen Benutzerkennung und Eingabe eines Paßwortes möglich sein.

M 2.129 Zugriffskontrolle einer Datenbank

Um einen wirkungsvollen Schutz der Vertraulichkeit und Integrität der Daten einer Datenbank zu erreichen, müssen eine Reihe von Maßnahmen umgesetzt werden. Neben einer Zugangskontrolle der Datenbank, die in M 2.128 - Zugangskontrolle einer Datenbank beschrieben wird, sind dies im wesentlichen die folgenden Möglichkeiten der Zugriffskontrolle:

- Schutz der Datenbankobjekte
  Es sollte eine logische Zuordnung der Datenbankobjekte, also der Tabellen, Indizes, Datenbankprozeduren, etc., zu den Anwendungen erfolgen, die diese Objekte benutzen. Die daraus entstehenden Gruppen von Datenbankobjekten je Anwendung werden eigens hierfür einzurichtenden Kennungen zugeordnet. Damit können die Zugriffsberechtigungen der Datenbankobjekte so eingestellt werden, daß nur über diese speziellen Kennungen eine Modifikation der Objekte stattfinden kann. Greifen mehrere Anwendungen auf dieselben Datenbankobjekte zu, sollten diese als eigene Gruppe isoliert werden.
  Werden beispielsweise die Daten zweier Anwendungen A und B in der Datenbank verwaltet, so legt man zwei Datenbankkennungen AnwA und AnwB an. Alle Datenbankobjekte, die eindeutig der Anwendung A zugeordnet werden können, werden mit der Datenbankkennung AnwA angelegt und verwaltet. Analog wird mit den Datenbankobjekten von Anwendung B verfahren.
  Ein Beispiel für ein zentrales Datenbankobjekt, das von beiden Anwendungen benutzt wird, sei eine Tabelle, die alle ansteuerbaren Drucker beinhaltet. Datenbankobjekte dieser Kategorie sollten nicht einer Kennung der Anwendungen (AnwA oder AnwB) zugeordnet werden, statt dessen sollten solche Datenbankobjekte unter einer eigenen Kennung (z.B. Druck) zusammengefaßt und mit dieser zentralen Kennung verwaltet werden.
  Diese speziellen Kennungen sind nicht personenbezogen. Statt dessen erhalten eigens hierfür autorisierte Personen (z.B. der Datenbankadministrator oder der Administrator der zugehörigen Anwendung) das Paßwort der benötigten Kennung, falls Modifikationen an den Datenbankobjekten vorgenommen werden müssen.

- Schutz der Daten
  Durch eine Definition von Views können spezielle Benutzer-Sichten erzeugt werden, so daß die Daten der Datenbank nach bestimmten Kriterien sichtbar gemacht bzw. unsichtbar gehalten werden. Über einen View wird explizit festgelegt, welche Felder aus einer oder mehreren Tabellen ein Benutzer zu sehen bekommt. Durch die restriktive Vergabe von Zugriffsrechten (den im folgenden beschriebenen Grants) auf solche Views können vertrauliche Daten vor unberechtigtem Zugriff geschützt werden.
  Es müssen Zugriffsrechte (Grants) auf Tabellen, Views oder sogar einzelne Felder einer Tabelle vergeben werden. Diese Rechte sind immer an bestimmte Benutzer, Rollen oder Benutzergruppen gebunden. Zugriffsrechte sollten jedoch immer für Benutzergruppen oder Rollen und nicht für einzelne Personen vergeben werden, da dies sonst bei einer großen Anzahl von Benutzern zu einem hohen administrativen Aufwand führt. Es können Zugriffsberechtigungen lesender (read), ändernder (update), löschender (delete) oder neu einfügender (insert) Art unterschieden werden. Mit der Vergabe von Zugriffsberechtigungen sollte so sparsam wie möglich umgegangen werden, da man sonst sehr schnell den Überblick über die aktuellen Zugriffsrechte verliert und damit Sicherheitslücken geschaffen werden. Insbesondere sollte die Möglichkeit, Rechte an alle zu vergeben (GRANT ... TO PUBLIC), nicht genutzt werden.
  Im allgemeinen ist es nur dem Besitzer eines Datenbankobjektes erlaubt, Zugriffsberechtigungen an andere Benutzer weiterzugeben. Einige Datenbanksysteme stellen jedoch die Möglichkeit zur Verfügung, daß der Besitzer eines Datenbankobjektes auch das Recht, Zugriffsrechte weiterzugeben, an andere Benutzer vergeben kann. Von dieser Möglichkeit sollte nur in begründeten Ausnahmefällen Gebrauch gemacht werden, da man auf diese Weise die Kontrolle über den Zugriff auf die Daten bzw. die Datenbankobjekte verliert.

- Restriktiver Datenzugriff über Anwendungen
  Anwendungen sollten einen restriktiven Zugriff auf die Daten unterstützen, d.h. in Abhängigkeit der Benutzerkennung und der Gruppenzugehörigkeit sollten nur diejenigen Funktionalitäten und Daten zur Verfügung gestellt werden, die ein Benutzer für die Ausführung seiner Aufgaben benötigt. Eine Form der Realisierung ist hier die Verwendung von sogenannten Stored Procedures.
  Stored Procedures sind Abfolgen von SQL-Anweisungen, die in der Datenbank voroptimiert gespeichert werden. Beim Aufruf einer Stored Procedure müssen nur ihr Name und eventuelle Parameter angegeben werden, um die dahinterstehenden SQL-Anweisungen auszuführen. Dies hat zum einen den Vorteil, daß nicht die gesamten SQL-Anweisungen zum Datenbankserver übertragen werden müssen, was bei komplexeren Operationen die Netzbelastung vermindert. Zum anderen kann das Datenbanksystem die SQL-Anweisungen in einer optimierten Form ablegen, so daß sie schneller ausgeführt werden. Die stärkste Einschränkung bei der Rechtevergabe ist die Vergabe von Zugriffsrechten auf Stored Procedures statt auf Tabellen oder Views. Wenn Zugriffsrechte nur auf Stored Procedures vergeben werden, können die Benutzer nur die von den Datenbankverantwortlichen ausgewählten Operationen ausführen.

M 2.130 Gewährleistung der Datenbankintegrität
Die Integritätssicherung und -überwachung in einer Datenbank soll die Korrektheit der zugehörigen Daten bzw. einen korrekten Zustand der Datenbank gewährleisten. Die folgenden Techniken sind zur Vermeidung inkorrekter Daten bzw. Zustände innerhalb einer Datenbank zu beachten:

- Zugriffskontrolle
  Damit ist der Schutz der betreffenden Datenbank vor unautorisiertem Zugriff mittels der Vergabe von Zugriffsrechten gemeint, wie in M 2.129 - Zugriffskontrolle einer Datenbank beschrieben. Damit wird dem manipulativen Ändern von Daten bzw. Datenbankobjekten (wie z.B. Tabellen) vorgebeugt.
  Verantwortlich für die Umsetzung der Zugriffskontrolle ist der Datenbankadministrator.
  Auf eine detaillierte Ausführung wird an dieser Stelle verzichtet und statt dessen auf die Maßnahme M 2.129 - Zugriffskontrolle einer Datenbank verwiesen

- Synchronisationskontrolle
  Die Synchronisationskontrolle dient der Verhinderung von Inkonsistenzen, die durch einen parallelen Zugriff auf denselben Datenbestand entstehen können. Es gibt dazu verschiedene Techniken, wie z.B. das Sperren von Datenbankobjekten (Locking) oder die Vergabe von Zeitstempeln (Timestamps).
  Verantwortlich für die Umsetzung sind die Verantwortlichen der IT-Anwendungen, insofern ein zusätzlicher Mechanismus zur Verfügung gestellt werden muß, der über die Möglichkeiten des DBMS hinausgeht.
  Auf eine detaillierte Ausführung wird verzichtet, da im allgemeinen jedes DBMS eine Synchronisationskontrolle durchführt. Vom Einsatz eines DBMS, welches dies nicht leisten kann, wird dringend abgeraten.

- Integritätskontrolle
  Hierunter fällt die Vermeidung semantischer Fehler bzw. semantisch unsinniger Zustände der Datenbank durch Einhaltung und Überwachung der geforderten Integritätsbedingungen. Diese können sich auf einzelne Relationen beziehen oder mehrere Relationen miteinander in Beziehung setzen (referentielle Integrität). Beispiele sind die Angabe eines Primärschlüssels für eine Relation, die Definition von Wertebereichen zu den einzelnen Attributen oder die Formulierung spezieller Bedingungen mittels einer assertion-Klausel. Dies kann durch das DBMS automatisch mittels eines Monitors überprüft werden, der z.B. durch die Verwendung von Triggern oder Stored Procedures realisiert werden kann. Damit sind prinzipiell beliebige Transaktionen möglich, jedoch werden diejenigen vom DBMS zurückgewiesen, die die Datenbank-Konsistenz verletzen würden.
  Verantwortlich für die Umsetzung sind die Verantwortlichen der IT-Anwendungen respektive der fachliche Administrator, falls es sich um eine Umsetzung der Integritätsbedingungen in Form von Relationen, Primärschlüsseln oder allgemeinen Datenbankobjekten handelt.
  Im Rahmen der Konzeption einer IT-Anwendung sind zu erstellen

- ein Datenmodell, welches neben den Datenbankobjekten auch deren Beziehungen untereinander abbildet, und
- ein Fachkonzept, welches u.a. Bedingungen beschreibt, unter denen Daten manipuliert werden dürfen.

Im Rahmen der Realisierung einer IT-Anwendung sind die folgenden Punkte zu beachten:

- Die konkrete Umsetzung des in der konzeptionellen Phase definierten Datenmodells muß festgelegt werden. Hierzu gehören die Definition und Anlage von Tabellen, Indizes, Wertebereichen usw.
- Die Definition von Triggern oder Stored Procedures erfolgt im Rahmen der Realisierung des Fachkonzepts. Trigger und Stored Procedures können dabei sowohl innerhalb der Anwendung (in den Programmen), als auch der Datenbank (für Tabellen) Verwendung finden. Trigger, die auf Datenbankebene eingesetzt werden, wirken unabhängig von darüberliegenden Anwendungen und sind aus diesem Grund zentral zu verwalten.

M 2.131 Aufteilung von Administrationstätigkeiten bei Datenbanksystemen
Um einen geordneten Betrieb von Datenbanksystemen zu ermöglichen, sind Administratoren zu bestimmen. Diesen obliegt neben allgemeinen Administrationsarbeiten insbesondere die Benutzerverwaltung einschließlich der Verwaltung der Zugriffsrechte. Zusätzlich sind sie für die Sicherheitsbelange der betreuten Datenbanksysteme zuständig.

Neben den in M 2.26 - Ernennung eines Administrators und eines Vertreters und M 3.10 - Auswahl eines vertrauenswürdigen Administrators und Vertreters genannten Maßnahmen sind speziell für Datenbanksysteme folgende Dinge zu beachten.
Es sollten grundsätzlich zwei verschiedene Administrator-Rollen unterschieden werden:

- die fachlich übergreifende Administration der Datenbank-Software und
- die Administration der anwendungsspezifischen Belange.

Diese beiden Aufgaben sollten von verschiedenen Personen durchgeführt werden, um eine Trennung der anwendungsspezifischen und fachlich übergreifenden Administration einer Datenbank zu erreichen.

Der grundsätzliche Betrieb des DBMS, die Durchführung der Datensicherungen oder die Archivierung von Datenbeständen sind beispielsweise Bestandteil der fachlich übergreifenden Datenbankadministration.

Bei der anwendungsspezifischen Administration werden dagegen die Erfordernisse der einzelnen Anwendungen an die Datenbank bearbeitet. Dies kann z.B. die Verwaltung der zugehörigen Datenbankobjekte, die Unterstützung der Benutzer bei Problemen bzw. Fragen oder die Verwaltung der entsprechenden Datenbankkennungen beinhalten. Letzteres ist allerdings nur dann

möglich, wenn die Verwaltung der Datenbankennungen je Anwendung über ein entsprechendes Berechtigungskonzept durch die Datenbank-Software unterstützt wird, also von den fachlich übergreifenden Berechtigungen getrennt werden kann.

Der fachlich übergreifende Administrator richtet die für die anwendungsspezifischen Belange zuständigen Administratorkennungen mit den zugehörigen Berechtigungen ein. Dazu gehört insbesondere das Recht, Datenbanken anzulegen. Die Rechtevergabe für die einzelnen Benutzer sollte dagegen für jede anwendungsspezifische Datenbank getrennt durchgeführt werden und zwar vom jeweils zuständigen anwendungsspezifischen Administrator.

M 2.132 Regelung für die Einrichtung von Datenbankbenutzern/ -benutzergruppen
Für die Einrichtung von Benutzern/Benutzergruppen in einer Datenbank bilden die Voraussetzung für eine angemessene Vergabe von Zugriffsrechten (siehe M 2.129 - Zugriffskontrolle einer Datenbank) und für die Sicherstellung eines geordneten und überwachbaren Betriebsablaufs. Im allgemeinen erhält dazu jeder Datenbankbenutzer eine interne Datenbankkennung, über die ihn das Datenbanksystem identifiziert. Damit können nur autorisierte Personen auf die Datenbank zugreifen.
In Anlehnung an M 2.30 - Regelung für die Einrichtung von Benutzern / Benutzergruppen sollte ein Formblatt existieren, um von jedem Benutzer bzw. für jede Benutzergruppe zunächst die erforderlichen Daten abzufragen:

- Name, Vorname,
- Vorschlag für die Benutzerkennung (wenn nicht durch Konventionen vorgegeben),
- Organisationseinheit,
- Erreichbarkeit (z.B. Telefon, Raum),
- ggf. Projekt,
- ggf. Anwendungen, die benutzt werden sollen und auf das Datenbanksystem zugreifen,
- ggf. Angaben über die geplante Tätigkeit im Datenbanksystem und die dazu erforderlichen Rechte sowie die Dauer der Tätigkeit,
- ggf. Restriktionen auf Zeiten, Zugriffsberechtigungen (für bestimmte Tabellen, Views etc.), eingeschränkte Benutzerumgebung,
- ggf. Zustimmung von Vorgesetzten.

Es sollte eine begrenzte Anzahl von Rechteprofilen festgelegt werden. Ein neuer Benutzer wird dann einem oder mehreren Profilen zugeordnet und erhält damit genau die für seine Tätigkeit erforderlichen Rechte. Dabei sind die datenbankspezifischen Möglichkeiten bei der Einrichtung von Benutzern und Gruppen zu beachten. Es ist sinnvoll, Namenskonventionen für die

Benutzer- und Gruppenkennungen festzulegen (z.B. Benutzer-ID = Kürzel Organisationseinheit ; lfd. Nummer).

Dabei können Benutzer-, Rollen- und Gruppenprofile benutzt werden. Soweit möglich, sollten jedoch keine benutzerspezifischen Profile verwendet werden, da dies bei einer großen Anzahl von Benutzern zu einem hohen administrativen Aufwand führt. Bei der Definition von Gruppenprofilen muß man zwischen restriktiven und großzügigen Berechtigungsprofilen abwägen. Werden die Gruppenprofile zu restriktiv gehandhabt, muß eine große Anzahl von Gruppen verwaltet werden, was zu einem hohen administrativen Aufwand führt. Werden die Gruppenprofile dagegen zu großzügig definiert, kann es zu Redundanzen zwischen verschiedenen Gruppen kommen oder zur Einräumung von unnötig umfangreichen Rechten, was wiederum zur Verletzung der Vertraulichkeit von Daten führen kann.

In der Regel muß jedem Benutzer eine eigene Datenbankkennung zugeordnet sein, es dürfen nicht mehrere Benutzer unter derselben Kennung arbeiten.

Normalerweise besteht zwischen der Datenbankkennung und der Benutzerkennung des zugrundeliegenden Betriebssystems keine Verbindung. Einige Hersteller bieten in ihrer Datenbank-Software jedoch die Möglichkeit an, die Betriebssystemkennung in das Datenbanksystem zu übernehmen. Dies erspart den Anwendern eine Paßwortabfrage für den Zugang zur Datenbank, falls diese sich bereits mit Ihrer eigenen Betriebssystemkennung angemeldet haben.

So können beispielsweise unter Oracle sogenannte OPS$ -Kennungen verwendet werden. Eine solche Kennung setzt sich aus dem Präfix „OPS$“ und der Betriebssystemkennung des Anwenders zusammen. Nur wenn sich ein Anwender mit seiner Betriebssystemkennung am Datenbanksystem anmeldet, wird kein Paßwort vom DBMS abgefragt. Meldet sich der Anwender dagegen unter einer anderen Kennung an, so erfolgt eine Paßwortabfrage.

Diese Möglichkeit beinhaltet allerdings die Gefahr, daß bei einer Schutzverletzung auf Betriebssystemebene (z.B. das Knacken des entsprechenden Paßwortes) der Zugriff auf die Datenbank nicht mehr verhindert werden kann. Der Schutz der Datenbank ist demnach stark von der Sicherheit des zugrundeliegenden Betriebssystems abhängig. Dabei handelt es sich im allgemeinen nicht um das üblicherweise sichere Betriebssystem des Datenbank-Servers, sondern um das eines Clients, der unter Umständen wesentlich schwächer geschützt ist. Deshalb wird von der Verwendung dieser Möglichkeit abgeraten, statt dessen sollte bei der Forderung nach einer einfachen Handhabung für die Benutzer (Stichwort Single-Sign-On) der Einsatz eines Zusatzproduktes zur zentralen Benutzerverwaltung für den gesamten IT-Betrieb erwogen werden (z.B. ISM Access Master von Bull). Aber auch hier müssen die konkreten Sicherheitsanforderungen mit dem entsprechenden Zusatzprodukt abgeglichen werden.

M 2.133 Kontrolle der Protokolldateien eines Datenbanksystems
Die in einem Datenbanksystem mögliche Protokollierung bzw. Auditierung ist in einem sinnvollen Umfang zu aktivieren. Werden zuviele Ereignisse protokolliert, wird die Performance

der Datenbank negativ beeinflußt und die Protokolldateien wachsen stark an. Es muß also immer zwischen dem Bedürfnis, möglichst viele Informationen zur Sicherheit der Datenbank zu sammeln, und der Möglichkeit, diese Informationen zu speichern und auszuwerten, abgewogen werden.
Dabei sind insbesondere folgende Vorkommnisse von Interesse:

- Anmeldezeiten und -dauer der Benutzer,
- Anzahl der Verbindungen zur Datenbank,
- fehlgeschlagene bzw. abgewiesene Verbindungsversuche,
- Auftreten von Deadlocks innerhalb des Datenbanksystems,
- I/O-Statistik für jeden Benutzer,
- Zugriffe auf die Systemtabellen (siehe auch M 4.69 - Regelmäßiger Sicherheitcheck der Datenbank),
- Erzeugung neuer Datenbankobjekte und
- Datenmodifikationen (evtl. mit Datum, Uhrzeit und Benutzer).

Die Protokollierung sicherheitsrelevanter Ereignisse ist als Sicherheitsmaßnahme allerdings nur dann wirksam, wenn die protokollierten Daten auch ausgewertet werden. Daher sind die Protokolldateien in regelmäßigen Abständen durch einen Revisor auszuwerten. Ist es organisatorisch oder technisch nicht möglich, einen unabhängigen Revisor mit der Auswertung der Protokolldateien zu betrauen, ist eine Kontrolle der Tätigkeiten des Administrators nur schwer möglich.

Die Protokolldaten müssen regelmäßig gelöscht werden, um ein übermäßiges Anwachsen der Protokolldateien zu verhindern. Sie dürfen allerdings nur dann gelöscht werden, wenn die Protokolldateien vorher ausgewertet und kontrolliert wurden. Dies kann manuell oder automatisch geschehen, falls entsprechende Werkzeuge zur Verfügung stehen.

Weiterhin ist der Zugriff auf die Protokolldateien strikt zu beschränken. Einerseits muß verhindert werden, daß Angreifer ihre Aktionen durch nachträgliche Änderung der Protokolldateien verbergen können, andererseits könnten über die gezielte Auswertung von Protokolldateien Leistungsprofile der Benutzer erstellt werden. Deshalb dürfen beispielsweise Änderungen überhaupt nicht vorgenommen werden können und lesender Zugriff darf nur den Revisoren gestattet werden.

Um die Auswertung der Protokolldaten zu vereinfachen, können vom Datenbank-Administrator zusätzliche Tools eingesetzt werden, die eine automatisierte Überwachung durchführen. Solche Produkte können beispielweise die Log-Dateien von Datenbanksystemen nach vorgegebenen Mustern auswerten und bei Bedarf einen Alarm erzeugen.
Weitere Maßnahmen, die in diesem Zusammenhang beachtet werden müssen, sind in M 2.64 -

Kontrolle der Protokolldateien zu finden.

M 2.134 Richtlinien für Datenbank-Anfragen
Die relationale Datenbanksprache SQL (Standard Query Language) ist eine international standardisierte Sprache für relationale Datenbanksysteme, die eine weite Verbreitung erfahren hat und in den meisten DBMS implementiert ist. Mittels SQL können sowohl Modifikationen der Daten (UPDATE, INSERT, DELETE), als auch der Datenbankobjekte formuliert (CREATE, ALTER, DROP) sowie Informationen abgefragt werden (SELECT). Um einen sicheren Betrieb eines Datenbanksystems zu gewährleisten, sollten die folgenden Grundsätze in einer Richtlinie für Datenbank-Anfragen beschrieben sein.

- SQL-Anfragen sollten so exakt wie möglich formuliert werden. Dies gilt insbesondere für SQL-Anfragen, die aus Anwendungen heraus gestellt werden. So führt beispielsweise die SQL-Anweisung
  SELECT * FROM <Tabelle> WHERE <Bedingung>
  bei Änderungen des Tabellenschemas (Hinzufügen bzw. Löschen von Feldern oder Vertauschen der Reihenfolge von Feldern) unweigerlich zu Fehlern oder sogar zu einem Absturz der zugehörigen Anwendung.

- Felder sollten immer explizit angegeben werden. Damit ist sichergestellt, daß die Daten in der erwarteten Reihenfolge zur Verfügung stehen und beispielsweise nur diejenigen Daten selektiert werden, die man tatsächlich benötigt.

- Für einschränkende Datenbankanfragen (WHERE-Klausel) ist die Reihenfolge der angegebenen Selektionsbedingungen von großer Bedeutung. Die WHERE-Klausel sollte so formuliert werden, daß als erstes diejenige Bedingung angegeben wird, die die kleinstmögliche Ergebnismenge selektiert und erst zum Schluß die Bedingung greift, die die größte Ergebnismenge liefern würde. Auf diese Weise wird die Performance des Datenbanksystems optimiert, da sich durch die geschickte Anordnung der Selektionsbedingungen der Suchvorgang erheblich verkürzen läßt. Das gleiche gilt analog für Datenbankanfragen, die über mehrere Tabellen hinweg formuliert werden (sogenannte Joins).

  Es sei an dieser Stelle erwähnt, daß Datenbankmanagementsysteme bereits häufig Datenbankanfragen selbständig optimieren. Oft werden sogar mehrere Optimierungsstrategien zur Auswahl angeboten, die über verschiedene Parameter ausgewählt werden können. Werden diese sogenannten Optimizer vom DBMS verwendet, kann dies allerdings dazu führen, daß sorgfältig formulierte Datenbankabfragen intern vom DBMS nicht in der erwarteten Art und Weise abgearbeitet werden.

  In diesem Zusammenhang bieten einige Datenbankmanagementsysteme die Möglichkeit, die Abarbeitung von Datenbankanfragen zu untersuchen (z. B. in Oracle mit EXPLAIN oder für Ingres mittels SETOEP). Desweiteren besteht die Möglichkeit, über sogenannte HINTS in der Datenbankanfrage deren Abarbeitung explizit zu definieren und somit den

Optimizer im Prinzip auszuschalten. Von dieser Möglichkeit sollte allerdings so wenig wie möglich Gebrauch gemacht werden. Welche Optimizer das DBMS unterstützt sowie deren Vor- und Nachteile sind in den Handbüchern des DBMS normalerweise dokumentiert. Falls mehrere Optimizer zur Auswahl stehen, sollte beim Administrator nachgefragt werden, welcher Optimizer eingesetzt wird.

- Im Falle von Joins sollte zusätzlich beachtet werden, daß die Zuordnung von Feldern zu den Tabellen eindeutig erfolgt.
- Existieren Views auf Tabellen, so sollten diese auch für die Formulierung von Datenbankanfragen benutzt werden.
- Alle Datenbanktransaktionen sollten explizit mit einem COMMIT bestätigt werden. Falls das DBMS ein automatisches COMMIT unterstützt, sollte dieses nicht aktiviert werden, da es sonst u.U. zu ungewollten Inkonsistenzen in der Datenbank kommen kann.
- Zur Vermeidung von Sperrkonflikten oder gar Deadlocks ist für jede fachliche Datenbank eine Sperrstrategie festzulegen (z.B. hierarchisches Sperren oder explizites Sperren aller Tabellen am Anfang der Transaktion).
- Anwendungsentwickler sollten nach jeder SQL-Anweisung den Fehlerstatus prüfen, so daß die Anwendung so früh wie möglich auf eingetretene Fehler reagieren kann.
- Falls das DBMS bestimmte systemspezifische Kommandos unterstützt, mit denen beispielsweise die Protokollierung ausgeschaltet oder das Locking-Verfahren verändert werden kann, sollten die Berechtigungen für diese Kommandos den Benutzern entzogen werden. Hier ist also im Vorfeld genau zu klären, welche systemspezifischen Einstellungen bzw. Kommandos von den Benutzern bzw. den Anwendungsentwicklern geändert bzw. benutzt werden dürfen.
- Bei der Entwicklung von Anwendungen sollten alle Datenbankzugriffe in einem Modul oder einem bestimmten Teil des Programmcodes zusammengefaßt werden, da sonst zur Überprüfung der obigen Grundsätze der gesamte Programmcode des Anwendungssystems herangezogen werden müßte. Hierdurch wird die Wartung und Pflege des Anwendungssystems, z.B. bei Änderungen des Datenmodells, erleichtert.

M 2.135 Gesicherte Datenübernahme in eine Datenbank

In vielen Datenbanksystemen besteht aus Anwendungssicht die Notwendigkeit, Daten aus anderen Systemen zu übernehmen. Dabei lassen sich prinzipiell die beiden folgenden Kategorien unterscheiden:

- Erst- oder Altdatenübernahme
  Dies betrifft die Übernahme von Daten aus Altsystemen, wenn beispielsweise ein neues Datenbanksystem beschafft wurde und produktiv eingesetzt werden soll. Hierbei ist insbesondere sicherzustellen, daß

- die Daten in einem Format vorliegen, das in die Zieldatenbank übernommen werden kann,
- die Daten vollständig sind, d.h. für alle Felder, die in der Zieldatenbank gefüllt werden sollen, müssen Daten zur Übernahme zur Verfügung gestellt werden, und
- die Konsistenz und Datenintegrität der Datenbank gewährleistet ist.

Im Vorfeld der Datenübernahme ist ein Konzept zu erstellen, wie die zu übernehmenden Daten aufbereitet werden müssen und wie die Übernahme konkret durchgeführt werden soll. Weiterhin ist unbedingt eine Komplettsicherung der Altdaten vorzunehmen. Erfolgt die Datenübernahme in mehreren Schritten, sollte vor jedem einzelnen Schritt eine unabhängige Datensicherung durchgeführt werden.

- Regelmäßige Datenübernahme
  Befinden sich in der Zieldatenbank bei einer Datenübernahme bereits Daten, die nicht verändert werden dürfen, oder werden in regelmäßigen Zeitabständen Daten in eine Datenbank übernommen, so
  - ist vor der Datenübernahme eine Komplettsicherung der Datenbank durchzuführen,
  - sollte die Datenübernahme wenn möglich außerhalb der regulären Betriebszeiten stattfinden,
  - müssen die betroffenen Benutzer von der bevorstehenden Datenübernahme rechtzeitig informiert werden, insbesondere dann, wenn mit Einschränkungen hinsichtlich der Verfügbarkeit oder des Antwortzeitverhaltens zu rechnen ist,
  - ist vor der ersten Datenübernahme ein Konzept zu erstellen, wie die zu übernehmenden Daten aufbereitet werden müssen bzw. wie die Übernahme konkret durchzuführen ist. Insbesondere muß in diesem Konzept berücksichtigt werden, wie Konflikte zwischen den bereits existierenden Daten in der Zieldatenbank und den zu übernehmenden Daten vermieden werden, d.h. inwieweit die Integrität und Konsistenz der Zieldatenbank gewahrt bleibt. Desweiteren sind Vorkehrungen zu treffen, um eine mehrfache Übernahme der gleichen Daten zu verhindern.

Vor der Durchführung einer Datenübernahme ist festzulegen, was beim Auftreten von Fehlern zu unternehmen ist. Dies beinhaltet z.B., ob beim Auftreten eines fehlerhaften Datensatzes mit dem nächsten Satz fortgefahren werden kann, oder ob die komplette Datenübernahme abgebrochen werden muß. Weiterhin ist festzulegen, wie die Datenübernahme nach einem Abbruch wieder aufgesetzt wird.

M 2.136 Einhaltung von Regelungen bzgl. Arbeitsplatz und Arbeitsumgebung
Am häuslichen Arbeitsplatz müssen dieselben Vorschriften und Richtlinien bezüglich der Gestaltung des Arbeitsplatzes (z.B. Einrichtung eines Bildschirmarbeitsplatzes) und der Arbeitsumgebung gelten wie in der Institution. Dies sollte in Absprache mit dem Telearbeiter durch den in der Institution Verantwortlichen für den Arbeits- und Gesundheitsschutz, dem IT-Sicherheitsbeauftragten, dem Datenschutzbeauftragten sowie dem Betriebs- bzw. Personalrat

und dem direkten Vorgesetzten des Telearbeiters begutachtet werden können.

M 2.137 Beschaffung eines geeigneten Datensicherungssystems
Ein Großteil der Fehler, die beim Erstellen oder Restaurieren einer Datensicherung auftreten, sind Fehlbedienungen. Daher sollte bei der Beschaffung eines Datensicherungssystem nicht allein auf seine Leistungsfähigkeit geachtet werden, sondern auch auf seine Bedienbarkeit und insbesondere auf seine Toleranz gegenüber Benutzerfehlern.
Bei der Auswahl von Sicherungssoftware sollte darauf geachtet werden, daß sie die folgenden Anforderungen erfüllt:

- Die Datensicherungssoftware sollte ein falsches Medium ebenso wie ein beschädigtes Medium im Sicherungslaufwerk erkennen können.
- Sie sollte mit der vorhandenen Hardware problemlos zusammenarbeiten.
- Es sollte möglich sein, Sicherungen automatisch zu vorwählbaren Zeiten bzw. in einstellbaren Intervallen durchführen zu lassen, ohne daß hierzu manuelle Eingriffe (außer dem eventuell notwendigen Bereitstellen von Sicherungsdatenträgern) erforderlich wären.
- Es sollte möglich sein, einen oder mehrere ausgewählte Benutzer automatisch über das Sicherungsergebnis und eventuelle Fehlermeldungen per E-Mail oder ähnliche Mechanismen zu informieren. Die Durchführung von Datensicherungen inklusive des Sicherungsergebnisses und möglicher Fehlermeldungen sollten in einer Protokolldatei abgespeichert werden.
- Die Sicherungssoftware sollte die Sicherung des Backup-Mediums durch ein Paßwort, oder noch besser durch Verschlüsselung unterstützen. Weiterhin sollte sie in der Lage sein, die gesicherten Daten in komprimierter Form abzuspeichern.
- Durch Vorgabe geeigneter Include- und Exclude-Listen bei der Datei- und Verzeichnisauswahl sollte genau spezifiziert werden können, welche Daten zu sichern sind und welche nicht. Es sollte möglich sein, diese Listen zu Sicherungsprofilen zusammenzufassen, abzuspeichern und für spätere Sicherungsläufe wieder zu benutzen.
- Es sollte möglich sein, die zu sichernden Daten in Abhängigkeit vom Datum ihrer Erstellung bzw. ihrer letzten Modifikation auszuwählen.
- Die Sicherungssoftware sollte die Erzeugung logischer und physischer Vollkopien sowie inkrementeller Kopien (Änderungssicherungen) unterstützen.
- Die zu sichernden Daten sollten auch auf Festplatten und Netzlaufwerken abgespeichert werden können.
- Die Sicherungssoftware sollte in der Lage sein, nach der Sicherung einen automatischen Vergleich der gesicherten Daten mit dem Original durchzuführen und nach der Wiederherstellung von Daten einen entsprechenden Vergleich zwischen den rekonstruierten Daten und dem Inhalt des Sicherungsdatenträgers durchzuführen.

- Bei der Wiederherstellung von Dateien sollte es möglich sein auszuwählen, ob die Dateien am ursprünglichen Ort oder auf einer anderen Platte bzw. in einem anderen Verzeichnis wiederhergestellt werden. Ebenso sollte es möglich sein, das Verhalten der Software für den Fall zu steuern, daß am Zielort schon eine Datei gleichen Namens vorhanden ist. Dabei sollte man wählen können, ob diese Datei immer, nie oder nur in dem Fall, daß sie älter als die zu rekonstruierende Datei ist, überschrieben wird, oder daß in diesem Fall eine explizite Anfrage erfolgt.

Falls mit dem eingesetzten Programm die Datensicherung durch Paßwort geschützt werden kann, sollte diese Option genutzt werden. Das Paßwort ist dann gesichert zu hinterlegen (siehe M 2.22 - Hinterlegen des Paßwortes).

Bei den meisten Betriebssystemen werden Programme für Datensicherungen mitgeliefert. Nicht alle erfüllen allerdings die Ansprüche an Produkte für professionelle und komfortable Datensicherungen. Stehen aber keine solchen Produkte zur Verfügung, so sollten die systemzugehörigen Programme verwendet werden.

M 2.138 Strukturierte Datenhaltung
Eine schlecht strukturierte Datenhaltung kann zu einer Vielzahl von Problemen führen. Alle IT-Benutzer sind daher darauf hinzuweisen, wie eine gut strukturierte und übersichtliche Datenhaltung aussehen sollte. Auf allen Servern sollten entsprechende Strukturen durch die Administratoren vorgegeben werden. Dies ist ohnehin Voraussetzung, um eine differenzierte Vergabe von Zugriffsrechten realisieren zu können.

Programm- und Arbeitsdateien sollten immer in getrennten Bereichen gespeichert werden. Dies erleichtert auch die Durchführung von Datensicherungen und die Sicherstellung des korrekten Zugriffsschutzes. Bei den meisten Applikationsprogrammen ändern sich nach der Installation keine oder nur sehr wenige Konfigurationsdateien. Soweit möglich, sollten alle Dateien, die sich regelmäßig ändern, in gesonderten Verzeichnissen abgespeichert werden, damit nur diese in die regelmäßigen Datensicherungen mitaufgenommen werden müssen.

Bei vernetzten Systemen stellt sich außerdem die Frage, welche Programme bzw. Dateien auf den lokalen Festplatten oder auf einem Netzserver abgelegt werden sollten. Beides hat Vor- und Nachteile und muß sowohl von der organisatorischen Struktur als auch von der eingesetzten Hard- und Software abhängig gemacht werden. So sollten z.B. Dateien mit hohen Verfügbarkeitsansprüchen zusammen mit den zugehörigen Applikationsprogrammen besser auf den Arbeitsplatzrechnern gehalten werden als auch einem Netzserver. Dann muß allerdings auch die entsprechende Notfallvorsorge für diese Arbeitsplatzrechner betrieben werden.

Es sollten aufgaben- oder projektbezogene Verzeichnisse eingerichet werden, um die Zuordnung von Dateien zu erleichtern. Es sollten möglichst wenig Daten in personenbezogenen Verzeichnissen abgelegt werden.

Um zu verhindern, daß für die weitere Arbeit grundlegenden Dateien wie Briefvorlagen, Formularen, Projektplänen o.ä. unterschiedliche Versionsstände existieren, sollten diese zentral verwaltet werden. Sie sollten beispielsweise auf einem Server so vorgehalten werden, daß jeder lesend darauf zugreifen kann, aber es sollte für jede solche Datei jeweils nur eine Person geben, die sie verändern darf.

Es sollte regelmäßig überprüft werden,

- ob Daten aus dem Produktionssystem entfernt werden können, weil sie archiviert oder gelöscht werden können,
- ob Zugriffsrechte entzogen werden können, weil Mitarbeiter die Projektgruppe verlassen haben,
- ob auf allen IT-Systemen die aktuellsten Versionen von Formularen, Vorlagen, etc. gespeichert sind.

Dies ist durch die Benutzer für deren IT-Systeme bzw. die von ihnen verwalteten Verzeichnisse und von den Administratoren der Server regelmäßig zu überprüfen. Diese Prüfungen sollten mindestens vierteljährlich durchgeführt werden, da sonst die Kenntnisse über Inhalt und Herkunft der Dateien wieder aus den Gedächtnissen der Mitarbeiter verschwunden sind.

M 2.2000 Jahr-2000-Fähigkeit von Produkten, Programmen und Daten
Das Jahr-2000-Problem ist nur vordergründig ein Problem der rechnerinternen Uhr, die Jahresangaben nur zweistellig darstellt und damit alle datumsbasierten Abfragen nur unzureichend beantwortet. Die verkürzte und nicht korrekte zweistellige Datumsangabe wird über das Betriebssystems an Standardsoftware oder Anwenderprogramme zur Verarbeitung weitergegeben. Die Datumsangaben werden dann einerseits Steuerung von Programm und Betriebsabläufen verwendet, andererseits speichern Programme die datumsrelevanten Informationen in Dateien oder Datenbanken. Findet die Verarbeitung und Speicherung von Informationen in einer vernetzten Welt statt, sind außer den erwähnten noch weitere IT-Komponenten beteiligt.

Alle IT-Komponenten, die nicht „Jahr-2000-fähig“ sind, sind mangelhafte Arbeitsmittel. Eine fehlende „Jahr-2000-Fähigkeit“ von Produkten, Programmen und Daten stellt im juristischen Sinn einen erheblichen Mangel dar und entspricht damit nicht den Anforderungen an die IT-Sicherheit. Eine wesentliche Voraussetzung für die Verfügbarkeit, die Integrität und die Vertraulichkeit von IT-Anwendungen und den verarbeiteten Informationen sind integere IT-Komponenten. In einem Jahr-2000 Projekt sind alle IT-Komponenten auf „Jahr-2000-Fähigkeit“ zu prüfen, bei Mangel ist diese herzustellen.
Begriffsbestimmung „Jahr-2000-Fähigkeit“
„Jahr-2000-Fähigkeit“ bedeutet, daß weder die Leistung noch die Funktionsfähigkeit der gelieferten Produkte bzw. der betroffenen Anwendungen durch den Wechsel des Datums zum Jahr 2000 beeinträchtigt wird. Kein aktueller Wert des Tagesdatums darf vor, während und nach dem Jahr 2000 eine Unterbrechung oder Störung verursachen. Alle Änderungen zeitbezogener

Daten müssen die geforderten Ergebnisse für alle gültigen Werte des Datums liefern.

Alle datumsrelevanten Elemente in Schnittstellen und Datenspeichern ermöglichen ohne menschliche Eingriffe die eindeutige und korrekte Festlegung des Jahrhunderts. Werden Elemente des Datums ohne Angabe des Jahrhunderts dargestellt, muß das korrekte Jahrhundert im Hinblick auf alle Handhabungen und Auswirkungen im Zusammenhang mit diesen Elementen eindeutig sein. Dies schließt die korrekte Verarbeitung der Schaltjahre ein.

Sofern vertraglich vereinbart, gilt dies auch für das Zusammenwirken mit anderen Produkten.

Da die Datenverarbeitung nur ein integraler Bestandteil von Geschäftsprozessen ist, ist die Herstellung der Jahr-2000-Fähigkeit eine Aufgabe des Gesamtunternehmens. In den Bereichen und Dienststellen mit Jahr-2000-Projekten, in denen bisher kein eigenes Vorgehen erarbeitet wurde oder die Anwendung eines bekannten Vorgehensmodells nicht vereinbart wurde, wird ein Vorgehen nach dem Jahr-2000-Leitfaden „Tackling the Year 2000 Problem“ der englischen Administration (CCTA, U.K.) empfohlen.

Schritte eines projektorientierten Vorgehens:

1. Initiierung eines Jahr-2000-Projektes mit Klärung der Kompetenzen und Verantwortlichkeiten.
2. Erstellen einer Jahr-2000-Inventarliste mit allen IT-Systemen, IT-Anwendungen, Daten und Vorhaben.
3. Grobe Bewertung der Kritikalität der IT-Systeme, IT-Anwendungen und Daten.
4. Überprüfen der kritischen IT-Systeme und IT-Anwendungen, Schätzung des Lösungsaufwandes.
5. Verfeinern und aktualisieren der Jahr-2000 Inventarliste; Angaben zu Prioritätensetzung, Betroffenheit, Vorgehen, Lösungsalternativen, Kosten, Terminen und Risiken.
6. Planung / Reservierung der benötigten finanziellen, personellen und zeitlichen Ressourcen.
7. Analyse / Umstellung / Test
8. Nachbereitung

Bei knappen Ressourcen wird die Lösung des Jahr-2000-Problems anhand einer Prioritätenliste der IT-Anwendungen von „vital“ zu „marginal“ empfohlen.

Die Rechtsabteilung ist frühzeitig in das Jahr-2000 Projekt einzubinden. Hier sind insbesondere die Allgemeinen Geschäftsbedingungen frühzeitig um „Jahr-2000-Klauseln“ zu erweitern und bei Abschluß neuer Verträge bindend.
Dies trifft insbesondere zu:

- für den Kauf von Hardware oder für die Beschaffung von Gesamtsystemen,
- für die Wartung von Hard- und die Pflege von Software,
- für Lizenzen sowie die Herstellung von Individualsoftware und
- für Dienstleistungen.

Bestehende Verträge sind auf Aspekte der „Jahr-2000-Fähigkeit“ zu überprüfen ggf. in Zusammenarbeit mit den Vertragspartnern nachzubessern.

Für den Bereich der Bundesbehörden hat die „Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung“ (KBSt) mit den KBSt-Briefen Nr. 3/97 und Nr. 5/97 auf das Jahr-2000-Problem hingewiesen und Hilfen für die Lösung des Jahr-2000-Problems zur Verfügung gestellt. In diesen Briefen ist auch der KBSt Vorschlag bei Abschluß von BVB-Verträgen enthalten. Die KBSt-Briefe können über das Bundesministerium des Innern; Arbeitsgruppe OI3 (KBSt); Postfach 170290; D-53108 Bonn bezogen werden.

Das BSI stellt unterschiedliche Informationen zum Jahr-2000-Problem auf dem Internet-Server des BSI (http://www.bsi.bund.de) zur Verfügung. Der Bericht „Jahr-2000-Problem in der Bürokommunikation“ enthält die Beschreibung einer projektorientierten Vorgehensweise und eine Sammlung von Informationsquellen der Hersteller von Hard- und Software-Produkten.

Der Bericht befindet sich auf der CD-ROM zum IT-Grundschutzhandbuch:
GSHB_98\HILFSM\J2K.DOC

H.3 Maßnahmenkatalog Personal

M 3.1 Geregelte Einarbeitung/Einweisung neuer Mitarbeiter
Neuen Mitarbeitern müssen interne Regelungen, Gepflogenheiten und Verfahrensweisen im IT-Einsatz bekannt gegeben werden. Ohne eine entsprechende Einweisung kennen sie ihre Ansprechpartner bzgl. IT-Sicherheit nicht, sie wissen nicht, welche IT-Sicherheitsmaßnahmen durchzuführen sind und welche IT-Sicherheitspolitik die Behörde bzw. das Unternehmen betreibt. Daraus können Störungen und Schäden für den IT-Einsatz erwachsen.
Daher kommt der geregelten Einarbeitung neuer Mitarbeiter eine entsprechend hohe Bedeutung zu.
Die Einarbeitung bzw. Einweisung sollte zumindest folgende Punkte umfassen:

- Planung der notwendigen Schulungen; arbeitsplatzbezogene Schulungsmaßnahmen (s. auch M 3.4 - Schulung vor Programmbenutzung und M 3.5 - Schulung zu IT-Sicherheitsmaßnahmen),
- Vorstellung aller Ansprechpartner, insbesondere zu IT-Sicherheitsfragen,

- Erläuterung der hausinternen Regelungen und Vorschriften zur IT-Sicherheit.

Hilfreich zur Durchführung der Einarbeitung ist ein Laufzettel oder eine Checkliste, aus der die einzelnen Aktivitäten und der erreichte Stand der Einarbeitung ersichtlich sind.

M 3.2 Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
Bei der Einstellung von Mitarbeitern sollen diese verpflichtet werden, einschlägige Gesetze (z.B. § 5 BDSG "Datengeheimnis"), Vorschriften und interne Regelungen einzuhalten. Damit sollen neue Mitarbeiter mit den bestehenden Vorschriften und Regelungen zur IT-Sicherheit bekannt gemacht und gleichzeitig zu deren Einhaltung motiviert werden. Dabei ist es sinnvoll, nicht nur die Verpflichtung durchzuführen, sondern auch die erforderlichen Exemplare der Vorschriften und Regelungen auszuhändigen und gegenzeichnen zu lassen bzw. für die Mitarbeiter an zentraler Stelle zur Einsichtnahme vorzuhalten.

M 3.3 Vertretungsregelungen
Vertretungsregelungen haben den Sinn, für vorhersehbare (Urlaub, Dienstreise) und auch unvorhersehbare Fälle (Krankheit, Unfall, Kündigung) des Personenausfalls die Fortführung der Aufgabenwahrnehmung zu ermöglichen. Daher muß vor Eintritt eines solchen Falles geregelt sein, wer wen in welchen Angelegenheiten mit welchen Kompetenzen vertritt. Dies ist besonders im Bereich der Informationsverarbeitung von Bedeutung, da dafür meist Spezialwissen erforderlich ist und eine zeitgerechte Einarbeitung unkundiger Mitarbeiter für den Vertretungsfall nicht möglich ist.
Für die Vertretungsregelungen sind folgende Randbedingungen einzuhalten:

- Die Übernahme von Aufgaben im Vertretungsfall setzt voraus, daß der Verfahrens- oder Projektstand hinreichend dokumentiert ist.

- Das Benennen eines Vertreters reicht in der Regel nicht aus, es muß überprüft werden, wie der Vertreter zu schulen ist, damit er die Aufgaben inhaltlich übernehmen kann. Stellt sich heraus, daß es Personen gibt, die aufgrund ihres Spezialwissens nicht kurzfristig ersetzbar sind, so bedeutet deren Ausfall eine gravierende Gefährdung des Normalbetriebes. Hier ist es von besonders großer Bedeutung, einen Vertreter zu schulen.

- Es muß festgelegt sein, welcher Aufgabenumfang im Vertretungsfall von wem wahrgenommen werden soll.

- Der Vertreter darf die erforderlichen Zugangs- und Zutrittsberechtigungen nur im Vertretungsfall erhalten.

- Ist es in Ausnahmefällen nicht möglich, für Personen einen kompetenten Vertreter zu benennen oder zu schulen, sollte frühzeitig überlegt werden, welche externen Kräfte für den Vertretungsfall eingesetzt werden können.

M 3.4 Schulung vor Programmnutzung
Durch unsachgemäßen Umgang mit IT-Anwendungen hervorgerufene Schäden können vermieden werden, wenn die Benutzer eingehend in die IT-Anwendungen eingewiesen werden. Daher ist es unabdingbar, daß die Benutzer vor der Übernahme IT-gestützter Aufgaben ausreichend geschult werden. Dies betrifft sowohl die Nutzung von Standardprogrammpaketen als auch von speziell entwickelten IT-Anwendungen.
Darüber hinaus müssen auch bei umfangreichen Änderungen in einer IT-Anwendung Schulungsmaßnahmen durchgeführt werden.
Stehen leicht verständliche Handbücher zu IT-Anwendungen bereit, so kann anstelle der Schulung auch die Aufforderung stehen, sich selbständig einzuarbeiten. Eine wesentliche Voraussetzung dazu ist allerdings die Bereitstellung ausreichender Einarbeitungszeit.

M 3.5 Schulung zu IT-Sicherheitsmaßnahmen
Die überwiegende Zahl von Schäden im IT-Bereich entsteht durch Nachlässigkeit. Um dies zu verhindern, ist jeder einzelne zum sorgfältigen Umgang mit der IT zu motivieren. Zusätzlich sind Verhaltensregeln zu vermitteln, die ein Verständnis für die IT-Sicherheitsmaßnahmen wecken. Insbesondere sollen folgende Themen in der Schulung zu IT-Sicherheitsmaßnahmen vermittelt werden:

- Sensibilisierung für IT-Sicherheit
  Jeder Mitarbeiter ist auf die Notwendigkeit der IT-Sicherheit hinzuweisen. Das Aufzeigen der Abhängigkeit der Behörde bzw. des Unternehmens und damit der Arbeitsplätze von dem reibungslosen Funktionieren der IT-Systeme ist ein geeigneter Einstieg in die Sensibilisierung. Darüber hinaus ist der Wert von Informationen herauszuarbeiten, insbesondere unter den Gesichtspunkten Vertraulichkeit, Integrität und Verfügbarkeit. Diese Sensibilisierungsmaßnahmen sind in regelmäßigen Zeitabständen zu wiederholen, evtl. auch durch praktische Hinweise z.B. in der Hauspost.

- Die mitarbeiterbezogenen IT-Sicherheitsmaßnahmen
  Zu diesem Thema sollen die IT-Sicherheitsmaßnahmen vermittelt werden, die in einem IT-Sicherheitskonzept erarbeitet wurden und von den einzelnen Mitarbeitern umzusetzen sind. Dieser Teil der Schulungsmaßnahmen hat eine große Bedeutung, da viele IT-Sicherheitsmaßnahmen erst nach einer entsprechenden Schulung und Motivation effektiv umgesetzt werden können.

- Die produktbezogenen IT-Sicherheitsmaßnahmen
  Zu diesem Thema sollen die IT-Sicherheitsmaßnahmen vermittelt werden, die inhärent mit einem Softwareprodukt verbunden sind und bereits im Lieferumfang enthalten sind. Dies können neben Paßwörtern zur Anmeldung, der Pausenschaltung durch Bildschirmschoner auch Möglichkeiten der Verschlüsselung von Dokumenten oder Datenfeldern sein. Hinweise und Empfehlungen über die Strukturierung und Organisation von Dateien, die Bewegungsdaten enthalten, können die Vergabe von Zugriffsrechten erleichtern und den Aufwand zu Datensicherung deutlich reduzieren.

- Das Verhalten bei Auftreten eines Computer-Virus auf einem PC
  Hier soll den Mitarbeitern vermittelt werden, wie mit Computer-Viren umzugehen ist. Mögliche Inhalte dieser Schulung sind (siehe M 6.23 - Verhaltensregeln bei Auftreten eines Computer-Virus):
  - Erkennen des Computer-Virusbefalls
  - Wirkungsweise und Arten von Computer-Viren
  - Sofortmaßnahmen im Verdachtsfall
  - Maßnahmen zur Eliminierung des Computer-Virus
  - Vorbeugende Maßnahmen
- Der richtige Einsatz von Paßwörtern
  Hierbei sollen die Bedeutung des Paßwortes für die IT-Sicherheit sowie die Randbedingungen erläutert werden, die einen wirksamen Einsatz eines Paßwortes erst ermöglichen (vgl. auch M 2.11 - Regelung des Paßwortgebrauchs).
- Die Bedeutung der Datensicherung und deren Durchführung
  Die regelmäßige Datensicherung ist eine der wichtigsten IT-Sicherheitsmaßnahmen in jedem IT-System. Vermittelt werden soll das Datensicherungskonzept der Behörde bzw. des Unternehmens und die von jedem einzelnen durchzuführenden Datensicherungsaufgaben. Besonders bedeutend ist dies für den PC-Bereich, in dem jeder Benutzer selbst die Datensicherung verantwortlich durchführen muß.
- Der Umgang mit personenbezogenen Daten
  An den Umgang mit personenbezogene Daten sind besondere Anforderungen zu stellen. Mitarbeiter, die mit personenbezogenen Daten (sowohl in IT-Systemen als auch in Akten) arbeiten müssen, sind für die gesetzlich erforderlichen Sicherheitsmaßnahmen zu schulen. Dies betrifft den Umgang mit Auskunftsersuchen, Änderungs- und Verbesserungswünschen der Betroffenen, gesetzlich vorgeschriebene Löschfristen, Schutz der Vertraulichkeit und die Übermittlung der Daten.
- Die Einweisung in Notfallmaßnahmen
  Sämtliche Mitarbeiter (auch nicht unmittelbar mit IT befaßte Personen wie Pförtnerdienst oder Wachpersonal) sind in bestehende Notfallmaßnahmen einzuweisen. Dazu gehört die Erläuterung der Fluchtwege, die Verhaltensweisen bei Feuer, der Umgang mit Feuerlöschern, das Notfall-Meldesystem (wer als erstes wie zu benachrichtigen ist) und der Umgang mit dem Notfall-Handbuch.
- Vorbeugung gegen Social Engineering
  Die Mitarbeiter sollen auf die Gefahren des Social Engineering hingewiesen werden. Die typischen Muster solcher Versuche, über gezieltes Aushorchen an vertrauliche Informationen zu gelangen, ebenso wie die Methoden, sich dagegen zu schützen, sollten bekannt gegeben werden. Da Social Engineering oft mit der Vorspiegelung einer falschen Identität einhergeht, sollten Mitarbeiter regelmäßig darauf hingewiesen werden, die Identität

von Gesprächspartnern zu überprüfen und insbesondere am Telefon keine vertraulichen Informationen weiterzugeben.

M 3.6 Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern
Scheidet ein Mitarbeiter aus, so ist zu beachten:

- Vor dem Ausscheiden ist eine Einweisung des Nachfolgers durchzuführen.
- Von dem Ausscheidenden sind sämtliche Unterlagen, ausgehändigte Schlüssel, ausgeliehene IT-Geräte (z.B. tragbare Rechner, Speichermedien, Dokumentationen) zurückzufordern. Insbesondere sind die Behörden- bzw. Firmenausweise einzuziehen.
- Es sind sämtliche für den Ausscheidenden eingerichteten Zugangsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. Dies betrifft auch die externen Zugangsberechtigungen via Datenübertragungseinrichtungen. Wurde in Ausnahmefällen eine Zugangsberechtigung zu einem IT-System zwischen mehreren Personen geteilt (z.B. mittels eines gemeinsamen Paßwortes), so ist nach Ausscheiden einer der Personen die Zugangsberechtigung zu ändern.
- Ist die ausscheidende Person ein Funktionsträger in einem Notfallplan, so ist der Notfallplan zu aktualisieren.
- Sämtliche mit Sicherheitsaufgaben betrauten Personen, insbesondere der Pförtnerdienst, sind über das Ausscheiden des Mitarbeiters zu unterrichten.
- Ausgeschiedenen Mitarbeitern ist der unkontrollierte Zutritt zum Behörden- oder Firmengelände, insbesondere zu Räumen mit IT-Systemen zu verwehren.
- Optional kann sogar für den Zeitraum zwischen Aussprechen der Kündigung und dem Ausscheiden der Entzug sämtlicher Zugangs- und Zugriffsrechte auf IT-Systeme sowie darüber hinaus auch das Verbot, schützenswerte Räume zu betreten, ausgesprochen werden.

Als ein praktikables Hilfsmittel haben sich Laufzettel erwiesen, auf denen die einzelnen Aktivitäten des Ausscheidenden vorgezeichnet sind, die er vor Verlassen der Behörde bzw. des Unternehmens zu erledigen hat.

M 3.7 Anlaufstelle bei persönlichen Problemen
Für eine unzureichende Aufgabenerfüllung können oftmals persönliche Probleme eines Arbeitnehmers ursächlich sein. Als Probleme lassen sich beispielsweise hohe Schulden, Suchtkrankheiten aber auch Schwierigkeiten am Arbeitsplatz (Über-/Unterforderung, Mobbing) aufzählen. Um dem Betroffenen bei der Bewältigung dieser Probleme zu helfen, kann es in vielen Fällen hilfreich sein, wenn eine Vertrauensperson zur Verfügung steht. Dieser Ansprechpartner sollte dabei sowohl die Interessen des Betroffenen im Auge haben und konkrete Hilfestellung anbieten als auch die Interessen des Unternehmens bzw. Behörde wahren und gemeinsam mit dem

Betroffenen nach Lösungsmöglichkeiten suchen.
An diese Vertrauensperson müssen sich aber auch Vorgesetzte und Kollegen wenden können, wenn wiederholt Auffälligkeiten Dritter wahrgenommen wurden, die auf eine verminderte Zuverlässigkeit schließen lassen. Die Vertrauensperson muß dann die Möglichkeit haben, sich an den Betroffenen zu wenden und Hilfe anzubieten.
Eine solche Stelle können Personalrat, Betriebsrat, Betriebsärzte einnehmen. Die Einrichtung einer solchen Anlaufstelle ist allen Mitarbeitern bekanntzugeben. Externe Stellen sind zum Beispiel die Beratungsstellen der gesetzlichen Krankenkassen.

M 3.8 Vermeidung von Störungen des Betriebsklimas
Ein positives Betriebsklima motiviert die Mitarbeiter einerseits zur Einhaltung von IT-Sicherheitsmaßnahmen und bewirkt andererseits die Reduzierung von fahrlässigen oder vorsätzlichen Handlungen, die eine Störung des IT-Betriebs herbeiführen können. Daher sollte auch unter IT-Sicherheitsaspekten versucht werden, ein positives Betriebsklima zu erreichen. Die Vielzahl der Möglichkeiten kann hier nicht angeführt werden, es sei lediglich eine Auswahl möglicher Maßnahmen genannt, deren Angemessenheit im einzelnen zu prüfen wäre:

- Einrichtung eines Sozialraums,
- Vermeidung von Überstunden,
- Einhaltung von Pausenzeiten,
- geregelte Aufgabenverteilung,
- gleichmäßige Arbeitsauslastung,
- leistungsgerechte Bezahlung.

M 3.9 Ergonomischer Arbeitsplatz
Beim sinnvollen und effektiven Einsatz der IT ist es neben der klaren Beschreibung von Aufgaben, Pflichten, Rechten und Verantwortlichkeiten erforderlich, dafür zu sorgen, daß die Nutzung der IT in optimaler Weise erfolgen kann.
Der Arbeitsplatz ist ergonomisch zu gestalten. Stuhl, Tisch, Bildschirm und Tastatur müssen individuell einstellbar sein, um eine möglichst fehlerfreie Bedienung der IT zu ermöglichen und zu fördern. Das beinhaltet u.a., daß Rückenlehne, Sitzhöhe und Sitzfläche des Stuhls verstellbar sein müssen, aber auch, daß die Arbeitsmittel so angeordnet werden können, daß für die jeweilige Arbeitsaufgabe eine möglichst geringe Belastung entsteht.
Ein entsprechend ausgestatteter Arbeitsplatz erleichtert es auch, IT-Sicherheitsmaßnahmen einzuhalten. Gibt es verschließbare Schreibtische oder Schränke, so können Datenträger, Dokumentationen, Unterlagen und Zubehör darin verschlossen werden.

M 3.10 Auswahl eines vertrauenswürdigen Administrators und Vertreters
Den IT-System- oder TK-Anlagen-Administratoren und deren Vertretern muß vom Betreiber

großes Vertrauen entgegengebracht werden können. Sie haben - in Abhängigkeit vom eingesetzten System - weitgehende und oftmals alle Befugnisse. Administratoren und ihre Vertreter sind in der Lage, auf alle gespeicherten Daten zuzugreifen, ggf. zu verändern und Berechtigungen so zu vergeben, daß erheblicher Mißbrauch möglich wäre.
Das hierfür eingesetzte Personal muß sorgfältig ausgewählt werden. Es soll regelmäßig darüber belehrt werden, daß die Befugnisse nur für die erforderlichen Administrationsaufgaben verwendet werden dürfen.

M 3.11 Schulung des Wartungs- und Administrationspersonals
Das Wartungs- und Administrationspersonal sollte mindestens soweit geschult werden, daß

- alltägliche Administrationsarbeiten selbst durchgeführt,
- einfache Fehler selbst erkannt und behoben,
- Datensicherungen selbsttätig durchgeführt und
- die Eingriffe von externem Wartungspersonal nachvollzogen werden können.

Entsprechende Schulungen werden in der Regel von den Herstellern der IT-Systeme bzw. TK-Anlagen angeboten. Administratoren von TK-Anlagen sollten außerdem in der Lage sein,

- das Betriebsverhalten der TK-Anlage mit Hilfe der Kontrollanzeigen an den Geräten zu beurteilen,
- die TK-Anlage selbständig außer- und in Betrieb nehmen zu können.

M 3.12 Information aller Mitarbeiter über mögliche TK-Warnanzeigen, -symbole und -töne
Die Bedeutung der Warnanzeigen, -töne und -symbole der TK-Anlage sollte allen Mitarbeitern bekannt sein. Hierzu zählen insbesondere:

- Aufmerksamkeitston für direktes Ansprechen,
- Aufschalte-Warnton,
- Freisprechanzeige,
- Anzeige für aktiviertes direktes Ansprechen,
- Anzeige für automatischen Rückruf und
- Anzeige/Einblendung bei Dreierkonferenz.

Da die Nutzung bestimmter, eigentlich nicht freigegebener Leistungsmerkmale (Beispiel: Zeugenschaltung) zu Beeinträchtigungen der IT-Sicherheit führen kann, sollten besonders deren Warnanzeigen und -töne bekannt sein.

M 3.13 Sensibilisierung der Mitarbeiter für mögliche TK-Gefährdungen
Die Mitarbeiter müssen über die mit dem Benutzen einer digitalen TK-Anlage verbundenen Gefährdungen informiert werden. Dies könnte z.B. durch eine kurze Unterweisung oder mit Hilfe von Merkblättern geschehen. Es ist darauf hinzuweisen, daß ein abnormes Verhalten der TK-Anlage gemeldet werden soll. Bei Manipulationen an der TK-Anlage sollte eine unabhängige Kontrollinstanz wie IT-Sicherheitsmanagement oder Datenschutzbeauftragte informiert werden.

M 3.14 Einweisung des Personals in den geregelten Ablauf eines Datenträgeraustausches
Mangelnde Information und Einweisung der Mitarbeiter führt in vielen Fällen dazu, daß Restriktionen der Informationsweitergabe nicht oder nur unzulänglich eingehalten werden. Die Festlegungen, welchen Kommunikationspartnern wann welche Daten übermittelt werden dürfen (M 2.42 - Festlegung der möglichen Kommunikationspartner), ist den an einem Datenträgeraustausch Beteiligten daher zwingend bekanntzugeben. Außerdem sind die prinzipiellen Schritte für den Ablauf eines Datenträgeraustausches zu fixieren (eventuell als Dienstanweisung) und die Mitarbeiter zur Einhaltung zu verpflichten.
Zusätzlich ist eine Sensibilisierung der am Datenträgeraustausch beteiligten Mitarbeiter hinsichtlich möglicher Gefährdungen und einzuhaltender Sicherheitsmaßnahmen vor, während und nach dem Transport der Datenträger notwendig.
Werden bestimmte IT-gestützte Verfahren zum Schutz der Daten während des Austausches eingesetzt (wie etwa Verschlüsselung oder Checksummenverfahren), so sind diese Mitarbeiter in die Handhabung dieser Verfahren ausreichend einzuarbeiten.

M 3.15 Informationen für alle Mitarbeiter über die Nutzung eines Fax-Gerätes
Alle Mitarbeiter sind auf die Besonderheiten der Informationsübermittlung per Fax hinzuweisen sowie darüber zu informieren, daß die Rechtsverbindlichkeit einer Fax-Sendung stark eingeschränkt ist. Eine verständliche Bedienungsanleitung sollte am Fax-Gerät zur Verfügung stehen. Insbesondere ist, ggf. in Form einer Dienstanweisung, festzulegen,

- wer der Fax-Verantwortliche ist und damit für die Verteilung eingehender Fax-Sendungen und als Ansprechpartner in Fax-Problemfällen zuständig ist,
- wer das Faxgerät benutzen darf,
- daß das Versenden von vertraulichen Informationen per Fax vermieden werden sollte,
- daß ein einheitliches Fax-Vorblatt benutzt werden soll,
- daß sich vor Austausch schutzbedürftiger Informationen über ein Fax-Gerät Empfänger und Absender hierüber telefonisch verständigen,

- daß ggf. Einzelsendenachweise für die korrekte Übertragung zu kontrollieren und diese den Unterlagen beizufügen sind.

M 3.16 Einweisung in die Bedienung des Anrufbeantworters
Jeder, der einen Anrufbeantworter in seinem Bereich einsetzt, sollte sich mit der Bedienung vertraut machen und so Möglichkeiten und Grenzen des Gerätes kennenlernen. Somit werden Fehlbedienungen weitgehend ausgeschlossen. Darüber hinaus sollten die für Anrufbeantworter notwendigen IT-Sicherheitsmaßnahmen transparent gemacht werden.

M 3.17 Einweisung des Personals in die Modem-Benutzung
Die Mitarbeiter sind über mögliche Gefährdungen, einzuhaltende Sicherheitsmaßnahmen und Regelungen beim Betrieb eines Modems zu unterrichten. Hierbei sind insbesondere die Auswirkungen verschiedener Konfigurationen auf die Betriebssicherheit des Modems zu vermitteln. Jeder Modem-Benutzer sollte sich mit der Bedienung vertraut machen und so Möglichkeiten und Grenzen des Gerätes kennenlernen.

M 3.18 Verpflichtung der PC-Benutzer zum Abmelden nach Aufgabenerfüllung
Wird ein PC von mehreren Benutzern genutzt und besitzen die einzelnen Benutzer unterschiedliche Zugriffsrechte auf im PC gespeicherte Daten oder Programme, so kann der erforderliche Schutz mittels einer Zugriffskontrolle nur dann erreicht werden, wenn jeder Benutzer sich nach Aufgabenerfüllung am PC abmeldet. Ist es einem Dritten möglich, an einem PC unter der Identität eines anderen weiterzuarbeiten, so ist jegliche sinnvolle Zugriffskontrolle unmöglich. Daher sind alle PC-Benutzer zu verpflichten, sich nach Aufgabenerfüllung abzumelden. Ist keine Zugriffskontrolle realisiert, so ist die Abmeldung des Benutzers aus Gesichtspunkten der Ordnungsmäßigkeit dennoch vorzuschreiben.
Ist absehbar, daß nur eine kurze Unterbrechung der Arbeit erforderlich ist, kann anstelle des Abmeldens auch die manuelle Aktivierung der Bildschirmsperre erfolgen.

M 3.20 Einweisung in die Bedienung von Schutzschränken
Nach der Beschaffung eines Schutzschrankes sind die Benutzer in die korrekte Bedienung einzuweisen. Dies sollte auch bei der Neuübertragung einer Aufgabe erfolgen, die die Nutzung des Schutzschrankes umfaßt. Dabei sind zumindest folgende Punkte zu vermitteln:

- Der korrekte Umgang mit dem Schloß des Schutzschrankes ist vorzuführen. Auf typische Fehler ist hinzuweisen, zum Beispiel das Nichtverwerfen von Codeschlössern. Die Regelungen zur Schlüsselverwaltung, Schlüsselhinterlegung und Vertretungsregelung sind aufzuzeigen. Insbesondere ist einzufordern, daß der Schutzschrank bei Nichtbenutzung, auch kurzfristiger Art, verschlossen wird.

- Die Tastatur eines Servers ist unbedingt im Serverschrank aufzubewahren, damit nicht unberechtigte Konsol-Eingaben erfolgen können.

- Im Falle eines Serverschrankes ist darauf hinzuweisen, daß unnötige brennbare Materialien (Ausdrucke, überzählige Handbücher, Druckerpapier) nicht im Serverschrank aufbewahrt

werden sollen.

- Datensicherungsträger des Servers sollten in einem anderen Brandabschnitt gelagert werden. Eine Aufbewahrung im Serverschrank ist daher ungeeignet und nur dann zulässig, wenn ein Doppel der Datensicherungsbestände in einem anderen Brandabschnitt ausgelagert ist.
- Wird ein klimatisierter Serverschrank eingesetzt, sollten die Öffnungszeiten des Serverschrankes minimiert werden. Gegebenenfalls ist sporadisch zu kontrollieren, ob im Serverschrank Wasser kondensiert ist.

H.4 Maßnahmenkatalog Hardware und Software

M 4.1 Paßwortschutz für PC und Server
Der Paßwortschutz eines IT-Systems soll gewährleisten, daß nur solche Benutzer einen Zugriff auf die Daten und IT-Anwendungen erhalten, die eine entsprechende Berechtigung nachweisen. Unmittelbar nach dem Einschalten des IT-Systems muß der Berechtigungsnachweis erfolgen. Kann der Benutzer die erforderliche Berechtigung nicht nachweisen, so verhindert der Paßwortschutz den Zugriff auf das IT-System.
Realisiert werden kann der Paßwortschutz an einem IT-System auf verschiedene Weise:

- Die meisten BIOS-Varianten bieten die Installation eines Boot-Paßwortes an. Bei Fehleingaben wird der Bootvorgang nicht fortgesetzt. Ein BIOS-Paßwort ist nicht schwer zu überwinden, schützt aber vor Zufallstätern, sollte also zumindest überall da eingesetzt werden, wo keine besseren Zugriffsschutzmechanismen vorhanden sind (siehe auch unten: BIOS-Paßwortschutz).
- Gute Betriebssysteme enthalten bereits Zugriffsschutzmechanismen. In den meisten Fällen müssen diese aber noch aktiviert werden, beispielsweise durch die Vergabe von Paßwörtern für alle Benutzer. Näheres hierzu findet sich in den betriebssystem-spezifischen Bausteinen.
- Es wird Zusatzhardware oder -software installiert, die vor dem eigentlichen Start des Rechners ein Paßwort abfragt und bei falscher Paßworteingabe die weitere Nutzung des IT-Systems verhindert.

Für den Umgang mit Paßwörtern sind die Hinweise in M 2.11 - Regelung des Paßwortgebrauchs zu beachten, insbesondere ist das Paßwort regelmäßig zu ändern.

BIOS-Paßwortschutz
Moderne BIOS-Varianten bieten eine Vielzahl von Sicherheitsmechanismen an, mit denen sich die Benutzer oder die Systemadministration vertraut machen sollten. Auf keinen Fall sollten aber ungeschulte Benutzer BIOS-Einträge verändern, da hierdurch schwerwiegende Schäden verursacht werden können.

- Paßwortschutz: Bei den meisten BIOS-Varianten kann ein Paßwortschutz aktiviert werden. Dieser kann verhältnismäßig einfach überwunden werden, sollte aber auf jeden Fall benutzt werden, wenn keine anderen Zugriffsschutzmechanismen zur Verfügung stehen. Meist kann ausgewählt werden, ob das Paßwort vor jedem Rechnerstart oder nur vor Zugriffen auf die BIOS-Einstellungen überprüft werden soll. Teilweise können sogar verschiedene Paßwörter für diese Prüfungen benutzt werden. Um zu verhindern, daß Unbefugte die BIOS-Einstellungen ändern, sollte das Setup- oder Adminstrator-Paßwort immer aktiviert werden.
  Mit einigen (leider wenigen) BIOS-Varianten kann zusätzlich der Zugriff auf die Diskettenlaufwerke durch ein Paßwort geschützt werden. Dies sollte benutzt werden, um das unbefugte Aufspielen von Software oder das unbemerkte Kopieren von Daten zu verhindern.

- Boot-Reihenfolge: Als Bootfolge sollte immer „C:, A:“ eingestellt werden. Dies schützt vor der Infektion mit Boot-Viren, falls versehentlich eine Diskette im Laufwerksschacht vergessen wird, und spart Zeit und schont das Diskettenlaufwerk.

- Virenschutz, Virus-Warnfunktion: Wird diese Funktion aktiviert, verlangt der Rechner vor einer Veränderung des Bootsektors eine Bestätigung, ob diese durchgeführt werden darf.

M 4.2 Bildschirmsperre

Unter einer Bildschirmsperre versteht man die Möglichkeit, die auf dem Bildschirm aktuell vorhandenen Informationen zu verbergen. Die Aktivierung der Bildschirmsperre sollte erfolgen, wenn der Benutzer den Arbeitsplatz für eine nur kurze Zeit verläßt. Als weiteres Leistungsmerkmal sollte die Bildschirmsperre eine automatische Aktivierung bei längerer Pausenzeit aufweisen. Verfügt das Software-Produkt außerdem über eine Paßwort-Abfrage, wird bei der Abwesenheit des IT-Benutzers zusätzlich ein Zugriffsschutz für das IT-System gewährleistet.
Eine paßwortunterstützte Bildschirmsperre wird von MS-Windows 3.x als Bildschirmschoner angeboten. Die Dokumentation dazu sagt jedoch: Ist eine Non-Windows-Anwendung die aktuelle Anwendung, wird der Bildschirmschoner nicht automatisch aktiviert, unabhängig davon, ob die Anwendung in einem Fenster, von der MS-DOS-Befehlszeile oder als Symbol ausgeführt wird.Ünter Windows 95 aktiviert sich der Bildschirmschoner jedoch auch bei DOS-Anwendungen. Neben MS-Windows gibt es weitere Produkte, die einen paßwortunterstützenden Bildschirmschoner anbieten. Vor dem Einsatz solcher Produkte ist zu überprüfen, ob die Bildschirmsperre unter allen Applikationen funktioniert.
Unter Unix kann eine Bildschirmsperre mit Programmen wie lock oder - unter X-Windows - lockscreen erfolgen.

M 4.3 Regelmäßiger Einsatz eines Viren-Suchprogramms

Zum Schutz vor Computer-Viren können unterschiedliche Wirkprinzipien genutzt werden. Programme, die Speichermedien nach bekannten Viren durchsuchen, haben sich in der Vergangenheit als effektivstes und wirksamstes Mittel in der Viren-Bekämpfung erwiesen. Von Vorteil ist, daß neu erhaltene Software oder Datenträger schon vor dem ersten Einsatz geprüft werden kön-

nen. Man kann daher eine Infektion mit bekannten Computer-Viren grundsätzlich vermeiden. Ein weiterer Vorteil ist, daß man durch das Viren-Suchprogramm eine genauere Information über den jeweils entdeckten Virus erhält. Die bekannten Viren sind durch Spezialisten analysiert worden, so daß man weiß, ob und welche Schadensfunktionen vorhanden sind. Ein gutes Viren-Suchprogramm muß daher nicht nur in der Lage sein, viele Viren zu finden, sondern sie auch möglichst exakt identifizieren.
Zu beachten ist, daß Viren-Suchprogramme mit der Zeit ihre Wirksamkeit verlieren, da sie nur die zu ihrem Erstellungszeitpunkt bekannten Computer-Viren berücksichtigen, neu hinzugekommene jedoch meist nicht erkennen können. Daher ist eine regelmäßige Aktualisierung des Viren-Suchprogramms erforderlich.

Ebenso wie andere Programme können sie durch Aufruf (transient) oder im Hintergrund (resident) genutzt werden. Die Betriebsart des Suchprogramms hat entscheidenden Einfluß auf die Akzeptanz bei den Anwendern und damit auf die tatsächlich erreichte Schutzfunktion.
Beim transienten Betrieb wird das Programm aufgerufen, durchsucht die eingestellten Teile des Computers, beendet seine Arbeit danach und macht den Speicher wieder frei. Meist löst der Anwender den Aufruf aus. Diese Programme waren lange Zeit die wichtigsten Hilfsmittel im Kampf gegen Viren. Beim residenten Betrieb wird das Viren-Schutzprogramm beim Start des Rechners in den Speicher geladen und verbleibt dort aktiv bis zum Ausschalten. Es verrichtet seine Tätigkeit, ohne daß der Anwender dabei mitwirkt, er kann inzwischen seine eigentliche Arbeit, z.B. das Schreiben von Texten, ausführen. Diese Betriebsart hat erst in jüngster Zeit mit dem verstärken Einsatz von Windows-Programmen Bedeutung erlangt. Bei Windows arbeitet die Verwaltung des Speichers effektiver als unter dem zuvor vorwiegend genutzten MS-DOS. Die rasante technische Entwicklung hin zu größeren Speicherkapazitäten der Computer unterstützte diesen Trend. Unter MS-DOS waren speicherresidente Viren-Suchprogramme in ihrer Leistungsfähigkeit von den Herstellern oft gegenüber den transienten vermindert, um Speicherplatz zu sparen. Der wichtigste Vorteil des residenten Betriebes ist, daß die Sicherheitsmaßnahme (Viren-Suche) unabhängig vom Anwender wirksam ist. Dies erhöht die Sicherheit. Gleichzeitig führt es zu besserer Akzeptanz bei den Anwendern, da diese sich nicht um den Virenschutz zu kümmern brauchen. Sie merken meist nicht einmal, daß im Hintergrund das Schutzprogramm läuft, solange kein Virus gefunden wird. Im letzteren Falle wird die betroffene Datei für den Zugriff gesperrt, d. h., der Anwender kann sie nicht verwenden, solange das Schutzprogramm aktiv ist. Der Einsatz speicherresidenter Viren-Schutzprogramme unter WINDOWS ist die derzeitig beste Möglichkeit, sich vor Computer-Viren zu schützen, weil jede Datei vor deren Nutzung (Öffnen zur Bearbeitung, Kopieren, Drucken, Entpacken usw.) geprüft und bei Viren-Befall gesperrt werden kann. Welche Dateiarten überprüft werden, sind bei den meisten Produkten einstellbar. Einige residente Programme reagieren auch auf Aktionen, die für Computer-Viren typisch sind, z. B. das Lesen und spätere Zurückschreiben von Programmdateien. Dies kommt in der üblichen Praxis nicht vor, ist aber Voraussetzung bei der Infektion. Daher ist auch der Ausdruck Viren-Wächter für diese Programme üblich.

Ein weitere präventive Maßnahme ist der Einsatz von Checksummen-Prüfprogrammen. Hierbei werden zum Schutz vor Veränderung von den zu prüfenden Dateien oder Systembereichen

(z.B. Boot- und Partition-Sektor) Prüfsummen berechnet, die regelmäßig kontrolliert werden. Auf diese Weise können nicht nur Verseuchungen mit bisher unbekannten Computer-Viren erkannt werden, sondern auch andere unberechtigte Veränderungen an Dateien. Verhaltensregeln bei Auftreten eines Computer-Virus sind unter M 6.23 Verhaltensregeln bei Auftreten eines Computer-Virus beschrieben.

Als vorbeugende Maßnahme gegen Virenbefall bieten BIOS-Versionen die Möglichkeit, über das CMOS-Setup die Boot-Reihenfolge zu vertauschen (erst C:, dann A:) oder das Booten von Diskette ganz zu unterbinden. Ebenso kann die Unterteilung der Festplatte in mehrere Partitionen die Rekonstruktion von Daten nach einem Virus-Schaden erleichtern (Anmerkung: Dies gilt auch bei einem Headcrash).

M 4.4 Verschluß der Diskettenlaufwerkschächte
Mittels spezieller Einschiebvorrichtungen kann ein Diskettenlaufwerkschacht verschlossen werden. Damit kann erreicht werden,

- daß der PC oder der Server nicht mehr von Diskette unkontrolliert gebootet werden kann,
- daß Software nicht unkontrolliert eingespielt werden kann und
- daß Daten nicht mehr unberechtigt auf Diskette kopiert werden können.

Insbesondere sollten daher die bootfähigen Diskettenlaufwerke verschlossen werden.
Bei der Beschaffung von Diskettenschlössern ist darauf zu achten, daß herstellerseitig eine möglichst große Anzahl unterschiedlicher Schlüssel angeboten werden. Andererseits erfordert dies organisatorische Maßnahmen im Bereich der Schlüsselverwaltung. Quelle: Sicherheitsberater 11/95; Order PC
Ersatzweise kann auch der Ausbau der Diskettenlaufwerke erwogen werden.

M 4.5 Protokollierung der TK-Administrationsarbeiten
Alle Eingaben, die über die Wartungseingänge der TK-Anlage vorgenommen werden, sollten protokolliert werden. Dies kann entweder über einen Protokolldrucker und/oder auf anderen Speichermedien erfolgen. Auf die erzeugten Protokolldateien darf der TK-Anlagenadministrator kein Schreibrecht besitzen. Die vom Drucker erzeugten Ausdrucke sollten laufende Seitenzahlen besitzen, die einzelnen Protokollmeldungen laufende Meldungsnummern.
Das BSI hat in Zusammenarbeit mit dem Zentralverband der Elektro- und Elektronikindustrie (ZVEI) einen Katalog von Anforderungen erarbeitet, der auch eine verbesserte Protokollierung beinhaltet. Dieser Katalog soll bei der Beschaffung neuer TK-Anlagen für Bundesbehörden zum Tragen kommen. Bei vorhandenen TK-Anlagen sollte überprüft werden, inwieweit die Hersteller solche verbesserten Möglichkeiten als Update anbieten können.

M 4.6 Revision der TK-Anlagenkonfiguration (Soll-Ist-Abgleich)
Nach jeder Konfigurationsveränderung, z. B. der Freigabe einer Berechtigung für einen Teilnehmer, sollte diese in eine Ist-Bestandsliste eingetragen werden. Diese Liste kann per Hand oder

automatisiert geführt werden. In regelmäßigen (nicht unbedingt gleichmäßigen) Abständen (z. B. alle 6 Monate) sollte diese Ist-Bestandsliste zumindest stichprobenartig mit der Realität verglichen werden. Unstimmigkeiten sind mit Hilfe der Protokolle aufzuklären. Insbesondere sollte kontrolliert werden, ob

- alle nicht vergebenen Rufnummern auch wirklich nicht eingerichtet sind,
- verbotene Berechtigungen auch nirgendwo vergeben sind,
- deaktivierte Leistungsmerkmale auch wirklich inaktiv sind,
- deaktivierte Dial-In-Funktionen auch wirklich inaktiv sind.

Das BSI hat in Zusammenarbeit mit dem Zentralverband der Elektro- und Elektronikindustrie (ZVEI) einen Katalog von Anforderungen erarbeitet, der unter anderem auch Forderungen nach einer besseren Unterstützung von Revisionstätigkeiten beinhaltet. Dieser Katalog soll bei der Beschaffung neuer TK-Anlagen für Bundesbehörden zum Tragen kommen. Bei vorhandenen TK-Anlagen sollte überprüft werden, inwieweit die Hersteller solche verbesserten Möglichkeiten als Update anbieten können.

M 4.7 Änderung voreingestellter Paßwörter
Viele IT-Systeme, TK-Anlagen und Netzkoppelelemente (bspw. ISDN-Router, Sprach-Daten-Multiplexer etc.) besitzen nach der Auslieferung durch den Hersteller noch voreingestellte Standardpaßwörter. Diese sollten als erstes durch individuelle Paßwörter ersetzt werden. Hierbei sind die einschlägigen Regeln für Paßwörter zu beachten (vgl. M 2.11 Regelung des Paßwortgebrauchs).
Achtung: Bei einigen TK-Anlagen werden vorgenommene Änderungen der Konfiguration nur im RAM abgelegt. Dies gilt auch für Paßwortänderungen. Daher ist nach einer solchen Operation stets eine Datensicherung vorzunehmen und eine neue Sicherungskopie zu erstellen. Unterbleibt dies, so ist nach einem Restart"der Anlage wieder das Standardpaßwort gültig. Weiterhin sollte überprüft werden, ob nach Einrichten eines neuen Paßworts das Standardpaßwort tatsächlich seine Gültigkeit verloren hat und nicht weiterhin für den Systemzugang genutzt werden kann.

M 4.8 Schutz des TK-Bedienplatzes
Sollte die TK-Anlage mit Hilfe eines Bedien-PC administriert werden, so ist dieser mindestens mit den für PCs üblichen Schutzmaßnahmen, siehe Kapitel 5.1 DOS-PC (ein Benutzer), zu versehen.
Optional:
Sollte die TK-Anlage nicht über ausreichende Sicherheitsfunktionen für Rechteverwaltung und Zugangsschutz verfügen, so kann überlegt werden, marktgängige Zusatzeinrichtungen (Portcontroller) einzusetzen. Mit Hilfe solcher Geräte können sichere Identifizierungs- und Authentisierungsverfahren realisiert werden.

M 4.9 Einsatz der Sicherheitsmechanismen von X-Windows
Release 5 der X-Window-Software bietet nur wenige Maßnahmen, um die Sicherheit bei der

Übertragung von Daten zwischen dem X-Server und dem X-Client zu erhöhen, so daß der Einsatz von X-Window-Software nur in einer sicheren Umgebung empfohlen werden kann.

- Rechnerspezifische Zugriffskontrolle: Auf jedem X-Server gibt es eine Liste zugelassener Rechner, die mit dem Befehl xhost verändert werden kann. Sie muß auf jeden Fall auf die Rechner beschränkt bleiben, die einen Zugriff auf den X-Server benötigen, und es sollte auf keinen Fall ein globaler Zugriff mit xhost + ermöglicht werden. Darüber hinaus muß beachtet werden, daß jeder Benutzer auf einem der zugelassenen Rechner uneingeschränkten Zugriff auf den X-Server hat.

- Benutzerspezifische Zugriffskontrolle: Der X-Server Prozeß läßt sich so konfigurieren, daß bei einem Login (z. B. mit Hilfe von xdm) ein Schlüssel generiert wird, der zur Authentisierung bei einer Übertragung zwischen Client und Server benutzt wird. Dieser Schlüssel (MAGIC COOKIE) wird im Heimatverzeichnis des Benutzers in der Datei .Xauthority abgelegt und kann mit Hilfe des Befehls xauth an den X - Client übertragen werden. Während allerdings der MIT-MAGIC-COOKIE-Mechanismus nur als eine Art Paßwort angesehen werden muß, das bei seiner Übertragung abgehört werden kann, bietet ein in Verbindung mit NIS angebotener und mit einer DES-Verschlüsselung arbeitender Mechanismus mehr Sicherheit und sollte deshalb möglichst eingesetzt werden.

Mit einem Zusatzprogramm können unter X-Windows die Tastendrücke eines entfernten Rechners in Klarschrift übersetzt und eingesehen werden. Bei der Benutzung des Programms xterm kann das Weiterleiten von Tastendrücken verhindert werden, indem verhindert wird, daß KeyPress-Events, welche es bekommt, noch an andere Applikationen weitergeleitet werden. Dafür muß die secure keyboard-Option über das xterm-Menü eingeschaltet werden, so daß das entsprechende Fenster exklusiven Zugriff auf die Tastatur hat.

M 4.10 Paßwortschutz für TK-Endgeräte Endgeräte, insbesondere Telefone, können oft mit einem Paßwortschutz versehen werden. Bei aktiviertem Paßwortschutz stehen Leistungsmerkmale, wie Rufumleitung, Heranholen von Rufen etc. erst nach Eingabe des Paßwortes zur Verfügung. Ohne die Kenntnis des Paßwortes können in der Regel nur interne Gespräche geführt werden. Um einen Mißbrauch dieser Leistungsmerkmale zu verhindern, sollte von dieser Möglichkeit des Paßwortschutzes immer Gebrauch gemacht werden.

M 4.11 Absicherung der TK-Anlagen-Schnittstellen
Die Schnittstellen einer TK-Anlage, über die Administrationstätigkeiten ausgeführt werden können, stellen schützenswerte Punkte dar. Sie sollten daher besonders abgesichert werden. Über unbenutzte oder ungesicherte Schnittstellen können von Unbefugten, etwa unter Zuhilfenahme eines Laptops, Manipulationen am System durchgeführt werden. Der Paßwortschutz auf einen TK-Bedienplatz oder PC-Gateway wäre in einem solchen Fall wirkungslos. Ziel ist es also, dies zu verhindern, zumindest aber den Versuch erkennbar zu machen. Aus diesem Grund sollten die benutzten Schnittstellen gut verschraubt und ggf. zusätzlich verplombt werden. Unbenutzte Schnittstellen können durch verschraubte und verplombte Abschlußkappen gesichert werden.

M 4.12 Sperren nicht benötigter Leistungsmerkmale

Der Umfang der verfügbaren Leistungsmerkmale sollte auf das notwendige Minimum beschränkt werden. Die Software nicht benötigter Leistungsmerkmale sollte, wenn möglich, von der Anlage entfernt werden. Da dies in vielen Fällen nicht möglich ist, können diese Leistungsmerkmale nur gesperrt (deaktiviert) werden. Von Zeit zu Zeit sollte überprüfte werden, ob diese Leistungsmerkmale auch wirklich gesperrt sind.

M 4.13 Sorgfältige Vergabe von IDs

In Unix-Systemen werden anhand von Benutzer- und Gruppenkennungen von Prozessen / Dateien unter anderem Verursacher von Aktionen festgestellt und Rechte vergeben. Daher ist eine sorgfältige Vergabe dieser Kennungen erforderlich.
Jeder Login-Name, jede Benutzer-ID (UID) und jede Gruppen-ID (GID) darf nur einmal vorkommen. Auch nach dem Löschen eines Benutzers bzw. einer Gruppe sollen Login-Name und UID bzw. GID für eine bestimmte Zeit nicht neu vergeben werden.
Jeder Benutzer muß Mitglied mindestens einer Gruppe sein. Jede in der Datei /etc/passwd vorkommende GID muß in der Datei /etc/group definiert sein.
Jede Gruppe sollte nur die Benutzer enthalten, die unbedingt notwendig sind. Dieses ist insbesondere für die Systemgruppen (wie root, sys, bin, adm, news, uucp, nuucp oder daemon) wichtig.
Logins mit UID 0 (Super-User) dürfen außer für den Systemadministrator root nur für administrative Logins nach vorher festgelegten Regeln vergeben werden (siehe M 2.33 Aufteilung der Administrationstätigkeiten unter Unix).
Es ist sinnvoll, für Login-Namen und UIDs / GIDs Namenskonventionen festzulegen.
Die Dateien /etc/passwd und /etc/group sollten nicht mit Editoren bearbeitet werden, da Fehler die Systemsicherheit stark beeinträchtigen können. Es sollten ausschließlich die entsprechenden Administrationstools benutzt werden, die allerdings sehr systemspezifisch sind.

M 4.14 Obligatorischer Paßwortschutz unter Unix

Der Paßwortschutz für jeden Account auf einem Unix-Rechner stellt sicher, daß nur ein berechtigter Benutzer sich unter seinem Login-Namen einloggen kann, indem nach Eingabe des Login-Namens eine Authentisierung durch Eingabe des Paßworts erfolgt.
Bei der Verwendung von Paßwörtern für Benutzer und Gruppen sind die unter M 2.11 Regelung des Paßwortgebrauchs beschriebenen Regeln zu beachten. Es muß beachtet werden, daß bei einigen Systemen nur eine begrenzte Zeichenanzahl bei der Paßwort-Prüfung berücksichtigt wird. Zur Realisierung dieser Maßnahmen sollten entsprechende Programmversionen von passwd (teilweise Public Domain), die die Einhaltung dieser Regeln sicherstellen, oder administrative Maßnahmen, z. B. Shellskripts und entsprechende cron-Einträge, benutzt werden.
Die Paßwörter sollen nicht in der allgemein lesbaren Datei /etc/passwd, sondern in einer für die Benutzer nicht lesbaren shadow-Paßwortdatei gespeichert sein.
Die Datei /etc/passwd ist regelmäßig auf Benutzerkennungen ohne Paßwort zu untersuchen. Wird eine solche gefunden, ist der Benutzer zu sperren. Ist für Gruppen Paßwortzwang vereinbart worden, so ist entsprechend die Datei /etc/group zu prüfen. Es empfiehlt sich jedoch, für Gruppen keine Paßwörter zu vergeben und für jede Gruppe nur so wenig Benutzer wie

möglich einzutragen. Das Wechseln zwischen Gruppen, in denen der Benutzer eingetragen ist, wird dadurch erleichtert, und unberechtigtes Wechseln durch systematisches Ausprobieren von Paßwörtern mit Hilfe entsprechender Programme ist nicht möglich.

M 4.15 Gesichertes Login
Es sollte ein Login-Programm verwendet bzw. Optionen aktiviert werden, so daß die folgenden Maßnahmen durchgeführt werden können:

- Die Anzahl erfolgloser Login-Versuche wird beschränkt.
- Nach jedem erfolglosen Login-Versuch vergrößert sich die Wartezeit bis zur nächsten Login-Aufforderung. Nach einer bestimmten Anzahl von Fehlversuchen wird der Account und / oder das Terminal gesperrt. Dabei ist zu bedenken, daß dadurch nicht der Administrator ausgesperrt werden darf, es muß ihm an der Konsole eine Zugangsmöglichkeit offen bleiben (siehe auch M 1.32 - Geeignete Aufstellung von Konsole, Geräten mit austauschbaren Datenträgern und Druckern).
- Der Zeitpunkt des letzten erfolgreichen Logins wird dem Benutzer beim Login gemeldet.
- Erfolglose Login-Versuche werden dem Benutzer beim Login gemeldet. Eventuell sollte diese Meldung bei mehreren darauffolgenden Logins wiederholt werden.
- Der Zeitpunkt des letzten Logouts wird dem Benutzer beim Login gemeldet. Hierbei wird zwischen Logouts zu einem interaktiven Login und solchen zu einem nicht-interaktiven Login (Logout von Hintergrundprozessen) unterschieden.
- Für das Login über Netze, in denen Paßwörter unverschlüsselt übertragen werden, empfiehlt sich die zusätzliche Verwendung von Einmalpaßwörtern (siehe auch M 5.34 - Einsatz von Einmalpaßwörtern).

M 4.16 Zugangsbeschränkungen für Accounts und / oder Terminals
Der Account und / oder das Terminal eines Benutzers sollen außerhalb der offiziellen Arbeitszeit gesperrt werden. Soweit das nicht mit vertretbarem Aufwand möglich ist (zum Beispiel bei sehr unregelmäßigen oder häufig wechselnden Arbeitszeiten), sollte die Sperrung zumindest zu den Zeiten erfolgen, die grundsätzlich außerhalb der Arbeitszeit liegen.
Falls Mitarbeiter nur an einem bestimmten Terminal oder IT-System innerhalb des Netzes arbeiten, ist die Nutzung der Benutzer-Kennung und des dazugehörenden Paßwortes auf diesen Rechner zu beschränken, so daß ein Einloggen von einem anderen Rechner aus ausgeschlossen ist.
Unter Unix ist für Terminals der jeweilige Benutzer als Eigentümer des entsprechenden Gerätetreibers einzutragen. Sobald dieser sich ausgeloggt hat, sollte automatisch wieder root Eigentümer werden. Nur der jeweilige Benutzer sollte hierfür Leseberechtigung haben. Falls ein Benutzer Nachrichten (z.B. mit talk) von anderen Systembenutzern empfangen möchte, muß er ihnen Schreibberechtigung für den Gerätetreiber einräumen. Es ist zu überprüfen, ob dies unbedingt notwendig ist.

In PC-Netzen kann die Anzahl von gleichzeitigen Anmeldungen unter einem Account von mehreren PCs aus beschränkt werden. Zum Schutz vor dem unbemerktem Eindringen von Angreifern sollte verhindert werden, daß sich ein Benutzer an mehreren PCs gleichzeitig anmelden kann.

M 4.17 Sperren und Löschen nicht benötigter Accounts und Terminals
Accounts, die über einen längeren Zeitraum nicht benutzt werden, sollten gesperrt und später gelöscht werden. Unter Unix sind die entsprechenden Einträge in /etc/passwd, /etc/group und das Heimatverzeichnis des Benutzers zu löschen. Ebenso ist darauf zu achten, daß weitere Benutzereinträge in Dateien wie /etc/hosts, shadows, u.a. gelöscht werden. Die Daten des Heimatverzeichnisses sollten vorher gesichert werden. Bei der Sperrung bzw. auf jeden Fall vor dem Löschen eines Accounts sollte der betroffene Benutzer informiert werden. Beim Löschen von Accounts ist darauf zu achten, daß auch die Dateien des Benutzers gefunden werden, die nicht in seinem Heimatverzeichnis liegen. Solche Dateien müssen gelöscht oder anderen Benutzern zugeordnet werden. Weiterhin ist darauf zu achten, daß laufende Prozesse und noch anstehende Aufträge gelöscht werden, z. B. unter Unix in der crontab.
Ebenso sollten Terminals, die über einen längeren Zeitraum nicht benutzt werden, gesperrt und später entfernt werden.
Unter Unix sind vom System vorgegebene Logins (z.B. sys, bin, adm, uucp, nuucp, daemon und lp), die nicht benötigt werden, zu sperren, indem in das zugehörige Paßwortfeld in der Datei /etc/passwd z. B. LOCKEDëingetragen wird. Wenn ein neu einzurichtender Benutzer seinen Account nur für einen befristeten Zeitraum benötigt, sollte dieser nur befristet eingerichtet werden. Es kann vorteilhaft sein, Accounts grundsätzlich nur befristet einzurichten und in regelmäßigen Abständen (z.B. jährlich) bei Bedarf zu verlängern. Ist absehbar, daß ein Benutzer eines lokalen Netzes längere Zeit abwesend ist (Urlaub, Krankheit, Abordnung, ...), so sollte sein Account für diese Zeit im Netz-Server gesperrt werden, so daß das Arbeiten unter seiner Benutzerkennung für diese Zeit nicht mehr möglich ist. Jeder Benutzer sollte dem Netzadministrator Zeiten längerer Abwesenheit mitteilen.

M 4.18 Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus
Um das Aktivieren des Monitor-Modus und das Booten in den Single-User-Modus zu verhindern, sollten folgende Maßnahmen ergriffen werden:

- Wenn es (abhängig von der Unix-Variante und der zugrundeliegenden Hardware) möglich ist, muß zum Schutz des Unix-Servers ein BIOS-Paßwort vergeben werden.
- Beim Booten in den Single-User-Modus sollte das Super-User-Paßwort abgefragt werden, um Unberechtigten den Zugang zum Unix-Server zu erschweren.
- Wenn Tastaturschlösser vorhanden sind, sollten diese zum Schutz der Systemkonsole benutzt werden, um den Zugang zum Monitor-Modus zu verhindern.

Diese Maßnahme wird ergänzt durch folgende Maßnahmen:

- M 1.32 Geeignete Aufstellung von Konsole, Geräten für austauschbare Datenträger und Druckern
- M 4.21 Verhinderung des unautorisierten Erlangens von Administratorrechten

M 4.19 Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen
Die hier genannten Maßnahmen gelten für Dateien und Verzeichnisse, für die der Administrator zuständig ist, das heißt für solche, die entweder für alle Benutzer von Bedeutung sind oder die Administrationszwecken dienen. Es reicht nicht aus, die Rechte eines Programms zu überprüfen, es muß auch die Rechtevergabe aller Programme überprüft werden, die von diesem Programm aus aufgerufen werden (insbesondere zur Vermeidung Trojanischer Pferde). Die Attribute aller Systemdateien sollten möglichst so gesetzt sein, daß nur der Systemadministrator Zugriff darauf hat. Verzeichnisse dürfen nur die notwendigen Privilegien für die Benutzer zur Verfügung stellen.
Das s-Bit sollte nur gesetzt sein, wenn unbedingt erforderlich. Bei Shellskripts soll das s-Bit nicht gesetzt sein. Das s-Bit darf nur vom Administrator gesetzt werden, die Notwendigkeit hierfür ist zu begründen und zu dokumentieren.
In Verzeichnissen, in denen alle Benutzer Schreibrechte haben müssen (z.B. /tmp), soll das t-Bit (Sticky-Bit) gesetzt sein.

M 4.20 Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen
Die hier genannten Maßnahmen gelten für Dateien und Verzeichnisse eines Benutzers (incl. Mail-Dateien). Die Benutzer sollten die Attribute ihrer Dateien und Verzeichnisse so setzen, daß andere Benutzer nicht darauf zugreifen können. Wenn anderen Benutzern der Zugriff erlaubt werden soll, sollten entsprechende Benutzergruppen eingerichtet werden.
Für benutzerspezifische Konfigurationsdateien wie .profile, .exrc, .login, .cshrc sollte nur der jeweilige Eigentümer Rechte besitzen.
Auf Unix-Systemen haben diverse Programme benutzerspezifische Konfigurationsdateien wie .exrc, .emacs oder .mailrc, die nach Programmaufruf automatisch durchlaufen werden und Variablen und Optionen für den Benutzer setzen. Damit in diesen keine trojanischen Pferde installiert werden können, sollte nur der jeweilige Eigentümer Zugriffsrechte besitzen.
Die Datei .exrc wird gelesen, bevor die Editoren ex oder vi gestartet werden. Falls sich eine gleichnamige Datei im aktuellen Verzeichnis befindet, wird diese bei einigen Unix-Versionen ausgewertet. Alle eingesetzten Unix-Versionen müssen daraufhin überprüft werden, da damit auch die Ausführung von Betriebssystemkommandos bei jedem Editoraufruf möglich ist.
Das s-Bit sollte nur gesetzt sein, wenn unbedingt erforderlich. Bei Shellskripts soll das s-Bit nicht gesetzt sein. Das s-Bit sollte nur nach Einbeziehung des Administrators gesetzt werden, die Notwendigkeit hierfür ist zu begründen und zu dokumentieren.

umask:
Mit umask (user file creation mode mask) wird für jeden Benutzer festgelegt, welche Attribute zur Regelung der Zugriffsrechte eine von ihm neu angelegte Datei erhält. In den benutzerspezifischen Konfigurationsdateien wie /etc/profile oder den $HOME/.profile-Dateien sollte umask = 0027 (-rw-r——) oder umask = 0077 (-rw———-) eingestellt sein, damit die Dateiattribute für

neu angelegte Dateien nur dem Erzeuger (und evtl. der Gruppe) Zugriffsrechte geben.

Mail-Dateien:
Die Attribute der Mail-Dateien sollten regelmäßig daraufhin überprüft werden, ob nur der jeweilige Eigentümer auf die Dateien Zugriff hat.

M 4.21 Verhinderung des unautorisierten Erlangens von Administratorrechten
Durch den Befehl su kann jeder Benutzer Super-User-Rechte erlangen, wenn er das entsprechende Paßwort besitzt. Da die Anzahl fehlerhafter Versuche bei su nicht beschränkt ist, besteht ein erhöhtes Risiko, daß das Paßwort durch systematisches Probieren mit Hilfe entsprechender Programme herausgefunden wird. Deshalb sollte su nur für den Super-User zugänglich sein. Alternativ könnte ein modifiziertes su installiert werden, bei dem die Anzahl erfolgloser Versuche beschränkt ist, sich die Wartezeit bis zur nächsten su-Aufrufmöglichkeit nach jedem erfolglosen Login-Versuch vergrößert und nach einer bestimmten Anzahl von Fehlversuchen die Ausführmöglichkeit und / oder das Terminal gesperrt wird. Wenn das System es zuläßt, kann der Login-Name des Super-Users anders als root genannt werden.
Der Administrator darf nur von der Konsole aus arbeiten, um zu verhindern, daß bei einem Abhören der Leitung sein Paßwort bekannt wird. Unter Unix SVR4 z.B. kann dies erreicht werden, indem die Datei /etc/default/login entsprechend konfiguriert wird.
Bei BSD-Unix kann sich root nur an Terminals einloggen, die in der Datei /etc/ttytab als secure gekennzeichnet sind. Ist diese Option bei allen Terminals entfernt, kann sich ein Administrator an einem Terminal nur über das Kommando su als root einloggen. Es ist daher zu überlegen, das Kommando su auch für root nicht ausführbar zu machen.
Ist bei BSD-Unix die Konsole in der Datei /etc/ttytab als secure gekennzeichnet, wird kein Paßwort beim Hochfahren in den Single-User-Modus abgefragt, daher muß dieser Eintrag unbedingt entfernt werden.
Wenn ein Benutzer bzw. ein Benutzer-Programm eine Super-User-Datei (Dateien mit Eigentümer root und gesetztem s-Bit) ausführt, erhält dieser Benutzer bzw. dieses Programm bei der Ausführung Super-User-Rechte. Das ist für bestimmte Anwendungen erforderlich, kann aber unter Umständen auch mißbräuchlich benutzt werden. Deshalb ist darauf zu achten, daß nur die notwendigsten Programmdateien Super-User-Dateien werden und keine weiteren Super-User-Dateien von Dritten hinzugefügt werden.
Automatisches Mounten von Geräten für austauschbare Datenträger:
Mit sich auf dem gemounteten Laufwerk befindenden s-Bit-Programmen kann ein Benutzer Super-User-Rechte erlangen. Automatisches Mounten sollte daher restriktiv gehandhabt werden. Bei der Freigabe von Verzeichnissen, die von anderen Rechnern gemountet werden dürfen, sind die unter M 5.17 - Einsatz der Sicherheitsmechanismen von NFS beschriebenen Einschränkungen zu beachten. Es sollten insbesondere keine Verzeichnisse mit root-Rechten und nur bei Bedarf Verzeichnisse mit Schreibrechten freigegeben werden.
Diese Maßnahme wird ergänzt durch folgende Maßnahmen:

- M 1.32 Geeignete Aufstellung von Konsole, Geräten für austauschbare Datenträger und Druckern

- M 4.18 Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus

M 4.22 Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System

Mit den Unix-Befehlen ps, finger, who und (bei UNIX SVR4) listusers lassen sich Informationen über einen Benutzer (z.B. Arbeitsverhalten) ermitteln. Es ist zu überlegen, ob das Ausführen dieser Befehle für jeden Benutzer erlaubt sein soll (Datenschutz, Ausspähen von Login-Namen u.ä.). Im Zweifelsfall sollte der Zugriff auf diese Befehle beschränkt werden.
Beim Aufruf von Kommandos dürfen keine sensitiven Informationen als Parameter mit eingegeben werden, wie z.B. ein Paßwort, da andere Benutzer mit ps diese Angaben sehen können.

M 4.23 Sicherer Aufruf ausführbarer Dateien

Es muß sichergestellt werden, daß nur freigegebene Versionen ausführbarer Dateien und keine eventuell eingebrachten modifizierten Versionen (insbesondere Trojanische Pferde) aufgerufen werden.
Daher soll das jeweils aktuelle Arbeitsverzeichnis (.) nicht als Pfad in der Variable PATH enthalten sein. Ausführbare Dateien sollen nur in dafür vorgesehenen Verzeichnissen gespeichert sein. In den in einer PATH-Variable enthaltenen Verzeichnissen darf nur der Eigentümer Schreibrecht haben. Dieses soll regelmäßig überprüft werden. Bei Unix-Systemen mit IFS-Variable soll diese auf den Standardwert (space, tab und newline) gesetzt sein und insbesondere nicht auf „/“.

M 4.24 Sicherstellung einer konsistenten Systemverwaltung

In vielen komplexen IT-Systemen, z. B. unter Unix oder in einem Netz, gibt es eine Administratorrolle, die keinerlei Beschränkungen unterliegt. Unter Unix ist das der Super-User root, in einem Novell-Netz der SUPERVISOR. Durch fehlende Beschränkungen ist die Gefahr von Fehlern oder Mißbrauch besonders hoch.
Um Fehler zu vermeiden, soll unter dem Super-User-Login nur gearbeitet werden, wenn es notwendig ist; andere Arbeiten soll auch der Administrator nicht unter der Administrator-Kennung erledigen. Insbesondere dürfen keine Programme anderer Benutzer unter der Administrator-Kennung aufgerufen werden. Ferner sollte die routinemäßige Systemverwaltung (zum Beispiel Backup, Einrichten eines neuen Benutzers) nur menügesteuert durchgeführt werden können.
Durch Aufgabenteilung, Regelungen und Absprache ist sicherzustellen, daß Administratoren keine inkonsistenten oder unvollständigen Eingriffe vornehmen. Zum Beispiel darf eine Datei nicht gleichzeitig von mehreren Administratoren editiert und verändert werden, da dann nur die zuletzt gespeicherte Version erhalten bleibt.
Wenn die Gefahr des Abhörens von Leitungen zwischen Konsole und Terminals besteht, darf der Administrator nur an der Konsole arbeiten, damit keine Paßwörter abgehört werden können.
Für alle Administratoren sind zusätzliche Benutzer-Kennungen einzurichten, die nur über die eingeschränkten Rechte verfügen, die die Administratoren zur Aufgabenerfüllung außerhalb der Administration benötigen. Für Arbeiten, die nicht der Administration dienen, sollen die Ad-

ministratoren ausschließlich diese zusätzliche Benutzer-Kennungen verwenden.

M 4.25 Einsatz der Protokollierung im Unix-System
Die Protokollmöglichkeiten des einzelnen Unix-Systems sind einzusetzen und gegebenenfalls durch Shellskripts zu ergänzen.
Folgende Maßnahmen sollen ergriffen werden:

- Die Protokoll-Dateien sollen regelmäßig ausgewertet werden. Die Auswertung sollte nicht immer zum selben Zeitpunkt erfolgen, um zu verhindern, daß ein Angreifer diese Tatsache ausnutzt. Wenn z. B. der Administrator jeden Tag um 17.00 Uhr die Systemaktivitäten überprüft, kann ein Angreifer um 18.00 Uhr unbemerkt tätig werden.

- Soweit erforderlich, sollen sie gesichert werden, bevor sie zu groß oder vom System gelöscht werden.

- Die Datei-Attribute der Protokolldateien sollen so gesetzt sein, daß Unberechtigte keine Änderungen oder Auswertungen der Protokolle vornehmen können.

- Folgende Protokolldateien sollten mindestens erstellt und kontrolliert werden: Logins (auch Fehlversuche), Aufruf von su, Fehlerprotokollierungsdatei / Protokollierung wichtiger Vorgänge (errorlog), Administratortätigkeiten (insbesondere von root ausgeführte Befehle)

M 4.26 Regelmäßiger Sicherheitscheck des Unix-Systems
Unix-Betriebssysteme bieten standardmäßig verschiedene Sicherheitseigenschaften an. Diese können jedoch nur zum Erfolg führen, wenn sie sinnvoll eingesetzt werden. Die hierfür notwendigen Einstellungen sollen mit Hilfe von Tools automatisiert überprüft werden, um

- Inkonsistenzen innerhalb eines Unix-Systems erkennen und beseitigen zu können und

- den Systemverwalter in die Lage zu versetzen, das Unix-Betriebssystem unter optimaler Ausnutzung der gegebenen Sicherheitsmechanismen zu verwalten.

Diese Prüfung kann mit im Unix-System vorhandenen Programmen, selbsterstellten Shellskripts oder Public-Domain-Programmen erfolgen. Für einige Unix-Varianten sind auch kommerzielle Programme verfügbar.
Beispiele:

- /etc/pwck
  Mit diesem Befehl nimmt man eine Konsistenzprüfung der Datei /etc/passwd vor. Es wird überprüft, ob alle notwendigen Einträge vorgenommen wurden, ob das Login-Verzeichnis für den Benutzer existiert und ob das Login-Programm vorhanden ist. Ähnliche Funktionen beinhaltet der zusätzliche Befehl logins bei Unix SVR4, mit dem auch Accounts ohne Paßwort gefunden werden können.

- /etc/grpck
  Mit diesem Befehl nimmt man eine Konsistenzprüfung der Datei /etc/group vor. Es wird überprüft, ob alle notwendigen Einträge vorgenommen wurden, ob alle Mitglieder einer Gruppe auch in der Benutzerpaßwortdatei vorhanden sind und ob die Gruppennummer mit der dort angegebenen übereinstimmt.

- tripwire
  Mit diesem Public-Domain-Programm können Integritätsprüfungen von Dateien durchgeführt werden. Dazu werden Prüfsummen über Dateien gebildet und in einer Datenbank gespeichert.

- cops
  Dieses Public-Domain-Programm dient zur Überprüfung der Sicherheit von Unix-Systemen, z. B. werden verschiedene Systemeinstellungen, Zugriffsrechte, SUID-Dateien etc. überprüft und potentielle Sicherheitslücken aufgezeigt.

- tiger
  Mit diesem Public-Domain-Programm können Unix-Systeme ähnlich wie mit cops auf Sicherheitslücken überprüft werden.

- SATAN
  Mit diesem Public-Domain-Programm kann die Netz-Sicherheit analysiert werden. Es überprüft vernetzte Unix-Systeme auf bekannte, aber oftmals nicht beseitigte Schwachstellen.

- crack
  Mit diesem Public-Domain-Programm überprüft man, ob zu einfache, leicht erratbare Paßwörter vorhanden sind.

M 4.27 Paßwortschutz am tragbaren PC

Jeder tragbare PC sollte mit einem Paßwortschutz versehen werden, der verhindert, daß der PC unberechtigt benutzt werden kann. Die im Umgang mit Paßwörtern zu beachtenden Regeln sind in M 2.11 - Regelung des Paßwortgebrauchs aufgeführt worden. Bei modernen tragbaren PCs sollte das BIOS-Bootpaßwort aktiviert werden, wenn dessen Nutzung möglich ist. Erst nach Eingabe des korrekten Bootpaßwortes wird der Rechner dann hochgefahren. Ist keine Paßwortroutine installiert, sollte, wenn keine Verschlüsselung der Daten erfolgt, die Speicherung von schutzbedürftigen Daten auf der Festplatte verboten und deren Speicherung stattdessen nur auf Disketten zugelassen werden. Diese Disketten sind dann getrennt vom tragbaren PC aufzubewahren, zum Beispiel in der Brieftasche.
Einige tragbare PCs sehen auch die Möglichkeit einer Pausenschaltung vor, die über eine spezielle Tastenkombination aktiviert werden kann. Erst nach Eingabe des entsprechenden Paßwortes ist die weitere Nutzung des tragbaren PC möglich. Ist eine Pausenschaltung vorhanden, so sollte sie für kurze Arbeitsunterbrechungen genutzt werden. Ist es absehbar, daß die Unterbrechung länger dauert, ist der Rechner auszuschalten.

M 4.28 Software-Reinstallation bei Benutzerwechsel eines tragbaren PC
Wechselt der Benutzer eines tragbaren PC, so muß sichergestellt sein, daß auf dem PC weder schutzbedürftige Daten noch Computer-Viren vorhanden sind. Die Löschung von Daten kann durch vollständiges Überschreiben oder mit Hilfe spezieller Löschprogramme vorgenommen werden. Ein aktuelles Viren-Suchprogramm muß anschließend zum Einsatz kommen. Beide Vorgänge müssen für alle benutzen Datenträger (Festplatte, Diskette) durchgeführt werden.
Es empfiehlt sich jedoch, die Festplatte des tragbaren PC neu zu formatieren und anschließend die erforderliche Software und Daten neu aufzuspielen. Beim Formatieren von DOS-Datenträgern ist darauf zu achten, daß der Parameter /U (in DOS 6.2 enthalten) benutzt wird, damit das Formatieren nicht über den Befehl unformat wieder rückgängig gemacht werden kann.

M 4.29 Einsatz eines Verschlüsselungsproduktes für tragbare PCs
Um zu verhindern, daß aus einem trotz aller Vorsichtsmaßnahmen gestohlenen tragbaren PC schutzbedürftige Daten ausgelesen werden, ist der Einsatz eines Verschlüsselungsprogramms zu überlegen. Mit Hilfe der marktgängigen Produkte ist es möglich, die betreffenden Daten dergestalt zu verschlüsseln, daß nur derjenige, der über den geheimen Schlüssel verfügt, in der Lage ist, die Daten zu lesen und zu gebrauchen.
Die Sicherheit der Verschlüsselung hängt dabei von drei verschiedenen Punkten zentral ab:

- Der verwendete Verschlüsselungsalgorithmus muß so konstruiert sein, daß es ohne Kenntnis des verwendeten Schlüssels nicht möglich ist, den Klartext aus dem verschlüsselten Text zu rekonstruieren. Nicht möglich bedeutet dabei, daß der erforderliche Aufwand zum Brechen des Algorithmus bzw. zum Entschlüsseln in keinem Verhältnis steht zum dadurch erzielbaren Informationsgewinn.

- Der Schlüssel ist geeignet zu wählen. Nach Möglichkeit sollte ein Schlüssel zufällig erzeugt werden. Wenn es möglich ist, einen Schlüssel wie ein Paßwort zu wählen, sollten die diesbezüglichen Regeln aus M 2.11 - Regelung des Paßwortgebrauchs beachtet werden.

- Der Verschlüsselungsalgorithmus (das Programm), der verschlüsselte Text und die Schlüssel dürfen nicht zusammen auf einem Datenträger gespeichert werden. Es bietet sich an, den Schlüssel einzeln aufzubewahren. Dies kann dadurch geschehen, daß er auf einer Pappkarte in Form einer Scheckkarte aufgeschrieben und anschließend wie eine Scheckkarte im Portemonnaie aufbewahrt wird. Werden die Schlüssel auf Disketten gespeichert, so sollten die Disketten getrennt vom tragbaren PC aufbewahrt werden (z.B. in der Brieftasche).

Eine Verschlüsselung kann online oder offline vorgenommen werden. Online bedeutet, daß sämtliche Daten der Festplatte (bzw. einer Partition) verschlüsselt werden, ohne daß der Benutzer dies aktiv veranlassen muß. Eine Offline-Verschlüsselung wird explizit vom Benutzer initiiert. Er muß dann auch entscheiden, welche Dateien verschlüsselt werden sollen.
Für den Bereich der öffentlichen Verwaltung kann das BSI für den Einsatz auf stationären und tragbaren PCs ein Offline-Verschlüsselungsprogramm unter gewissen Randbedingungen zur Verfügung stellen, das den Sicherheitsanforderungen im Bereich des mittleren Schutzbedarfs genügt. Ein Anforderungsvordruck befindet sich im Teil Hilfsmittel des vorliegenden

IT-Grundschutzhandbuchs.

M 4.30 Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen

Einige der Standardprodukte im PC-Bereich bieten eine Reihe von nützlichen IT-Sicherheitsfunktionen, deren Güte im einzelnen unterschiedlich sein kann, aber Unbefugte behindern bzw. mögliche Schäden verringern. Im folgenden seien fünf dieser Funktionen kurz erläutert:

- Paßwortschutz bei Programmaufruf: das Programm kann nur gestartet werden, wenn vorher ein Paßwort korrekt eingegeben wurde. Dies verhindert die unberechtigte Nutzung des Programms.

- Zugriffsschutz zu einzelnen Dateien: das Programm kann nur dann auf eine geschützte Datei zugreifen, wenn das mit dieser Datei verknüpfte Paßwort korrekt eingegeben wird. Dies verhindert den unerlaubten Zugriff mittels des Programms auf bestimmte Dateien.

- Automatische Speicherung von Zwischenergebnissen: das Programm nimmt eine automatische Speicherung von Zwischenergebnissen vor, so daß ein Stromausfall nur noch die Datenänderungen betrifft, die nach dieser automatischen Speicherung eingetreten sind.

- Automatische Sicherung der Vorgängerdatei: wird eine Datei gespeichert, zu der im angegebenen Pfad eine Datei gleichen Namens existiert, so wird die zweite Datei nicht gelöscht, sondern mit einer anderen Kennung versehen. Damit wird verhindert, daß versehentlich eine Datei gleichen Namens gelöscht wird.

- Verschlüsselung von Dateien: das Programm ist in der Lage, eine Datei verschlüsselt abzuspeichern, so daß eine unbefugte Kenntnisnahme verhindert werden kann. Die Inhalte der Datei sind damit nur denjenigen zugänglich, die über den verwendeten geheimen Kryptierschlüssel verfügen.

- Automatisches Anzeigen von Makros in Dateien: diese Funktion soll das unbeabsichtigte Ausführen von Makros verhindern (Makro-Viren).

Je nach eingesetzter Software und damit vorhandenen Zusatzsicherheitsfunktionen kann der Einsatz dieser Funktionen sinnvoll sein. Für mobil eingesetzte IT-Systeme bietet sich insbesondere die Nutzung des Paßwortschutzes bei Programmaufruf und die automatischen Speicherung an.

M 4.31 Sicherstellung der Energieversorgung im mobilen Einsatz

Um die Energieversorgung eines tragbaren PC auch im mobilen Einsatz aufrechterhalten zu können, werden üblicherweise Batterien eingesetzt. Je nach Kapazität der Batterie und Bauweise des tragbaren PC reicht dies für einen beschränkten Zeitraum, z.B. einige Stunden, aus. Damit nach Abfall der Betriebsspannung keine Daten in flüchtigen Speichern verloren gehen, sollten einige Randbedingungen eingehalten werden:

- die Warnanzeigen des tragbaren PC (falls vorhanden), die den Spannungsabfall anzeigen, dürfen nicht ignoriert werden; es ist ggf. rechtzeitig eine Datensicherung durchzuführen,
- falls es absehbar ist, daß der mobile Einsatz längerfristig ist, sind aufladbare Batterien vorher nachzuladen und ggf. geladene Ersatzbatterien mitzuführen,
- bei der Übergabe eines mobilen IT-Systems ist der ausreichende Ladezustand der Batterien sicherzustellen.
- Das Ladenetzteil kann optional mitgeführt werden.

Es empfiehlt sich darüber hinaus, während der Nutzung des mobilen IT-Systems in kurzen Abständen die verarbeiteten Daten auf einem nichtflüchtigen Medium zu speichern. Dazu können auch automatische Datensicherungen in Standardprogrammen benutzt werden.

M 4.32 Physikalisches Löschen der Datenträger vor und nach Verwendung
Neben den in Maßnahme M 2.3 - Datenträgerverwaltung dargestellten Umsetzungshinweisen zur Löschung oder Vernichtung von Datenträgern sind für den Datenträgeraustausch folgende Punkte zu beachten:

Magnetische Datenträger, die für den Austausch bestimmt sind, sollten vor dem Beschreiben mit den zu übermittelnden Informationen physikalisch gelöscht werden. Es soll damit sichergestellt werden, daß keine Restdaten weitergegeben werden, für deren Erhalt der Empfänger keine Berechtigung besitzt.
Eine für den mittleren Schutzbedarf ausreichende physikalische Löschung kann erreicht werden, indem der komplette Datenträger oder zumindest die genutzten Bereiche mit einem bestimmten Muster überschrieben werden. Möglich ist auch eine Formatierung des Datenträgers, wenn diese nicht wieder rückgängig gemacht werden kann (Beispiel DOS Version 5.0: format /u). Es werden einige handelsübliche Produkte angeboten, die sogar die physikalische Löschung einzelner Dateien gewährleisten.
In der Regel sind die übertragenen Daten auch für den Empfänger schützenswert. Analog ist auch hier nach dem Wiedereinspielen der Daten eine physikalische Löschung des Datenträgers vorzusehen.
Auf den Einsatz von optischen Datenträger (hier: WORM) ist zum Zwecke des Datenaustausches dann zu verzichten, wenn sich darauf weitere, nicht für den Empfänger bestimmte Informationen befinden, die nicht gelöscht werden können.

M 4.33 Einsatz eines Viren-Suchprogramms vor und nach einer Datenübertragung
Neben den in M 2.3 - Datenträgerverwaltung dargestellten Umsetzungshinweisen sollte unmittelbar vor und unmittelbar nach einer Datenübertragung sowie beim Austausch von Datenträgern eine Virenüberprüfung durchgeführt werden (vgl. M 4.3 - Regelmäßiger Einsatz eines Viren-Suchprogramms). Es ist darauf zu achten, daß das eingesetzte Viren-Suchprogramm auch Makro-Viren (vgl. M 4.44 - Prüfung eingehender Dateien auf Makro-Viren) erkennen kann.
Ein Protokoll der Absender-Überprüfung sollte einem übermittelten Datenträger beigefügt oder

einer Datei, die elektronisch versandt wird, angehängt werden. Es empfiehlt sich, dieses Protokoll als Kopie zu verwahren. Der Empfänger hätte anhand dieses Protokolls einen ersten Eindruck von der Integrität der übermittelten Daten, was ihn jedoch nicht von einer erneuten Virenüberprüfung entbindet. Der Absender kann andererseits bei eventuellen Beschwerden bezüglich Virenbefall der Daten plausibel machen, daß ein Befall auf Seiten des Absenders unwahrscheinlich war.

M 4.34 Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
Werden vertrauliche Informationen oder Informationen mit hohem Integritätsanspruch übertragen und besteht eine gewisse Möglichkeit, daß diese Daten Unbefugten zur Kenntnis gelangen, von diesen manipuliert werden oder durch technische Fehler verändert werden können, sollte ein logisches Verfahren zum Schutz der Daten für den Transport oder die Übermittlung in Betracht gezogen werden.

Vertraulichkeitsschutz durch Verschlüsselung
Für die Übertragung vertraulicher Informationen bedarf es deren Verschlüsselung. Das entscheidende Merkmal eines Verschlüsselungsverfahrens ist die Güte des Algorithmus sowie der Schlüsselauswahl. Ein anerkannter Algorithmus, der für den mittleren Schutzbedarf ausreicht, ist der Data Encryption Standard (DES). Dieser ist leicht zu programmieren, zumal der Quell-Code in vielen Fachbüchern in der Programmiersprache C abgedruckt ist. Für den Bereich der öffentlichen Verwaltung kann das BSI für den Einsatz auf stationären und tragbaren PCs ein Offline-Verschlüsselungsprogramm (MIC 7.0) unter gewissen Randbedingungen zur Verfügung stellen, daß den Sicherheitsanforderungen im Bereich des mittleren Schutzbedarfs genügt. Ein Anforderungsvordruck befindet sich im Teil Hilfsmittel des vorliegenden IT-Grundschutzhandbuchs. Um den Anforderungen der Vertraulichkeit der zu übertragenden Informationen zu entsprechen, müssen das IT-System des Absenders und des Empfängers den Zugriffsschutz auf das Verschlüsselungsprogramm ausreichend gewährleisten. Ggf. sollte dieses Programm auf einem auswechselbaren Datenträger gespeichert, in der Regel verschlossen aufbewahrt und nur bei Bedarf eingespielt/genutzt werden.

Integritätsschutz durch Checksummen, Verschlüsselung oder Digitaler Signaturbildung
Ist für den Datenaustausch lediglich die Integrität der zu übermittelnden Daten sicherzustellen, muß unterschieden werden, ob ein Schutz nur gegen zufällige Veränderungen, z.B. durch Übertragungsfehler, oder auch gegen Manipulationen geleistet werden soll. Sollen ausschließlich zufällige Veränderungen erkannt werden, können Checksummenverfahren (z.B. Cyclic Redundancy Checks) oder fehlerkorrigierende Codes zum Einsatz kommen. Schutz gegenüber Manipulationen bieten darüber hinaus Verfahren, die unter Verwendung eines symmetrischen Verschlüsselungsalgorithmus (z.B. DES) aus der zu übermittelnden Information einen sogenannten Message Authentication Code (MAC) erzeugen. Andere Verfahren bedienen sich eines asymmetrischen Verschlüsselungsalgorithmus (z.B. RSA) in Kombination mit einer Hash-Funktion und erzeugen eine „Digitale Signatur“. Die jeweiligen erzeugten „Fingerabdrücke“ (Checksumme, fehlerkorrigierende Codes, MAC, Digitale Signatur) werden zusammen mit der Information an den Empfänger übertragen und können von diesem überprüft werden.

Für die Übermittlung oder den Austausch ggf. notwendiger Schlüssel sei hier auf Maßnahme M 2.46 - Angepaßtes Schlüsselmanagement bei Verschlüsselung verwiesen.

M 4.35 Verifizieren der zu übertragenden Daten vor Versand
Vor dem Versenden des Datenträgers ist dieser darauf zu überprüfen, ob die gewünschten Informationen - und auch nur diese - vom Datenträger rekonstruierbar sind.
Um die korrekte Übertragung zum Datenträger zu überprüfen, kann ein Programm eingesetzt werden, daß die ursprüngliche mit der übertragenen Datei zeichenweise vergleicht (auf einem PC unter DOS z.B. mittels des Befehls comp).
Auch sollten alle Dateien des Datenträgers aufgelistet werden (z.B. mit dir unter DOS oder ls unter Unix), um sicherzustellen, daß nur für den Empfänger bestimmte Dateien auf diesem Datenträger enthalten sind.
Befanden sich vorher andere Daten auf diesem Datenträger, so sind diese physikalisch zu löschen (M 4.32 - Physikalisches Löschen der Datenträger vor und nach Verwendung).

M 4.36 Sperren bestimmter Fax-Empfängerrufnummern
Besteht die Notwendigkeit, das zufällige oder absichtliche Versenden von Informationen oder Unterlagen per Fax an eine nicht gewünschte Empfängerrufnummer zu verhindern, so bietet die heutige Technik dazu mindestens drei Lösungen:
Bei einigen Geräten ist es möglich, die Versendung von Faxen an bestimmte Fax-Empfängerrufnummern zu unterbinden (positiver Ausschluß) oder alternativ alle Empfängerrufnummern außer einigen ausgewählten Rufnummern zu sperren (negativer Ausschluß).
Die gleiche Art der Berechtigungsvergabe kann auch in modernen TK-Anlagen erreicht werden, vorausgesetzt, das Fax-Gerät ist über eine solche Anlage ans Telefonnetz angeschlossen.
Wenn ein Fax-Gerät oder die TK-Anlage eine solche Möglichkeit nicht bietet, so kann zum Beispiel vom Betreiber des öffentlichen Netzes eine Zusatzeinrichtung gemietet werden, die den Verbindungsaufbau zu bestimmten Rufnummern (positiver und negativer Ausschluß) verhindert.

M 4.37 Sperren bestimmter Fax-Absenderrufnummern
Damit bestimmte Fax-Sendungen das eigene Fax-Gerät nicht blockieren können, z.B. bei Überlastung durch spezielle Fax-Aktionen von Werbeagenturen, kann ggf. eine Sperre bestimmter Fax-Senderrufnummern realisiert werden.
Einige moderne Fax-Geräte (Gruppe 4) sind in der Lage, die übermittelte Senderrufnummer auszuwerten und den Empfang von Fax-Sendungen ausgewählter Rufnummern zu verweigern.
Eine weitere Möglichkeit besteht darin, daß beim Telefon-Netzbetreiber kostenpflichtig eine geschlossene Benutzergruppe eingerichtet wird, wenn Empfänger und Sender an digitalen Vermittlungsstellen angeschlossen sind. Teilweise wird diese Möglichkeit auch von modernen TK-Anlagen angeboten (vgl. auch [BSI1998] Kapitel 8.1 - TK-Anlage).

M 4.38 Abschalten nicht benötigter Leistungsmerkmale
Nicht benötigte Leistungsmerkmale (insbesondere die Fernabfrage) sollten nach Möglichkeit abgeschaltet werden, um vor Mißbrauch und Fehlbedienung geschützt zu sein. Zur Entscheidung,

ob ein Leistungsmerkmal benötigt wird, sollten auch die damit verbundenen Sicherheitsrisiken einbezogen werden.

M 4.39 Abschalten des Anrufbeantworters bei Anwesenheit
In Zeiten, in denen der Anrufbeantworter nicht benötigt wird, kann er zum Schutz gegen Mißbrauch abgeschaltet oder vom Telefonnetz getrennt werden. Insbesondere in dem Fall, daß das Gerät über die Funktion der Raumüberwachung verfügt, sollte dies konsequent durchgeführt werden.
Zu beachten ist, daß sich in einigen Fällen die abgeschalteten Anrufbeantworter selbständig aktivieren, wenn die Verbindung nach einer gewissen Zeit nicht aufgebaut wird (z.B. nach 10-maligem Klingeln).

M 4.40 Verhinderung der unautorisierten Nutzung des Rechnermikrofons
Das Mikrofon eines vernetzten Rechners kann von denjenigen benutzt werden, die Zugriffsrechte auf die entsprechende Gerätedatei (unter Unix zum Beispiel /dev/audio) haben. Unter Windows NT bestimmen die Zugriffsrechte auf die entsprechenden Schlüssel der Registrierung (HKEY_LOCAL_MACHINE\HARDWARE\.), wer das Rechnermikrofon aktivieren kann. Diese Rechte sind daher sorgfältig zu vergeben. Der Zugriff auf die Gerätedatei sollte nur möglich sein, solange jemand an dem IT-System arbeitet. Wenn die Benutzung eines vorhandenen Mikrofons generell verhindert werden soll, muß es - wenn möglich - ausgeschaltet oder physikalisch vom Gerät getrennt werden.
Falls das Mikrofon in den Rechner integriert ist und nur durch Software ein- und ausgeschaltet werden kann, müssen die Zugriffsrechte so gesetzt sein, daß es kein Unbefugter benutzen kann. Dies kann z.B. erfolgen, indem unter Unix allen Benutzern die Leserechte auf die Gerätedatei /dev/audio bzw. unter Windows NT die Zugriffsrechte auf die entsprechenden Schlüssel der Registrierung entzogen werden. Dadurch ist ausgeschlossen, daß ein normaler Benutzer das Mikrofon benutzen kann, er kann aber weiterhin Audio-Dateien abspielen.
Bei IT-Systemen mit Mikrofon ist zu prüfen, ob Zugriffsrechte und Eigentümer bei einem Zugriff auf die Gerätedatei verändert werden. Falls dies der Fall ist oder falls gewünscht ist, daß jeder Benutzer das Mikrofon benutzen kann und es nicht nur in Einzelfällen durch den Systemadministrator freigegeben werden soll, muß der Administrator ein Kommando zur Verfügung stellen, das

- nur aktiviert werden kann, wenn jemand an dem IT-System angemeldet ist,
- nur durch diesen Benutzer aktiviert werden kann und
- die Zugriffsberechtigungen dem Benutzer nach dem Abmelden wieder entzieht.

Solange der Zugriff auf das Mikrofon durch kein sicheres Kommando geregelt wird, muß das Mikrofon physikalisch vom Rechner getrennt werden.

M 4.41 Einsatz eines angemessenen PC-Sicherheitsproduktes
Für den DOS-PC mit mehreren Benutzern ist der Einsatz eines PC-Sicherheitsproduktes vorzusehen. Für die Beschaffung eines Produktes oder für die Überprüfung schon im Einsatz

befindlicher Produkte kann folgende Mindestfunktionalität als Maßstab genutzt werden. Mit ihr soll erreicht werden, daß

- nur autorisierte Personen den PC benutzen können,
- die Benutzer auf die Daten nur in der Weise zugreifen können, die sie zur Aufgabenerfüllung benötigen,
- Unregelmäßigkeiten und Manipulationsversuche erkennbar werden.

Empfohlene Mindestfunktionalität für PC-Sicherheitsprodukte für den Einsatz bei DOS-PCs mit mehreren Benutzern:

- Identifikation und Authentisierung des Administrators und der Benutzer. Es sollte eine Sperre des Systems nach 3 fehlerhaften Authentisierungsversuchen stattfinden, die nur der Administrator zurücksetzen kann. Wird ein Paßwort verwendet, sollte das Paßwort mindestens sechs Stellen umfassen und verschlüsselt im System gespeichert werden.
- Rechteverwaltung und -kontrolle auf Festplatten und Dateien, wobei zumindest zwischen lesendem und schreibendem Zugriff unterschieden werden soll.
- Rollentrennung zwischen Administrator und Benutzer. Nur der Administrator kann Rechte zuweisen oder entziehen.
- Protokollierung der Vorgänge Anmelden, Abmelden und Rechteverletzung sollte möglich sein.
- Kein Systemzugriff auf Betriebssystemebene (DOS) darf für Benutzer möglich sein.
- Bildschirmsperre nach zeitweiser Inaktivität der Tastatur oder Maus und Reaktivierung mittels Identifikation und Authentisierung.
- Boot-Schutz soll verhindern, daß der PC unbefugt von Diskette gebootet werden kann.

Sinnvolle minimale Evaluationstiefe und Mindeststärke der Mechanismen für Zertifikate nach ITSEC: E2, mittel. Zusätzliche Forderungen an das PC-Sicherheitsprodukt:

- Benutzerfreundliche Oberfläche zur Erhöhung der Akzeptanz.
- Aussagekräftige und nachvollziehbare Dokumentation für Administrator und Benutzer.

Wünschenswerte Zusatzfunktionalität des PC-Sicherheitsproduktes:

- Rollentrennung zwischen Administrator, Revisor und Benutzer; nur der Administrator kann Rechte zuweisen oder entziehen und nur der Revisor hat Zugriff auf die Protokolldaten,
- Protokollierung von Administrationstätigkeiten,

- Unterstützung der Protokollauswertung durch konfigurierbare Filterfunktionen,
- Verschlüsselung der Datenbestände mit einem geeigneten Verschlüsselungsalgorithmus und in einer Weise, daß ein Datenverlust bei Fehlfunktion (Stromausfall, Abbruch des Vorgangs) systemseitig abgefangen wird.

Die Realisierung dieser Funktionalität kann sowohl in Hardware wie auch in Software erfolgen. Bei der Neubeschaffung eines Produktes sollte Maßnahme M 2.66 - Beachtung des Beitrags der Zertifizierung für die Beschaffung berücksichtigt werden.
Eine Übersicht über PC-Sicherheitsprodukte und deren Funktionalitäten befindet sich in der BSI-BOX. Die vom BSI zertifizierten IT-Produkte und -Systeme können der BSI Schrift 7148 entnommen werden.

Übergangslösung:
Sollte eine kurzfristige Beschaffung bzw. ein zügiger Einsatz eines solchen PC-Sicherheitsproduktes nicht möglich sein und haben die PC-Benutzer dieses PC keine gemeinsamen Daten, kann als Übergangslösung ein Verschlüsselungsprodukt eingesetzt werden. Mit diesem Produkt muß jeder Benutzer zu Beginn der Arbeit die ihm zugeordneten Daten entschlüsseln und bei Beendigung der Arbeit wieder verschlüsseln. Damit kann sichergestellt werden, daß die Vertraulichkeit der Daten gewahrt bleibt, jedoch wird nicht verhindert, daß die verschlüsselten Daten manipuliert werden können. Die Manipulation der Daten wird im allgemeinen bei der Entschlüsselung erkannt, da sich nicht sinnvolle Daten ergeben.
Für den Bereich der öffentlichen Verwaltung kann das BSI für den Einsatz auf stationären und tragbaren PCs ein Off-line-Verschlüsselungsprogramm unter gewissen Randbedingungen zur Verfügung stellen, daß den Sicherheitsanforderungen im Bereich des mittleren Schutzbedarfs genügt. Ein Anforderungsvordruck befindet sich im Teil Hilfsmittel des vorliegenden IT-Grundschutzhandbuchs.

M 4.42 Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung

Mehrere Gründe können zu der Notwendigkeit führen, daß innerhalb der Anwendungsprogramme selbst Sicherheitsfunktionalitäten wie eine Zugangskontrolle, eine Zugriffsrechteverwaltung und -prüfung oder eine Protokollierung implementiert werden müssen:

- Reichen die Protokollierungsmöglichkeiten des IT-Systems einschließlich zusätzlich eingesetzter IT-Sicherheitsprodukte nicht aus, um eine ausreichende Beweissicherung zu gewährleisten, so müssen diese Protokollelemente im Anwendungsprogramm implementiert werden. (Beispiel: BDSG, Anlage zum § 9, Eingabekontrolle: „zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind“.)
- Reicht die Granularität der Zugriffsrechte des IT-Systems einschließlich zusätzlich eingesetzter Sicherheitsprodukte nicht aus, um einen ordnungsgemäßen Betrieb zu gewährleisten, so muß eine Zugriffsrechteverwaltung und -kontrolle im Anwendungsprogramm implementiert werden. (Beispiel: eine Datenbank mit einer gemeinsamen Datenbasis.

Vorausgesetzt sei, daß je nach Funktion des Benutzers nur Zugriffe auf bestimmte Felder zulässig sind.)

- Ist es mit dem IT-System einschließlich zusätzlich eingesetzter IT-Sicherheitsprodukte nicht möglich, den Administrator daran zu hindern, auf bestimmte Daten zuzugreifen oder zumindest diesen Zugriff zu protokollieren und zu kontrollieren, dann muß dies bei Bedarf durch zusätzliche Sicherheitsfunktionen im Anwendungsprogramm implementiert werden. Zum Beispiel kann mit einer Verschlüsselung der Daten verhindert werden, daß der Administrator diese Daten im Klartext liest, wenn er nicht im Besitz des zugehörigen Schlüssels ist.

Diese zusätzlichen Anforderungen an IT-Anwendungen müssen schon in der Planung und Entwicklung berücksichtigt werden, da eine nachträgliche Implementation meist aus Kostengründen nicht mehr möglich ist.

M 4.43 Fax-Gerät mit automatischer Eingangskuvertierung
Fax-Geräte mit automatischer Eingangskuvertierung verhindern, daß eingegangene Faxe unberechtigt entnommen und unberechtigt gelesen werden. Eingehende Faxe werden so geknickt, daß nur das Fax-Vorblatt sichtbar bleibt, und dann in einem Klarsichtumschlag eingeschweißt. Danach fällt der Umschlag in ein verschließbares Fach im Fax-Gerät. Zugriff auf die Umschläge hat normalerweise nur der Berechtigte, der den Schlüssel zu diesem Fach besitzt. Eine unbefugte Kenntnisnahme ist vor Zustellung des Fax nur durch gewaltsames Öffnen des Faches oder Aufreißen des verschweißten Umschlages möglich und wird daher zumindest bemerkt.

M 4.44 Prüfung eingehender Dateien auf Makro-Viren
Eingehende Dateien im Wege des Datenträgeraustausch oder bei elektronischer Übermittlung sind einer Virenprüfung zu unterziehen. Dies gilt nicht nur für reguläre Programm-Dateien, sondern auch für solche Dateien, die mittels Anwendungsprogrammen erstellt wurden, die eine Makrosprache verwenden können. Für die nachfolgend aufgezählten Anwendungsprogramme ist derzeit bekannt, daß Makros mit Schadfunktionen erzeugt wurden:

- Winword (ab Version 2.0),
- Excel,
- AmiPro,
- Adobe Acrobat.

Sofern ein aktuelles Virensuchprogramm eingesetzt wird, das auch Makro-Viren erkennt, kann auf weitere Maßnahmen verzichtet werden. Da sich die Verbreitung der Makro-Viren jedoch erst in einem Anfangsstadium befindet, ist die Einrichtung einer Testumgebung anzuraten. Hier sollten übersandte Dateien mit dem jeweiligen Anwendungsprogramm auf Makro-Viren hin untersucht werden. Alternativ besteht die Möglichkeit, empfangene Dateien mit einem Editor zu bearbeiten, der die Datei in ein Format umwandelt, in dem die Makros nicht ablauffähig sind.

Auch in PostScript-Dateien kann es zu Problemen ähnlich wie bei Makro-Viren kommen. Bei PostScript-Anzeige-Programmen handelt es sich um Interpreter, die die PostScript-Sprache abarbeiten. Ab Level 2.0 der PostScript-Spezifikation gibt es auch PostScript-Befehle, um Dateien zu schreiben. Dadurch ist es möglich, PostScript-Dateien zu erzeugen, die während der Bearbeitung durch einen Interpreter, auch bereits bei der Anzeige am Bildschirm, andere Dateien modifizieren, löschen oder umbenennen können.
Konkrete Probleme existieren bei dem Programm ghostscript (gs). In den Unix-Versionen können die Schreibmöglichkeiten auf Dateien mit der Option -dSAFER abgeschaltet werden. Allerdings ist dies nicht die Voreinstellung. In Versionen für andere Betriebssysteme heißt diese Option ähnlich. Die Verwendung der Option -dSAFER wird dem Benutzer überlassen. Dies hat auch zur Folge, daß zahlreiche andere Programme, die intern ghostscript (gs) aufrufen (z.B. mosaic, netscape, xdvi, xfig, xv etc.), dies unterschiedlich realisieren. Die Option sollte daher als Default eingestellt werden. Beschreibungen, wie dies zu realisieren ist, finden sich in den Sicherheitsbulletins des DFN-CERT DSB-95:02 und DSB-95:03 vom 24. August 1995 (siehe auch M 2.35 - Informationsbeschaffung über Sicherheitslücken des Systems).
Betroffen von diesem Problem sind z.B. alle ghostscript-Versionen von Aladdin vor 3.22beta und die GNU-Versionen bis einschließlich 2.6.2. Bei älteren ghostscript-Versionen kann es daneben weitere PostScript-Befehle geben, mit denen Dateien modifiziert werden können. Es sollten nur ghostscript-Versionen eingesetzt werden, bei denen diese Probleme beseitigt wurden.
Der PostScript-Interpreter ghostview bietet ab der Version 1.5 eine Option -safer an, die die Sicherheitsfunktionen von ghostscript aktiviert. Versionen vor 1.5 bieten diesen Schutz nicht und sollten durch die aktuelle Version ersetzt werden.
Auch bei PDF-Dateien kann es zu ähnlichen Problemen kommen. Im Internet findet man häufig PDF-Dateien, die mit dem kostenlos verfügbaren Acrobat Reader gelesen werden können. In PDF-Dateien lassen sich Funktionen wie Programmaufrufe einbetten, die ein Sicherheitsrisiko für die Dateien des lokalen IT-Systems darstellen. Die eingebetteten Funktionen können bereits beim Öffnen des Dokuments oder durch das Bewegen im Dokument über sogenannte Action Trigger gestartet werden, ohne daß sich der Leser dessen bewußt ist.
Um dies zu vermeiden, sollten für das Lesen von PDF-Dateien nur Viewer wie ghostscript eingesetzt werden, die diese Funktionalität noch nicht verarbeiten können, oder die aktuellste Version des Acrobat Reader bzw. des Acrobat Exchange, bei denen die Benutzer über das Vorhandensein evtueller Makros informiert werden und der Ausführung explizit zustimmen müssen.

M 4.47 Protokollierung der Firewall-Aktivitäten

Es muß festgelegt werden, welche Ereignisse protokolliert werden und wer die Protokolle auswertet. Die Protokollierung muß den datenschutzrechtlichen Bestimmungen entsprechen. Für Protokolldaten ist insbesondere die Zweckbindung nach § 14 des BDSG zu beachten.
Die eingesetzten Packet-Filter müssen für jedes ein- oder ausgehende Paket IP-Nummer, Dienst, Zeit und Datum protokollieren können. Dabei sind auch Einschränkungen auf bestimmte Pakete (z.B. nur Pakete mit einer speziellen Quell-Adresse) möglich.
Für jede aufgebaute und abgewiesene Verbindung muß eine Protokollierung von Benutzer-Identifikation, IP-Nummer, Dienst, Zeit und Datum durchgeführt werden (Application-Gateway), wobei auch Einschränkungen auf bestimmte Verbindungen (z.B. für einen speziellen Benutzer)

möglich sind.
Es muß möglich sein, daß für bestimmte Benutzer keine Protokollierung vorgenommen wird, damit wegen einer zu großen Anzahl von Protokolleinträgen keine wichtigen Informationen übersehen werden. Diese Auswahl kann z.B. anhand des Rechteprofils einzelner Benutzer getroffen werden. Die Protokollinformationen von allen Komponenten sollten über einen vertrauenswürdigen Pfad an eine zentrale Stelle geschickt werden, damit die Protokollinformationen vor ihrer endgültigen Speicherung nicht verändert werden können.
Spezielle, einstellbare Ereignisse, wie z.B. wiederholte fehlerhafte Paßworteingaben für eine Benutzerkennung oder unzulässige Verbindungsversuche, müssen bei der Protokollierung hervorgehoben werden und sollten zu einer unverzüglichen Warnung des Firewall-Administrators führen. Wenn eine ordnungsgemäße Protokollierung nicht mehr möglich ist (z.B. weil auf dem zugehörigen Datenträger kein Platz mehr ist), muß die Firewall jeglichen Verkehr blockieren und eine entsprechende Meldung an den Administrator weitergeben.

M 4.48 Paßwortschutz unter Windows NT
Der Zugang zu einem Windows NT System muß für jeden Benutzer durch ein Paßwort geschützt sein. Benutzerkonten ohne Paßwort dürfen nicht existieren, da sie eine Schwachstelle im System darstellen. Es ist wichtig, daß auch die Benutzer die Schutzfunktion der Paßwörter kennen, denn die Mitarbeit der Benutzer trägt selbstverständlich zur Sicherheit des gesamten Systems bei.

Die Einrichtung eines neuen Benutzers erfolgt mit Hilfe des Dienstprogramms Benutzer-Manager über das Kommando „Neuer Benutzer“ . Dabei ist dazu in den Feldern „Kennwort“ und „Kennwortbestätigung“ ein Anfangspaßwort mit maximal 14 Zeichen einzugeben. Bei Paßwörtern unter Windows NT muß die Groß- und Kleinschreibung beachtet werden. Dabei sollte ein sinnvolles Anfangspaßwort vergeben werden, das dem Benutzer mitgeteilt wird. Die immer gleiche Wahl des Anfangspaßwortes oder das Setzen dieses Paßworts gleich dem Benutzernamen eröffnet eine Sicherheitslücke, die mit geringem Aufwand vermieden werden kann.

Die Option „Benutzer muß Kennwort bei der nächsten Anmeldung ändern“ sollte bei allen neuen Konten gesetzt sein, damit das Anmeldepaßwort nicht beibehalten wird. Dagegen sollte die Option „Benutzer kann Kennwort nicht ändern“ nur in Ausnahmefällen verwendet werden, etwa für vordefinierte Konten im Schulungsbetrieb. Die Option „Kennwort läuft nie ab“ sollte nur für Benutzerkonten, denen mit Hilfe der Systemsteuerungsoption „Dienste“ ein Dienst zugewiesen wird (zum Beispiel der Reproduktionsdienst) verwendet werden, da sie die Einstellung „Maximales Kennwortalter“ in den Richtlinien für Konten außer Kraft setzt und verhindert, daß das Paßwort abläuft.
Über den Benutzer-Manager können Richtlinien für Benutzerkonten, Benutzerrechte und für die Systemüberwachung festgelegt werden. In den Richtlinien für Benutzerkonten sollte als minimale Paßwortlänge der Wert 6, bei höheren Sicherheitsanforderungen der Wert 8 eingetragen werden (siehe auch M 2.11 - Regelung des Paßwortgebrauchs).

Die Paßwort-Historie sollte grundsätzlich eingeschaltet sein und sollte wenigstens 6 Paßwörter umfassen. Die Gültigkeitsdauer des Paßwortes („Maximales Kennwortalter“) sollte auf einem Zeitraum von maximal 6 Monaten begrenzt sein. Durch Festlegung eines Wertes für das „Minimale Kennwortalter“ kann verhindert werden, daß Benutzer ihr Paßwort mehrfach hintereinander ändern, um so die Historienprüfung zu umgehen. Das „Minimale Kennwortalter“ sollte jedoch nicht größer als 1 Tag gewählt werden, um dem Benutzer jederzeit eine Paßworttänderung zu ermöglichen .
Hinweis: Der Parameter „Sofortige Änderungen erlauben“ darf unter der Version 3.51 von Windows NT nicht gewählt werden, da sonst die Prüfung der Paßwort-Historie abgeschaltet wird.

Benutzerkonten sollten nach wiederholten ungültigen Paßworteingaben gesperrt werden, um Versuche zu erschweren, die Paßwörter der Benutzer zu erraten. Die Option „Konto sperren“ sollte auf jeden Fall aktiviert werden. Dazu sollte die Option „Sperren nach“, die die Anzahl (1 bis 999) der ungültigen Anmeldeversuche festlegt, die zur Sperrung des Kontos führen, auf einen Wert zwischen 3 und 10 gesetzt werden. Die Option „Konto zurücksetzen nach“, die die maximale Anzahl von Minuten (1 bis 99999) zwischen zwei ungültigen Anmeldeversuchen angibt, sollte auf etwa eine halbe Stunde gesetzt werden. Wenn z.B. für „Sperren nach“ der Wert 5 und für „Konto zurücksetzen nach“ der Wert 30 angegeben ist, erfolgt eine Sperrung nach 5 ungültigen Anmeldungsversuchen, die innerhalb von 29 Minuten unternommen wurden.
In der Regel sollte durch Aktivieren der Option „Für immer“ festgelegt werden, daß die Sperre so lange aktiv bleibt, bis ein Administrator sie aufhebt. Sofern hierdurch eine zu hohe Belastung der Administratoren verursacht wird, kann auch ein geeigneter Wert als „Dauer der Sperrung“ angegeben werden, damit die Kontensperre nur für eine begrenzte Zeitdauer erhalten bleibt. Wenn beabsichtigt ist, den Ursachen der Kontensperrung direkt nachzugehen, sollte ein hinreichend langes Zeitintervall, z.B. 1440 Minuten (1 Tag) angegeben werden, andernfalls sollte ein Wert von etwa 30 Minuten gewählt werden.

Es ist zu beachten, daß das vordefinierte Administratorkonto von dieser automatischen Sperrung ausgenommen ist, um ein völliges Verriegeln des Systems zu vermeiden (siehe M 4.77 - Schutz der Administratorenkonten unter Windows NT).
Dagegen sollte von der Option „Benutzer muß sich anmelden, um Kennwort zu ändern“ kein Gebrauch gemacht werden. Insbesondere mit der Einstellung „Benutzer muß Kennwort bei der nächsten Anmeldung ändern“ führt diese Einstellung dazu, daß neue Benutzer keinen Zugang zum Rechner erhalten.
Die in der Abbildung 1 dargestellten Werte für die Richtlinien geben einen für mittleren Sicherheitsbedarf ausreichenden Schutz:

M 4.49 Absicherung des Boot-Vorgangs für ein Windows NT System
Windows NT kann nur dann sicher betrieben werden, wenn vom Systemstart an gewährleistet ist, daß eine geschlossene Sicherheitsumgebung aufgebaut wird, also daß keine Wege an den Sicherheitsfunktionen des Betriebssystems vorbei bestehen. Dies erfordert, daß sich alle durch Windows NT schützbaren Ressourcen unter der Kontrolle des Betriebssystems befinden und daß es auch keine Möglichkeit gibt, fremde Systeme oder offene Systemumgebungen zu starten,

die den durch Windows NT gebotenen Schutz unterlaufen können. Dazu sind die folgenden Aspekte zu beachten:

- Alle vorhandenen Festplattenpartitionen müssen mit dem Dateisystem NTFS formatiert sein. Partitionen, die mit den Dateisystemen FAT, VFAT oder HPFS formatiert sind, können nicht gegen Zugriffe der Benutzer geschützt werden. Dies bedeutet einerseits, daß die auf ihnen abgelegten Daten beliebigen Zugriffen aller Benutzer ausgesetzt sind, und andererseits können diese Partitionen zum unkontrollierten Datenaustausch zwischen Benutzern mißbraucht werden.

- Ein ähnliches Risiko stellen Diskettenlaufwerke dar, da Disketten unter Windows NT nur mit dem Dateisystem FAT bzw. VFAT formatiert werden können. Aus diesem Grund sind Diskettenlaufwerke an allen Rechnern, die nicht unter strikter physischer Kontrolle stehen, grundsätzlich durch den Einbau von Diskettenschlössern zu sperren (siehe M 4.4 - Verschluß der Diskettenlaufwerkschächte). Auf Windows NT Clients können auch die Diskettenlaufwerke durch Deaktivieren über die Systemsteuerungsoption „Geräte“, Gerät „Floppy“, die Diskettenlaufwerke für unprivilegierte Benutzer außer Betrieb gesetzt werden. Hiervon sollte auf Windows NT Servern abgesehen werden (siehe hierzu M 4.52 - Geräteschutz unter Windows NT).

- Verfügt der Rechner über ein offenes Diskettenlaufwerk oder ist es möglich, von einem vorhandenen CD-ROM-Laufwerk zu booten, so besteht die Gefahr, daß der Rechner mit einem anderen Betriebssystem als Windows NT gestartet wird. Die gleiche Gefährdung ergibt sich, wenn auf einer lokalen Festplatte andere Betriebssysteme installiert sind. Dann kann der Anwender mit verschiedenen Programmen die Sicherheitsmechanismen von Windows NT umgehen. Inzwischen gibt es mehrere Programme, mit denen man Dateien, die unter NTFS geschützt sind, von einer DOS-Umgebung oder einer Linux-Umgebung lesen und z.T. auch ändern kann. Sowohl unter dem Betriebssystem MS-DOS als auch unter dem Betriebssystem Linux werden die vom Dateisystem NTFS gesetzten Sicherheitsattribute ignoriert. Der Anwender hat daher von MS-DOS bzw. von Linux aus Zugriff auf alle Dateien des Rechners. Aus diesem Grund dürfen neben Windows NT keine weiteren Betriebssysteme auf der Festplatte installiert sein. Außerdem ist der Boot-Vorgang durch eine mit einem BIOS-Paßwort geschützte Einstellung des BIOS so abzusichern, daß das System nicht von einem eventuell vorhandenen Diskettenlaufwerk oder von einem CD-ROM-Laufwerk aus gestartet werden kann (siehe M 4.1 - Paßwortschutz für PC und Server).

- Im Rahmen einer Neuinstallation von Windows NT hat man die Möglichkeit, die bestehende Installation des Betriebssystems zu aktualisieren oder eine neue Version parallel zu installieren. Bei der parallelen Installation wird die bestehende Dateistruktur nicht verändert, doch wird das vordefinierte Administratorkonto mit einem neuen Paßwort neu angelegt. Dieser neueÄdministrator hat dann vollen Zugriff auf alle Ressourcen des Rechners und damit auch auf alle Daten und Programme. Um diese Möglichkeit der Neuinstallation zu verhindern, dürfen Anwender nicht in der Lage sein, die Datei BOOT.INI

im Wurzelverzeichnis der ersten Platte zu verändern (siehe M 4.53 - Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT).

- Mit Hilfe der Installationsprogramme kann auch eine Notfalldiskette (siehe M 6.42 - Erstellung von Rettungsdisketten für Windows NT) erzeugt und mit dieser dann eine Systemrekonstruktion durchgeführt werden. Dabei wird der Zugriffsschutz der NTFS-Partition des Betriebssystems aufgehoben. Es ist aus diesem Grund unbedingt erforderlich, die Installationsprogramme, eine eventuell schon vorhandene Notfalldiskette und die Setup-Disketten so zu verwahren, daß sie gegen unbefugten Zugriff geschützt sind. Schutz gegen diese spezifische Bedrohung bietet auch die Sicherung der Diskettenlaufwerke durch Laufwerkschlösser (siehe M 4.4 - Verschluß der Diskettenlaufwerkschächte) und die Absicherung des Boot-Vorgangs durch die entsprechende Einstellung des BIOS (s.o.).

Unter Windows NT ist das Anmelden auf dem Server nur für Benutzer möglich, denen das Benutzerrecht Lokale Anmeldung"gegeben wurde. Diese Benutzer sind auf die ihnen zugewiesenen Rechte und Berechtigungen eingeschränkt. Um einen Mißbrauch der Möglichkeiten zum Anmelden auf dem Server zu vermeiden, sind die Benutzerrechte und die Zuordnungen zu Benutzergruppen entsprechend restriktiv vorzusehen (siehe Maßnahmen M 2.93 - Planung des Windows NT Netzes und M 4.50 - Strukturierte Systemverwaltung unter Windows NT).

M 4.50 Strukturierte Systemverwaltung unter Windows NT

Benutzergruppen

Benutzergruppen sind unter Windows NT Zusammenstellungen von Benutzerkonten. Wenn ein Benutzerkonto zu einer Gruppe hinzugefügt wird, erhält der betreffende Benutzer alle Rechte und Berechtigungen, die der Gruppe erteilt wurden. So kann man leicht bestimmte Benutzer mit gemeinsamen Möglichkeiten ausstatten. Nach Möglichkeit sollten die Rollen der Mitarbeiter auf Gruppen abgebildet und diesen Gruppen entsprechend ihren Bedürfnisse die Zugriffsrechte zugeteilt werden. Die Verwendung von Gruppen an Stelle der Zuweisung von Rechten und Berechtigungen an einzelne Benutzer erleichtert die Administration und trägt durch größere Transparenz zur Erhöhung der Systemsicherheit bei. Auch bei einer geringen Anzahl von Mitarbeitern sollten Gruppen gebildet werden. Hierdurch müssen bei einer Erweiterung keine grundsätzliche Umstrukturierung der Rechtestrukturen durchgeführt werden.

Die Benutzer sollten grundsätzlich nur der allgemeinen Gruppe „Benutzer“ sowie geeigneten frei definierten Gruppen, die die Organisationsstruktur widerspiegeln, zugeordnet werden. Zuordnungen zu den anderen vordefinierten Gruppen sollten nur in begründeten Einzelfällen vorgenommen werden. Alle Gruppen einer Arbeitsstation, die in Windows NT verwaltet werden, sind vom Typ „Lokale Gruppe“. Die Gruppe wird „lokal“ genannt, weil ihr Berechtigungen und Rechte nur für die eigene Arbeitsstation erteilt werden können. Sie kann jedoch Benutzerkonten aus der Arbeitsstation enthalten, und wenn die Arbeitsstation einer Domäne angehört, kann sie Benutzerkonten und globale Gruppen aus der eigenen Domäne und aus vertrauten Domänen beinhalten. Lokale Gruppen bieten ein einfaches Konzept zur Zusammenstellung von Benutzern der Arbeitsstation und von Domänen, die nur an der Arbeitsstation selbst verwendet werden.

Wenn ein Rechner, auf dem Windows NT ausgeführt wird, einer Domäne angehört, gibt es einen weiteren Gruppentyp, dem der Zugriff auf die Arbeitsstation ermöglicht werden kann. Es handelt sich um die „Globale Gruppe“, die an mehreren Orten verwendet werden kann: in der eigenen Domäne, auf Servern, auf Arbeitsstationen der Domäne und in vertrauten Domänen. Wenn eine Arbeitsstation einer Domäne angehört, bedeutet dies, daß den globalen Gruppen der Domäne und der vertrauten Domänen Berechtigungen und Rechte für die Arbeitsstation sowie die Zugehörigkeit zu lokalen Gruppen der Arbeitsstation erteilt werden können. Eine globale Gruppe kann nur Benutzerkonten der eigenen Domäne enthalten.

Vordefinierte Benutzergruppen
Welche Aktionen ein Benutzer durchführen kann, hängt von den Gruppenmitgliedschaften seines Benutzerkontos ab. Es sind mehrere Gruppen in Windows NT vordefiniert, und standardmäßig wird jeder Gruppe ein bestimmter Satz von Benutzerrechten erteilt. Bei Bedarf können mit dem Benutzer-Manager zusätzliche Gruppen erstellt und definiert werden, mit denen den ihnen zugewiesenen Benutzern der Zugriff auf individuell zusammengestellte Ressourcen ermöglicht wird.

Zusätzlich zu den Rechten werden einigen der vordefinierten lokalen Gruppen vordefinierte Funktionen zugeteilt. Rechte und Zugriffsberechtigungen können den Gruppen und Benutzerkonten direkt erteilt und von ihnen entfernt werden. Dagegen sind die vordefinierten Funktionen nicht direkt verwaltungsfähig. Vordefinierte Funktionen können für einen Benutzer nur bereitgestellt werden, wenn der Benutzer zum Mitglied einer geeigneten lokalen Gruppe ernannt wird.

Hinweis: Die oben beschriebenen Rechte, die unter Windows NT standardmäßig vergeben sind, sind alle einzeln daraufhin zu überprüfen, ob sie mit der festgelegten Sicherheitsstrategie vereinbar sind (siehe M 2.91 - Festlegung einer Sicherheitsstrategie für das Windows NT Client-Server-Netz). So sollte beispielsweise das Recht „Zugriff auf diesen Computer vom Netz“ der Gruppe „Jeder“ entzogen werden. Ob es ersatzweise der Gruppe „Benutzer“ zugestanden wird, ist im einzelnen zu klären.

Frei definierte Benutzergruppen
Gruppen sind zu verwenden, um auf einfache Weise den Zugriff auf Ressourcen wie zum Beispiel Verzeichnisse, Dateien und Drucker zu verwalten. Es ist zweckmäßig, zuerst einer Gruppe Ressourcenberechtigungen zuzuweisen und dann Benutzerkonten zu dieser Gruppe hinzuzufügen. Wenn die Berechtigungen einer Benutzergruppe zu ändern sind, so kann man einfach die gewünschten Berechtigungen zur Gruppe hinzufügen bzw. entfernen, anstatt dies für alle Benutzerkonten durchzuführen. Wenn ein neuer Benutzer Zugriff auf bestimmte Ressourcen erhalten soll, so braucht man nur das Konto des Benutzers zur geeigneten Gruppe hinzuzufügen.

M 4.51 Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT

Benutzerprofile dienen der Speicherung von benutzerspezifischen Einstellungen der Benutzerumgebung. Dies ist u.a. der Inhalt von Programmgruppen, die Netzwerk- und Druckerverbin-

dungen und die farbliche Darstellung des Bildschirms. Weiterhin können über Benutzerprofile die Möglichkeiten der Benutzer, mit Windows NT zu arbeiten, in verschiedener Hinsicht eingeschränkt werden. Die Verwaltung der Profile erfolgt mit dem Benutzerprofil-Editor (UPEDIT.EXE unter Windows NT 3.51 bzw. POLEDIT.EXE unter Windows NT 4.0).

Benutzerprofile können für verschiedene Einsatzzwecke erstellt werden:

- um bei Single-User-Systemen nach einer erneuten Anmeldung die ursprünglich festgelegten Einstellungen wiederherzustellen,
- um bei Multi-User-Systemen für jeden Benutzer eigene Einstellungen festzulegen,
- damit bei server-gespeicherten Benutzerprofilen jeder Benutzer von jeder NT-Workstation aus dieselbe Oberfläche erhält,
- um einheitliche Benutzerumgebungen zentral vorzugeben (sowohl bei Stand-alone-Systemen als auch bei bei vernetzten),
- um eine eingeschränkte Benutzerumgebung einzurichten, beispielweise um zu verhindern, daß Benutzer Änderungen an Desktop-Einstellungen vornehmen, oder den Zugriff auf die Systemsteuerung einzuschränken.

Grundsätzlich muß zwischen lokalen und server-gespeicherten Benutzerprofilen unterschieden werden. Lokale Benutzerprofile werden nur auf dem lokalem IT-System abgelegt, während server-gespeicherte Benutzerprofile zentral auf dem NT-Server verwaltet werden.
Fällt bei Verwendung von server-gespeicherten Benutzerprofilen der Server aus, dann wird auf die lokale Kopie zurückgegriffen.
Daneben muß zwischen persönlichen und verbindlichen Benutzerprofilen unterschieden werden. Persönliche Benutzerprofile sind vom Benutzer beliebig änderbar, verbindliche werden vom Administrator vorgegeben.
Verbindliche Profile bleiben von einer Sitzung zur nächsten erhalten, während einer Sitzung durchgeführte Veränderungen gehen beim Abmelden verloren. Diese Profile werden in dem Verzeichnis abgelegt, der im Profileintrag des betreffenden Kontos angegeben ist, und sie tragen unter der Version 3.51 von Windows NT die Dateinamenserweiterung .MAN. Ab Version 4.0 wird ein Profil dadurch als verbindliches Profil gekennzeichnet, daß die Datei NTUSER.DAT in NTUSER.MAN umbenannt wird.

Persönliche Profile, die auf einem Server abgelegt werden, können verwendet werden, um Benutzern unabhängig von der Arbeitsstation, von der aus sie sich anmelden, dieselbe Umgebung zur Verfügung zu stellen. Persönliche Profile werden in dem Verzeichnis abgelegt, der im Profileintrag des betreffenden Kontos angegeben ist, und sie tragen unter Version 3.51 die Dateinamenserweiterung .USR.
Unter Version 3.51 werden die Benutzerprofile im Verzeichnis %SystemRoot%\system32\config in den Benutzern zugeordneten Dateien abgelegt. Dabei werden die folgenden Einstellungen im Benutzerprofil abgelegt:

- Programm Manager: alle vom Benutzer einstellbaren Optionen einschließlich Programmgruppen, Programme und ihre Eigenschaften, sowie alle abspeicherbaren Einstellungen
- Datei-Manager: alle vom Benutzer wählbaren Einstellungen einschließlich der Netz-Verbindungen
- Kommandomodus: alle vom Benutzer wählbaren Einstellungen
- Druck Manager: netzweite Druckerverbindungen sowie alle abspeicherbaren Einstellungen
- Systemsteuerung: alle Einstellungen für Farben, Maus, Desktop, Zeiger, Tastatur, Ländereinstellungen und Klänge sowie die Einträge zur Benutzerumgebung im Element „System“
- Zubehör: alle benutzerspezifischen Einstellungen der Anwendungen
- Fremdanwendungen: alle Einstellungen, die von diesen Anwendungen als benutzerspezifische Optionen unterstützt werden
- Anmerkungen bei der online Hilfe: alle dort eingetragenen Anmerkungen des betreffenden Benutzers

Ab Version 4.0 werden Benutzerprofile als Verzeichnisbaum unter dem Unterverzeichnis Profiles des Windows-Verzeichnisses %SystemRoot%, also im allgemeinen \WINNT\Profiles, als Verzeichnis mit dem Namen des Benutzers, z.B. \WINNT\Profiles\Schmidt, abgelegt. Dabei wird die gesamte Struktur der Arbeitsoberfläche und insbesondere die Struktur der einzelnen Programmgruppen dort abgelegt. Die folgenden Unterverzeichnisse können dabei vorhanden sein:

- Anwendungsdaten: Anwendungsspezifische Daten
- Desktop: Elemente der Arbeitsoberfläche einschließlich der direkt auf der Arbeitsoberfläche abgelegten Dateien und Shortcuts
- Druckumgebung: Shortcuts zu den Einträgen in den Druckerordnern
- Favoriten: Shortcuts zu Programmeinträgen und Ordnern mit Favoriten
- Netzwerkumgebung: Shortcuts zu den Einträgen der Netzumgebung
- Persönlich: Shortcuts zu den Einträgen in den privaten Programmgruppen
- Recent: Shortcuts zu den zuletzt verwendeten Dokumenten
- SendTo: Shortcuts zu den Einträgen, die im Kontext-Menü als Ziele von Sende-Operationen, wie etwa zu einem Diskettenlaufwerk, verwendet werden können
- Startmenü: Struktur des gesamten Startmenüs einschließlich aller Shortcuts zu Programmen und Programmgruppen

- Vorlagen: Shortcuts zu Dokumentenvorlagen

Sonstige Einstellungen, wie etwa der Verweis auf das als Hintergrund der Arbeitsoberfläche verwendete Bild oder andere benutzerspezifische Einstellungen der Systemsteuerung, werden im Ordner Profiles in der Datei NTUSER.DAT abgelegt.
Die folgenden Optionen können unter Version 3.51 verwendet werden, um die Möglichkeiten der Benutzer mit Windows NT zu arbeiten in verschiedener Hinsicht einzuschränken:

- Einstellungen für Programm Manager: Hier kann festgelegt werden, ob Programme über „Datei - Ausführen“ gestartet werden dürfen, die aktuellen Einstellungen gespeichert werden dürfen und ob allgemeine Programmgruppen angezeigt werden. Außerdem kann die Autostartgruppe festgelegt werden.

- Einstellungen für Programmgruppen: Hier kann der Zugriff auf bestimmte Programmgruppen gesperrt werden und für ungesperrte Programmgruppen verschiedene Änderungsbefugnisse vergeben werden.

- Den Benutzern kann das Verbinden bzw. Trennen von Netzdruckern über den Druckmanager erlaubt oder verboten werden.

- Es kann erzwungen werden, daß die Ausführung des Anmeldeskriptes abgewartet wird, bevor der Programm-Manager gestartet wird. Diese Option sollte immer aktiviert sein, damit die im Anmeldeskript vorgesehenen Aktionen auf jeden Fall durchgeführt werden.

Ab der Version 4.0 können die folgenden Einschränkungen mit Hilfe des Systemrichtlinien-Editors festgelegt werden:

- Systemsteuerung: Hier kann der Zugriff auf die Systemsteuerungsoption „Anzeige“ beschränkt werden. Wenn diese Option gewählt wurde, können noch zusätzlich die Registerkarten „Hintergrund“, „Bildschirmschoner“, „Darstellung“ und „Einstellungen“ einzeln ausgeblendet werden, und die Option „Anzeige“ kann auch als Ganzes deaktiviert werden. Normalen Benutzern sollte der Zugriff auf die Systemsteuerung entzogen werden, da unbeabsichtigte Änderungen an den Systemeinstellungen Probleme verursachen können. Wenn zusätzlich der Zugriff auf die Systemsteuerungsoption „Anzeige“ bzw. die Registerkarte „Bildschirmschoner“ entzogen wird, kann verhindert werden, daß Benutzer die Bildschirmsperre deaktivieren. Dann muß der Administrator natürlich beim Einrichten von Benutzern die Bildschirmsperre aktivieren.

- Shell: Hier können folgende Einschränkungen festgelegt werden:
  + Befehl „Ausführen“ entfernen
  + Ordner unter Einstellungen im Menü „Start“ entfernen
  + „Task-Leiste“ unter Einstellungen im Menü „Start“ entfernen
  + Befehl „Suchen“ entfernen
  + Laufwerke im Fenster „Arbeitsplatz“ ausblenden
  + Netzwerkumgebung ausblenden
  + Kein Symbol „Gesamtes Netzwerk“ in der Netzwerkumgebung

+ Keine Arbeitsgruppen-Computer in Netzwerkumgebung
+ Alle Desktop-Elemente ausblenden
+ Befehl „Beenden“ deaktivieren
+ Keine Einstellungen beim Beenden speichern

- System: Hier können folgende Einschränkungen festgelegt werden:
  + Programme zum Bearbeiten der Registrierung deaktivieren
  + Nur zugelassene Anwendungen für Windows ausführen

  Für normale Benutzer sollte kein Zugriff auf die Registrierung möglich sein, da Änderungen an der Registrierung schwerwiegende Probleme verursachen können.
  Die meisten Benutzer müssen mit dem IT-System nur bestimmte Aufgabe wahrnehmen und benötigen dem entsprechend nur bestimmte Anwendungen. Daher sollte ihr Zugriff auch auf diese Anwendungen, wie z.B. ein Textverarbeitungsprogramm, eingeschränkt werden.

- Windows NT Shell: Hier können folgende Einschränkungen festgelegt werden:
  + Nur erlaubte Shell-Erweiterungen verwenden
  + Allgemeine Programmgruppen vom Menü „Start“ entfernen

Unter Windows NT können sehr differenzierte Benutzerprofile erstellt werden. Diese sollten entsprechend der Sicherheitspolitik der Behörde bzw. des Unternehmens erarbeitet werden. Dies kann zeitaufwendig sein, da für verschiedene Benutzergruppen auch jeweils auf diese zurechtgeschnittene Benutzerprofile erstellt werden sollten. Alle Benutzerprofile müssen vorher darauf getestet werden, ob diese weder Lücken offenlassen noch die Benutzer an ihrer Aufgabenerfüllung hindern. Es ist auch zu bedenken, daß zu weitgehende Einschränkungen nicht nur zur Unzufriedenheit der Benutzer bis hin zur völligen Ablehnung des Systems führen können, sondern auch den Administratoren viel Arbeit verursachen können, wenn diese ständig Benutzerwünsche umsetzen müssen, wie z.B. eine andere Schriftgröße einstellen.

Die Windows NT Umgebung wird durch die Werte des aktuellen Benutzerprofils festgelegt, selbst wenn der aktuelle Benutzer weder über ein vorgeschriebenes noch über ein persönliches Profil verfügt oder auch wenn aktuell niemand eingeloggt ist. Das User Default Profil wird unter den folgenden Bedingungen geladen:

- wenn der aktuelle Benutzer über kein eigenes (vorgeschriebenes oder persönliches) Profil verfügt und sich noch nie auf dem aktuellen Rechner eingeloggt hat;

- wenn ein Benutzer sich auf dem Gastkonto einloggt.

Im ersten Fall werden die aktuellen Werte der Benutzerumgebung beim Ausloggen in ein neu erstelltes lokales persönliches Profil abgespeichert, im zweiten Fall gehen sie beim Ausloggen verloren.

Wenn niemand eingeloggt ist, werden die aktuellen Werte für den Bildschirmhintergrund und andere Umgebungsvariablen durch das System Default Profil bestimmt.

M 4.52 Geräteschutz unter Windows NT
Normalerweise erlaubt Windows NT allen Programmen den Zugriff auf Disketten und CD-ROMs. Es ist empfehlenswert, diesen Zugriff auf den gerade interaktiv eingeloggten Benutzer zu beschränken, indem die Geräte diesem Benutzer beim Anmelden exklusiv zugeordnet werden.

Der Zugriff auf Diskettenlaufwerke sollte unter Windows NT 4.0 durch Eintrag / Veränderung des Wertes „AllocateFloppies“ im Schlüssel
SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon des Bereiches
HKEY_LOCAL_MACHINE der Registrierung auf den Wert REG_Zeichenfolge = 1 eingeschränkt werden.
Hinweis: Der Typ „REG_Zeichenfolge“, wie er in dem Programm Regedit.exe verwandt wird, entspricht dem Typ „REG_SZ“ im Programm Regedt32.exe.

Analog sollte der Zugriff auf CD-ROM-Laufwerke durch Eintrag/Veränderung des Wertes „AllocateCdRoms“ im Schlüssel SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon des Bereiches HKEY_LOCAL_MACHINE der Registrierung auf den Wert REG_Zeichenfolge = 1 bei Bedarf eingeschränkt werden.
Hinweis: Da die Geräte beim Abmelden wieder für den allgemeinen Zugriff freigegeben werden, müssen die Datenträger vor dem Abmelden aus den Geräten entfernt werden.

Sofern Diskettenlaufwerke vollständig abgeschaltet werden sollen, kann dies auch dadurch geschehen, daß in der Systemsteuerungsoption „Geräte“ das Laden des Treiberprogramms dadurch unterbunden wird, daß dem Gerät „Floppy“ die Startart „Deaktiviert“ zugewiesen wird. Nach dem nächsten Systemstart steht dann das Diskettenlaufwerk überhaupt nicht mehr zur Verfügung, und es kann nur von einem Administrator durch Zuweisen der Startart „System“ wieder nutzbar gemacht werden. Auf Servern sollte davon abgesehen werden, das Laden des Treiberprogramms für das Diskettenlaufwerk zu unterbinden. Sofern das Diskettenlaufwerk doch einmal z.B. zum Zwecke der Administration gebraucht wird, muß dem Gerät „Floppy“ die Startart „System“ zugewiesen werden und der Server muß heruntergefahren werden, da der Treiber erst beim Neustart wieder geladen wird. Dies kann zu Störungen des Dienstbetriebes führen. Server müssen in einer gesicherten Umgebung aufgestellt werden, vorhandene Diskettenlaufwerke sollten durch ein entsprechendes Schloß verschlossen werden.
Weiterhin erlaubt Windows NT allen Benutzern den Zugriff auf Bandlaufwerke, so daß jeder Benutzer den Inhalt jedes Bandes lesen und schreiben kann. Normalerweise bringt dies keine Probleme mit sich, da zu einem gegebenen Zeitpunkt jeweils nur ein Benutzer interaktiv angemeldet ist. Sofern dieser jedoch ein Programm laufen läßt, das auch nach dem Ausloggen noch auf das Bandlaufwerk zugreift, so kann dieses Programm möglicherweise auf ein Band zugreifen, das der nächste Benutzer, der sich anmeldet, auflegt. Aus diesem Grund sollten Rechner, die sich nicht in einer kontrollierten Umgebung befinden, neu gestartet werden, ehe das Bandlaufwerk genutzt wird.

Hinweis: Der Einsatz von selbstladenden Bandgeräten, die mehrere Bänder aus einem Reservoir laden können, darf nur unter sehr genau kontrollierten Randbedingungen zugelassen werden. In der Regel sollten derartige Geräte nur zur Datensicherung an einem Server installiert werden. Der interaktive Zugriff normaler Benutzer auf diesen Server ist nicht zulässig (siehe auch M 6.32 - Regelmäßige Datensicherung).

M 4.53 Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT

In Windows NT wird zwischen den Zugriffsberechtigungen auf Freigabeebene und den Zugriffsberechtigungen auf Datei- und Verzeichnisebene, die im folgenden auch NTFS-Berechtigungen genannt werden, unterschieden. Die Zugriffsberechtigungen auf Freigabeebene (Shares) werden in M 2.94 - Freigabe von Verzeichnissen unter Windows NT betrachtet.

Zugriffsberechtigungen auf Datei- und Verzeichnisebene stehen im Gegensatz zu den Freigabeberechtigungen (Share-Berechtigungen) nur auf Datenträgern mit dem Dateisystem NTFS zur Verfügung. Sie werden in der Regel vom Ersteller oder Besitzer eines Objektes (Verzeichnis oder Datei) vergeben. Auf Servern erfolgt dies meistens durch den Administrator. Die Festlegung von NTFS-Berechtigungen erfolgt unter Windows NT 4.0 typischerweise mittels des Windows NT Explorers oder über das Desktopsymbol „Arbeitsplatz“ . Im Kontextmenü des entsprechenden Verzeichnisses bzw. der entsprechenden Datei ist der Menüpunkt „Eigenschaften“ /„Sicherheit“ auszuwählen. Dadurch gelangt man zur Zugriffskontrolliste in Abb. 1.

Die entsprechende Zugriffskontrolliste findet sich unter Windows NT 3.51 im Datei-Manager unter „Sicherheit“ /„Berechtigungen“ . In diese Zugriffskontrolliste können bestehende Benutzergruppen und Benutzer aufgenommen und hier können jeder Benutzergruppe und jedem Benutzer Berechtigungen zugewiesen und entzogen werden. Auch ist es möglich, Benutzergruppen und Benutzer aus der Zugriffskontrolliste zu entfernen. Durch Aktivieren der Option „Berechtigungen für existierende Dateien ersetzen“ können die für das Verzeichnis festgesetzten Berechtigungen auf alle Dateien dieses Verzeichnisses übertragen werden. Wird die Option „Berechtigungen für Unterverzeichnisse ersetzen“ gewählt, werden die eingestellten Berechtigungen zudem auf alle Unterverzeichnisse übertragen. Auf diese Weise lassen sich leicht einheitliche Rechtestrukturen realisieren.

NTFS-Berechtigungen werden zunächst beim lokalen Zugriff wirksam. Müssen z.B. mehrere Benutzer an einem Computer arbeiten, so ist es möglich, durch Vergabe entsprechender Datei- und Verzeichnisberechtigungen sicherzustellen, daß jeder Benutzer nur Zugriff auf seine Daten hat.

Auch beim Zugriff über das Netz werden NTFS-Berechtigungen wirksam. Voraussetzung für den Netzzugriff ist aber, daß das Verzeichnis, auf das zugegriffen werden soll oder in dem sich das gewünschte Unterverzeichnis oder die gewünschte Datei befindet, zuvor freigegeben und mit einer entsprechenden Freigabeberechtigung versehen wurde (s. M 2.94 - Freigabe von Verzeichnissen unter Windows NT). Im Zusammenspiel zwischen Freigabeberechtigung und

NTFS-Berechtigung ist zu beachten, daß die jeweils restriktivere Berechtigung maßgebend ist. NTFS-Berechtigungen lassen sich feiner abstufen als Freigabeberechtigungen. Es ist insbesondere möglich, für jedes Unterverzeichnis und für jede Datei gesonderte NTFS-Berechtigungen zu vergeben. Von daher ist es auch möglich, Freigaben mit der Freigabeberechtigung „Vollzugriff“ für die Gruppe der Benutzer bzw. Domänen-Benutzer zu versehen und die effektiven Zugriffsrechte über die NTFS-Berechtigungen zu vergeben.

Die NTFS-Berechtigungen werden unterschieden in spezifische (auch individuelle) Berechtigungen und vordefinierte Standardberechtigungen, die Kombinationen der spezifischen Zugriffsberechtigungen darstellen.
Es gibt folgende individuellen Berechtigungen:
R – Lesen
W – Schreiben
X – Ausführen
D – Löschen
P – Berechtigungen ändern
O – Besitz übernehmen

Aus diesen Einzelberechtigungen sind unter Windows NT vorgegebene Standardberechtigungen kombiniert worden:

Standardberechtigung	Einzelberechtigungen
Kein	Zugriff
Lesen	RX
Ändern	RWXD
Anzeigen	RX
Hinzufügen	WX
Hinzufügen und Lesen	RWX
Vollzugriff	RWXDPO

Der Besitzer einer Datei bzw. eines Verzeichnisses hat in jedem Fall das Recht, Berechtigungen für die Datei bzw. das Verzeichnis zu vergeben und zu entziehen. Jeder, der ein Verzeichnis oder eine Datei erstellt, wird automatisch Besitzer dieser Ressource. Der Besitz an einem Verzeichnis bzw. an einer Datei kann durch „Besitz übernehmen“ (P) an andere Benutzer übertragen werden. Der Besitz an einem Verzeichnis oder einer Datei geht allerdings erst durch die Besitzübernahme durch den Empfänger auf diesen über. Es ist im Gegensatz zu anderen Betriebssystemen nicht möglich, Dateien und Verzeichnisse zu verschenken. Unabhängig von den Eintragungen in der Zugriffskontrolliste können Administratoren in jedem Fall den Besitz an Dateien und Verzeichnissen übernehmen.

Hinweis:
Benutzer sollten möglichst nie die Berechtigung „Vollzugriff“ vergeben, sondern höchstens die Berechtigung „Ändern“ , damit ihnen nicht der Besitz entzogen werden kann und sie immer die Hoheit über die Rechtevergabe behalten.

Alle Benutzer müssen darauf aufmerksam gemacht werden, regelmäßig mit dem Dateimanager oder dem Explorer zu überprüfen, ob sie noch Besitzer ihrer Verzeichnisse und Dateien sind. Dies ist der einzige Weg, mit dem Benutzer erkennen könne, ob von Ihnen gesetzte Zugriffsrechte umgangen worden sind.

Die in den folgenden Abschnitten genannten Maßnahmen gelten hauptsächlich für Dateien und Verzeichnisse, für die der Administrator zuständig ist, das heißt für solche, die entweder für alle Benutzer von Bedeutung sind oder die Administrationszwecken dienen. Es reicht nicht aus, die Rechte eines Programms zu überprüfen, es muß auch die Rechtevergabe aller Programme überprüft werden, die von diesem Programm aus aufgerufen werden (insbesondere zur Vermeidung Trojanischer Pferde).
Die Attribute aller Systemdateien sollten möglichst so gesetzt sein, daß nur der Systemadministrator Zugriff darauf hat. Verzeichnisse dürfen nur die notwendigen Privilegien für die Benutzer zur Verfügung stellen.

Verzeichnisse des Betriebssystems und der Anwendungsprogramme

Die Dateien und Verzeichnisse des Betriebssystems selbst müssen gegen unzulässige Zugriffe hinreichend geschützt werden. Die standardmäßig vorgesehenen Zugriffsrechte sollten unmittelbar nach der Installation des Systems auf schärfere Formen der Zugriffskontrolle auf die betreffenden Dateien und Verzeichnisse (das Windows-Verzeichnis, %SystemRoot%, z.B. \WINNT, das Windows-Systemverzeichnis %SystemRoot%\SYSTEM32 und eventuelle weitere Programmverzeichnisse, z.B. \MsOffice und \Programme, und alle Unterverzeichnisse) eingestellt werden.

Dabei ist jedoch zu beachten, daß manche Programme, insbesondere 16-Bit Programme, aber auch z.B. MS Winword 7.0, im Windows-Verzeichnis und/oder im Programmverzeichnis Initialisierungs- und Konfigurationsdateien anlegen. Sollen solche Programme genutzt werden, so kann es erforderlich werden, den Benutzern das Zugriffsrecht „Ändern“ auf die betreffenden Verzeichnisse und Dateien zu geben.

Nur Administratoren dürfen auf diese Dateien und Verzeichnisse schreibenden Zugriff haben. Für alle anderen Benutzer ist der Zugriff so einzuschränken, daß sie dort nur lesenden und ausführenden Zugriff (RX) haben:

Benutzer(gruppe)	Zugriffsrecht
SYSTEM	Vollzugriff
Administratoren	Vollzugriff
Benutzer	Lesen

Ggf. kann der Zugriff auf ausführbare Dateien (.EXE-, COM- und BAT-Dateien) noch weiter eingeschränkt werden, so daß nur ausführender Zugriff (X) auf diese Dateien möglich ist. In ähnlicher Weise sind die für den Systemstart kritischen Dateien \BOOT.INI, \NTDETECT.COM, \NTLDR, \AUTOEXEC.BAT und \CONFIG.SYS gegen unbefugte Veränderung durch unprivilegierte Benutzer zu schützen.

Dabei sollte allerdings - am besten in einer Testumgebung - überprüft werden, ob alle Anwendungsprogramme bei dieser restriktiven Einstellung noch lauffähig sind, oder ob einzelne Zugriffskontrollen doch um weitere Zugriffsmöglichkeiten ergänzt werden müssen, um beispielsweise die Abspeicherung temporärer Dateien oder von Konfigurationsinformationen in einem Programmverzeichnis zu erlauben. Generell sollte jedoch der Zugriff auf die Programmdateien selbst (.EXE-Dateien) und auf dynamische Bibliotheken (.DLL-Dateien) für die Gruppe „Jeder" auf lesenden Zugriff beschränkt werden, zumal diese Maßnahme auch einen gewissen Schutz gegen die Verbreitung von Viren bietet.

Temporäre Dateien

Temporäre Dateien, die von verschiedenen Anwendungsprogramme zum Auslagern und Zwischenspeichern von Daten verwendet werden, werden unter Windows NT im Verzeichnis %TEMP% (in der Regel C:\TEMP) abgelegt. Alle Anwender benötigen für dieses Verzeichnis auch das Recht, hier Dateien abzulegen, doch muß gleichzeitig verhindert werden, daß Benutzer auf temporäre Dateien anderer Benutzer Zugriff erhalten. Die Zugriffsrechte für das Verzeichnis sollten daher auf folgenden Wert geändert werden:

Benutzer(gruppe)	Zugriffsrecht
SYSTEM	Vollzugriff
Administratoren	Vollzugriff
Ersteller/Besitzer	Ändern
Benutzer	Hinzufügen

Registrierung

Die Registrierung von Windows NT befindet sich im Unterverzeichnis CONFIG des Windows-Systemverzeichnisses
%SystemRoot%\SYSTEM32, d.h. im allgemeinen im Verzeichnis
C:\WINNT\SYSTEM32\CONFIG. Auf dieses Verzeichnis muß der Anwender Zugriff haben, da die Registrierung automatisch durch Einstellungen des Benutzers in Anwendungsprogrammen geändert wird. Kann der Benutzer nicht auf dieses Verzeichnis zugreifen, führt das zu Systemfehlern oder zu einem Absturz des Systems. Die auf dieses Verzeichnis gesetzten Standardrechte, die möglichst nicht verändert werden sollten, sind unter Version 3.51:

Benutzer(gruppe)	Zugriffsrecht
SYSTEM	Vollzugriff
Administratoren	Vollzugriff
Ersteller/Besitzer	Ändern
Benutzer	Anzeigen

Ab Version 4.0 sind die Standardrechte:

Benutzer(gruppe)	Zugriffsrecht
SYSTEM	Vollzugriff
Administratoren	Vollzugriff
Ersteller/Besitzer	Vollzugriff
Jeder	Anzeigen

Die Gruppe „Jeder“ sollte allerdings durch die Gruppe „Benutzer“ ersetzt werden. Nur wenn Gäste auf dieses Verzeichnis Zugriff haben, muß die Gruppe „Jeder“ das Recht „Anzeigen“ haben.

Bei der Installation legt Windows NT das Verzeichnis %SystemRoot%\REPAIR an, um dort Konfigurationsinformationen abzuspeichern, die für eine ggf. notwendige Reparatur einer bestehenden Installation benötigt werden. Diese Dateien werden mit Hilfe des Dienstprogramms RDISK aktualisiert (siehe auch M 6.42 - Erstellung von Rettungsdisketten für Windows NT). Da da mit Hilfe dieser Dateien und entsprechender Schadsoftware Sicherheitsfunktionalitäten von Windows NT außer Kraft gesetz werden können, sollten die Rechte auf das Verzeichnis mit allen darin befindlichen Dateien wie folgt gesetzt werden:

Benutzer(gruppe)	Zugriffsrecht
System	Vollzugriff
Administratoren	Vollzugriff

Profile

Zum Abspeichern der Daten, die die Benutzeroberfläche und Einträge im Menü START ab der Version 4.0 beschreiben, legt Windows NT für jeden Benutzer vom System ein eigenes Profilverzeichnis im Unterverzeichnis Profiles des Windows-Verzeichnisses %SystemRoot% (in der Regel C:\WINNT\PROFILE) an. Unter der Version 3.51 werden Profile in Unterverzeichnissen des Systemverzeichnisses %SystemRoot%\SYSTEM32\CONFIG bzw. in für die einzelnen Benutzer explizit angegebenen Verzeichnissen abgespeichert. Auf diese Verzeichnisse muß der Benutzer vollen Zugriff haben, sofern er seine Benutzeroberfläche selbst verändern können soll. Dies ist jedoch nicht immer gewünscht (vgl. M 4.51 - Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT). Beim ersten Anmelden des Benutzers wird sein Benutzerprofil automatisch vom System erzeugt. Die Standard-Zugriffsrechte für das Verzeichnis sehen wie folgt aus:

Benutzer(gruppe)	Zugriffsrecht
SYSTEM	Vollzugriff
Administratoren	Vollzugriff
betreffender Benutzer	Vollzugriff

Neben dem Profilverzeichnis für den einzelnen Benutzer gibt es noch ein Verzeichnis für alle Benutzer (All Users) und ein Verzeichnis als Vorlage für neue Benutzer (Default User). Schreibenden Zugriff auf diese Verzeichnisse sollte nur Systemverwalter haben. Die Zugriffsrechte sollten wie folgt gesetzt werden:

Benutzer(gruppe)	Zugriffsrecht
SYSTEM	Vollzugriff
Administratoren	Vollzugriff
Benutzer	Lesen

Diese Einstellungen sollten nur verändert werden, wenn man dem Anwender das Recht nehmen möchte, seine Benutzeroberfläche zu verändern.

Benutzer-Verzeichnisse

Die Verzeichnisse für die Daten der einzelnen Benutzer sollten in der Regel so geschützt werden, daß nur die betreffenden Benutzer auf ihre Dateien zugreifen können. Andere Benutzer, auch Administratoren benötigen in der Regel keinen Zugriff auf die Daten eines Benutzers, es sei denn, daß dieser selbst explizit zusätzliche Zugriffsrechte vergibt. Damit ist in den meisten Fällen die folgende Voreinstellung für die Zugriffsrechte auf Benutzerverzeichnisse ausreichend:

Benutzer(gruppe)	Zugriffsrecht
SYSTEM	Vollzugriff
betreffender Benutzer	Vollzugriff

Benutzer, die einzelne Dateien oder Verzeichnisse anderen Benutzern zugänglich machen wollen, sollten hierfür Verzeichnisse außerhalb ihres Basisverzeichnisses einrichten. Ebenso sollten für Projektgruppen, die gemeinsam an bestimmten Dateien arbeiten, spezielle Verzeichnisse eingerichtet werden. Die Zugriffsrechte auf solche Verzeichnisse sollten auch wiederum explizit auf die Benutzer in diesen Gruppen beschränkt werden.

Sperren der Zugriffsrechte für Gäste

Bei den oben beschriebenen Zugriffskontrollisten ist davon ausgegangen worden, daß keine Benutzer der Gruppe „Gäste“ zugelassen sind. Deswegen ist die Gruppe „Jeder“ durch die Gruppe „Benutzer“ zu ersetzen. Mit dieser Maßnahme wird Gästen effektiv jede Möglichkeit zur Arbeit mit dem System und zum Zugriff auf Daten entzogen. Da dies jedoch unter Umständen dazu führen kann, daß bestimmte Anwendungssoftware nicht mehr korrekt läuft, sollte eine derartige Änderung zuerst an einem Testsystem vorgenommen und hinsichtlich ihrer Auswirkungen überprüft werden, ehe sie allgemein umgesetzt wird.

M 4.54 Protokollierung unter Windows NT

Die für die Protokollierung sicherheitsrelevanter Ereignisse festgelegten Regelungen können mit Hilfe der Option „Richtlinien“ des Benutzer-Managers umgesetzt werden, wobei für den mittleren Schutzbedarf geeignete Regelungen im allgemeinen denen der Abbildung 1 entsprechen.

Sofern auf einem Rechner Daten mit höheren Schutzanforderungen gespeichert und/oder verarbeitet werden, sollten zusätzlich noch erfolgreiche und abgewiesene Datei- und Objektzugriffe aufgezeichnet werden. Dabei sollte sich diese Aufzeichnung auf die Dateien, die besonders

schutzwürdige Informationen enthalten, sowie auf die zur Verarbeitung dieser Dateien benötigten Programme beschränken, damit die Protokolldatei nicht so umfangreich wird, daß sie nicht mehr mit tragbarem Aufwand auswertbar ist.

Bei höheren Sicherheitsanforderungen sollten auch Zugriffe und Zugriffsversuche auf die Registrierung, zumindest für die Schlüssel HKEY_LOCAL_MACHINE und HKEY_USERS, aufgezeichnet werden. Dabei empfiehlt es sich, alle abgewiesenen Versuche aufzuzeichnen und von den erfolgreichen zumindest die folgenden, die zu Veränderungen der Registrierung führen können (Abbildung 2):

Dabei ist zu beachten, daß Zugriffe auf die Registrierung nur dann aufgezeichnet werden, wenn bei den allgemeinen Überwachungsrichtlinien die Überwachung der Datei- und Objektzugriffe aktiviert ist.

Die Protokolldatei sollte durch Festlegung entsprechender Vorgaben mit dem Dienstprogramm Ereignisanzeige so groß angelegt werden, daß alle innerhalb eines vorgegebenen Zeitraums (beispielsweise in einer Woche) anfallenden Einträge mit Sicherheit abgespeichert werden können. Dabei sollte ein Sicherheitsspielraum vorgesehen werden, so daß in der Regel maximal nur etwa 30 % der Protokolldatei gefüllt werden. Nach Ablauf des vorgesehenen Zeitraums ist die Protokolldatei jeweils zu analysieren, zu archivieren und dann zu leeren, um Platz für neue Einträge zu schaffen. Um Systemausfälle durch Vollschreiben der Protokolldatei zu vermeiden, sollte normalerweise eine der Optionen „Überschreiben falls notwendig“ oder „Überschreiben älter als x Tage“ , wobei für x die Länge des vorgesehenen Archivierungszyklus, z.B. 30 Tage, angegeben wird, gewählt werden (Abbildung 3):

Für Systeme, für die erhöhte Sicherheitsanforderungen bestehen, sollte statt dessen die Option „Nie überschreiben (Protokoll manuell löschen)“ gewählt werden, was allerdings zum Systemstillstand bei Überlauf des Logs führt und dann einen entsprechenden Aufwand verursacht. Die Auswertung der Protokolle erfolgt mit dem Verwaltungsprogramm Ereignisanzeige, das durch Auswahl geeigneter Filterregeln die gezielte Auswertung sicherheitskritischer Vorgänge ermöglicht (Abbildung 4):

Die Auswertung des Sicherheitsprotokolls sollte einer geeigneten, allgemein verbindlichen Vorgabe folgen (siehe M 2.64 - Kontrolle der Protokolldateien und M 2.92 - Durchführung von Sicherheitskontrollen im Windows NT Client-Server-Netz).

M 4.55 Sichere Installation von Windows NT

Vor der Installation von Windows NT sollten einige Überlegungen getroffen werden, die im folgenden kurz dargestellt werden.

Sichere Systemversion

Schon bei der Beschaffung muß entschieden werden, ob Windows NT in der englischen oder in der deutschen Version zum Einsatz kommen soll. Außerderm muß Windows NT, um sicher zu

sein, wenigstens in der Version 3.51 mit dem jeweils aktuellen Service Pack betrieben werden (siehe auch M 4.76 - Sichere Systemversion von Windows NT). Sofern eine ältere Windows NT Installation vorhanden ist, sollte diese nach Möglichkeit auf die Version 4 oder zumindest auf die Version 3.51 aktualisiert werden.

Partitionen und Dateisysteme
Windows NT unterstützt neben dem eigenen Dateisystem NTFS auch das DOS-Dateisystem FAT und das OS/2-Dateisystem HPFS. Ein Großteil der sicherheitsrelevanten Einstellungen ist allerdings nur unter NTFS gültig. Bei der Installation von Windows NT ist daher zu beachten, daß keine HPFS- oder DOS-Partitionen angelegt werden, da für diese kein Zugriffsschutz gilt, so daß derartige Partitionen zum Unterlaufen des Schutzes von Windows NT mißbraucht werden können. Statt dessen müssen alle Partitionen mit dem NTFS-Dateisystem formatiert oder, sofern frühere Daten beibehalten werden sollen, zu diesem Dateisystem konvertiert werden.
Allerdings ist die Unterstützung des FAT-Dateisystems für Disketten notwendig, da das NTFS-Dateisystem aufgrund seiner Größe nicht auf Disketten untergebracht werden kann. Daher sollte der Zugriff auf Diskettenlaufwerke beschränkt werden (s. M 4.52 - Geräteschutz unter Windows NT).

Konfiguration des Anmelde-Vorgangs
Normalerweise zeigt Windows NT beim Anmelden den Namen des letzten Benutzers an, der sich am betreffenden Rechner eingeloggt hat. Diese Anzeige sollte durch Eintrag/Veränderung des Wertes „DontDisplayLastUserName“ im Schlüssel
SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon des Bereiches
HKEY_LOCAL_MACHINE der Registrierung auf den Wert REG_SZ = „1“ verhindert werden.
Um unberechtigte Benutzer vor einem unzulässigen Zugriff auf das System zu warnen, sollte vor dem eigentlichen Anmelde-Vorgang ein Fenster mit einem geeigneten Text angezeigt werden. Dies wird durch Eingabe geeigneter Texte in die beiden Einträge „LegalNoticeCaption“ und „LegalNoticeText“ im Schlüssel SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon des Bereiches
HKEY_LOCAL_MACHINE der Registrierung erreicht.
Die betreffenden Änderungen können mit Hilfe des Registrierungs-Editors (des Programms REGEDT32.EXE im Windows-Systemverzeichnis %SystemRoot%\SYSTEM32) vorgenommen werden. Dabei ist besondere Vorsicht anzuwenden, da fehlerhafte Einstellungen in der Registrierung dazu führen können, daß das System nicht mehr lauffähig ist. Ab der Version 4.0 von Windows NT können diese Werte mit Hilfe des Systemrichtlinien-Editors zentral für die einzelnen Arbeitsstationen vorgegeben werden.

Laden von Subsystemen
Die optionalen Subsysteme POSIX und OS/2 sollten nur dann installiert bleiben, wenn sie zur Durchführung von Anwendungen auch tatsächlich benötigt werden. Sofern dies nicht der Fall ist, sollte auf ihre Installation verzichtet werden, oder die Systeme sollten, falls diese schon erfolgt ist, wieder gelöscht werden. Dazu sind dann die Unterverzeichnisse POSIX bzw. OS2

des Windows-Systemverzeichnisses %SystemRoot%\SYSTEM32 mit ihren eventuellen Unterverzeichnissen zu löschen. Weiterhin sind die folgenden Programme und ladbaren Bibliotheken im Windows-Verzeichnis %SystemRoot%\SYSTEM32 zu löschen:

- OS/2:
  OS2.EXE, OS2SRV.EXE, OS2SS.EXE
- POSIX:
  PSXDLL.DLL, PAX.EXE, POSIX.EXE, PXSS.EXE

Starten von Diensten
Sofern Dienste, die keine Standarddienste von Windows NT sind, konfiguriert werden sollen, sollte bei Festlegung der Startart dieser Dienste (mit der Systemsteuerungsoption „Dienste“) nach Möglichkeit ein eigenes Benutzerkonto zum Start jedes dieser Dienste vorgesehen werden, um die Befugnisse des betreffenden Dienstes geeignet einschränken zu können. Das dabei verwendete Benutzerkonto muß über das Recht „Als Dienst starten“ verfügen, und es sollte außer für diesen Dienst nicht verwendet werden, also insbesondere auch kein Login von Benutzern zulassen. Dienste, die nicht auf diese Weise einem speziellen Benutzerkonto zugeordnet wurden, laufen im Kontext der speziellen Benutzergruppe SYSTEM (siehe M 4.50 - Strukturierte Systemverwaltung unter Windows NT), also in der Regel mit sehr weitgehenden Zugriffsberechtigungen.

Geräteschutz
Sofern der Computer über Diskettenlaufwerke, CD-ROM-Laufwerke und/oder Bandlaufwerke verfügt, sollten diese nach Möglichkeit spezifisch geschützt werden, wie in der Maßnahme M 4.52 - Geräteschutz unter Windows NT beschrieben.

Notfalldiskette
Bei der Installation bietet Windows NT an, eine Notfalldiskette mit den wichtigsten Konfigurationsinformationen zu erzeugen. Von dieser Möglichkeit sollte Gebrauch gemacht werden und die Diskette sollte bei Änderungen am System jeweils aktualisiert werden (siehe M 6.42 - Erstellung von Rettungsdisketten für Windows NT). Dabei empfiehlt es sich, die Aktualisierung der Notfalldiskette jeweils nach dem nächsten Systemstart vorzunehmen, wenn also sichergestellt ist, daß sich daß geänderte System noch starten läßt.

Vordefinierte Benutzerkonten
Das vordefinierte Administratorkonto ist Mitglied der vordefinierten Gruppe „Administratoren“. Es erhält die Rechte und Berechtigungen, die dieser Gruppe erteilt wurden. Das Administratorkonto wird von der Person verwendet, welche die Gesamtkonfiguration der Arbeitsstation oder des Servers verwaltet. Der Administrator besitzt mehr Kontrollmöglichkeiten über den Windows NT Computer als jeder andere Benutzer. Daher ist dieses Konto besonders zu schützen (siehe M 4.77 - Schutz der Administratorkonten unter Windows NT).Das vordefinierte Gastkonto ist Mitglied der Gruppe „Gäste“. Es erhält die Rechte und Berechtigungen, die dieser Gruppe erteilt wurden. Beispielsweise kann sich ein Benutzer beim Gastkonto anmelden,

Dateien erstellen und diese wieder löschen sowie Dateien lesen, für die ein Administrator den Gästen die Leseerlaubnis erteilt. Das Gastkonto wird als Service für Benutzer eingerichtet, die gelegentlich oder nur einmal den Rechner benutzen, so daß diese sich anmelden und mit eingeschränktem Funktionsumfang arbeiten können. Das Gastkonto ist bei der Installation von Windows NT 4.0 zunächst gesperrt, und es wird mit einem leeren Kennwort installiert. Das Gastkonto ist auf jeden Fall mit einem sicheren Paßwort zu versehen, und die Sperre sollte nicht aufgehoben werden, wenn es keine schwerwiegenden Gründe für seine Benutzung gibt. Das vordefinierte Gastkonto kann umbenannt, aber nicht gelöscht werden. Es sollte unmittelbar nach der Installation umbenannt werden.
Das Erstbenutzerkonto wird für den ersten Benutzer einer Arbeitsstation eingerichtet. Da es Mitglied der Gruppe „Administratoren“ ist, kann die Arbeitsstation mit dem Erstbenutzerkonto vollständig verwaltet werden. Das Erstbenutzerkonto wird bei der Installation von Windows NT erstellt, wenn die Arbeitsstation zu einer Arbeitsgruppe hinzugefügt wird oder wenn sie nicht für den Netzbetrieb konfiguriert wurde. Das System fordert zur Eingabe eines Benutzernamens und eines Kennworts auf. Wenn der Rechner bei der Installation von Windows NT zu einer Domäne hinzugefügt wird, wird das Erstbenutzerkonto nicht erstellt, weil erwartet wird, daß sich der Benutzer unter Verwendung eines Kontos von der Domäne anmeldet.

Hinweis: Sofern Windows NT bei der Installation ein Erstbenutzerkonto einrichtet, sollte dieses als Konto zur Systemverwaltung verwendet werden.

Installation im Netz
Weiterhin ist zu beachten, daß alle Clients bei der Konfiguration ihrer Netzsoftware als Mitglieder einer der vorher definierten Domänen (und nicht als Mitglieder von Arbeitsgruppen) konfiguriert werden. Falls auf ihnen Benutzerkonten benötigt werden, müssen diese immer als domänenweite Konten und nicht als lokale Konten definiert werden, um die Entstehung unüberschaubarer Rechtestrukturen zu vermeiden.
Zur Vereinfachung der Installation einer größeren Anzahl von Clients sollten vorher Skripten definiert werden, die eine automatische Installation und Konfiguration dieser Clients ermöglichen. Software aller Art sollte zentral auf einem Server bereitgestellt und von dort aus auf dem entsprechenden Rechner installiert werden.

M 4.56 Sicheres Löschen unter Windows NT und Windows 95

Windows NT
Windows NT legt in einer Master Dateitabelle alle Dateiinformationen wie Namen, Pfad und Attribute ab. Diese Angaben werden nicht verschlüsselt. Programme, die direkt auf die Festplatte zugreifen können, können unter Umgehung der Sicherheitsmechanismen von Windows NT auf alle Dateien beliebig zugreifen. Dies gilt insbesondere für Programme, die unter einem anderen Betriebssystem als Windows NT auf demselben Rechner laufen. Beim Löschen einer Datei unter dem Dateisystem NTFS wird diese nicht physikalisch gelöscht oder überschrieben, sondern ähnlich wie unter MS-DOS lediglich dem Zugriff entzogen, wobei jedoch unter Windows NT „ im Gegensatz zu der Situation bei MS-DOS “ sichergestellt ist, daß ein Zugriff auf diese gelöschten Daten, etwa mit einem Rekonstruktionsprogramm oder unter Verwendung

direkter Plattenzugriffe, nicht mehr möglich ist. Dennoch können gelöschte Dateien unter anderen Betriebssystemen als Windows NT mit Programmen, die direkt auf die Festplatte zugreifen können, wieder hergestellt werden.
Aus diesen Gründen muß Windows NT als einziges Betriebssystem installiert sein, und es muß verhindert werden, daß andere Betriebssysteme von Diskette gestartet werden können (siehe M 4.52 - Geräteschutz unter Windows NT und M 4.55 - Sichere Installation von Windows NT).
Windows 95/ Windows NT
Ab Windows NT Version 4.0 und unter Windows 95 werden Dateien beim Löschen, sofern der Benutzer nicht ausdrücklich ein direktes Löschen verlangt, zunächst in einen benutzerspezifischen Bereich, den sogenannten Papierkorb", verlagert. Aus diesem Bereich werden sie erst dann entfernt, wenn der von gelöschten Dateien belegte Speicherplatz die für das betreffende Plattenlaufwerk vorgegebene Größe überschreitet oder wenn der Benutzer explizit den Papierkorb leert. Der Inhalt des Papierkorbs sollte daher regelmäßig gelöscht werden, damit die Festplatte nicht zu voll wird und der Benutzer nicht den Überblick verliert. Die maximale Größe des für den Papierkorb reservierten Speicherplatzes kann auch unter „Eigenschaften“ des Icons „Papierkorb“ auf einen geeigneten kleineren Wert, z.B. 2 MByte, eingestellt werden. Dateien mit sensitivem Inhalt sollten nicht in den Papierkorb verschoben werden, sondern explizit gelöscht werden, indem beim Löschen die Umschalttaste gedrückt wird.
Unter Windows 95 besteht zudem die Möglichkeit aus dem Papierkorb gelöschte Dateien durch Hilfsprogramme zu rekonstruieren. Dateien mit besonders sensitivem Inhalt sollten daher - bevor sie in den Papierkorb verschoben werden - vollständig überschrieben werden (vgl. M 2.3 - Datenträgerverwaltung).

M 4.57 Deaktivieren der automatischen CD-ROM-Erkennung

Unter Windows 95 und Windows NT 4.0 können CD-ROMs automatisch erkannt und bearbeitet werden. Dadurch können auch auf der CD-ROM gespeicherte Programme automatisch auf dem Rechner ausgeführt werden. Die automatische CD-ROM-Erkennung sollte unter Windows 95 und Windows NT permanent unterbunden werden.
Unter Windows 95 ist dafür auf der Registerkarte Gerätemanager unter der Systemsteuerungsoption System für die CD-ROM die Eigenschaft „Automatische Benachrichtigung beim Wechsel“ zu deaktivieren.
Unter Windows NT 4.0 ist für die permanente Deaktivierung der automatischen CD-ROM-Erkennung in der Registrierung der Eintrag „Autorun“ im Schlüssel
\SYSTEM\CurrentControlSet\Services\Cdrom im Bereich HKEY_LOCAL_MACHINE auf den Wert REG_WORD = 0 zu setzen.
Falls die automatische CD-ROM-Erkennung gewünscht wird, läßt sich die automatische CD-ROM-Erkennung auch für jede CD-ROM einzeln durch Drücken der Shift-Taste beim Einlegen verhindern.

M 4.59 Deaktivieren nicht benötigter ISDN-Karten-Funktionalitäten

Moderne ISDN-Karten sowie deren Kommunikationssoftware bzw. das in das Karten-RAM geladene Betriebssystem besitzen zahlreiche, über die reinen ISDN-Funktionalitäten hinausgehende Leistungsmerkmale. Solche „Komfort-Funktionalitäten“ , welche teilweise auch bei

ausgeschaltetem IT-System angesprochen werden können, sind:

- der Empfang und Versand von Faxen,
- Funktionen eines digitalen Anrufbeantworters,
- das Abhören eingegangener Aufzeichnungen des digitalen Anrufbeantworters,
- das Telefonieren über ein im Lieferumfang der Karte enthaltenes Mikrofon bzw. einen enthaltenen Hörer.

Soweit es möglich ist, sollten nicht benötigte Karten-Funktionalitäten deaktiviert werden, am besten durch das Entfernen des jeweiligen Softwaremoduls. Lassen sich Karten-Funktionalitäten lediglich durch Parameter konfigurieren, so muß die korrekte Einstellung der Parameter regelmäßig geprüft werden.

M 4.60 Deaktivieren nicht benötigter ISDN-Router-Funktionalitäten
Neben Servicefunktionen bzw. der Fernwartung (siehe M 2.108 - Verzicht auf Fernwartung der ISDN-Netzkoppelelemente) können auch Funktionen der Router-Betriebssysteme zu Sicherheitslücken führen. Beispielsweise ist das Aufrufen einer Telnet-Sitzung auf dem Router und das sich anschließende Manipulieren der Management Information Base möglich, wenn dieser mit einem Unix-Betriebssystem ausgestattet ist.
Soweit es möglich ist, sind diese nicht benötigten Funktionalitäten zu deaktivieren, am besten durch das Entfernen des jeweiligen Softwaremoduls. Lassen sich Karten-Funktionalitäten lediglich durch Parameter konfigurieren, so muß die korrekte Einstellung der Parameter regelmäßig geprüft werden.

M 4.61 Nutzung vorhandener Sicherheitsmechanismen der ISDN-Komponenten
Sind gemäß Maßnahme M 2.106 - Auswahl geeigneter ISDN-Karten in der Beschaffung ISDN-Karten mit Sicherheitsfunktionalitäten für das IT-System oder den Router, wie

- Fähigkeit zur Durchführung einer Authentisierung über PAP und CHAP (Password Authentikation Protocol und Challenge Handshake Authentication Protocol, RFC 1994),
- Einsatz eines Verschlüsselungsverfahrens (symmetrisch/asymmetrisch) in Hard- oder Software,
- Möglichkeit der Auswertung von CLIP-Rufnummern (Calling Line Identification Presentation) zur Authentisierung,
- Möglichkeit des Führens einer Rufnummerntabelle für das Durchführen eines Call-Backs und
- Möglichkeit der Protokollierung nicht erfolgreicher Verbindungsaufbauten (Ablehnung aufgrund falscher Rufnummern- oder PAP/CHAP-Authentisierung),

beschafft worden, sollten diese auch geeignet genutzt werden, wie es die Maßnahmen M 5.46 - Authentisierung mittels CLIP/COLP, M 5.47 - Callback basierend auf CLIP/COLP, M 5.48 - Authentisierung mittels PAP/CHAP und M 4.34 - Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen beschreiben. Voraussetzung hierfür ist, daß alle Kommunikationspartner mit ISDN-Karten, die möglichst gleiche Sicherheitsfunktionalitäten aufweisen, ausgestattet werden.

M 4.62 Einsatz eines D-Kanal-Filters

Ein D-Kanal-Filter wird zwischen ISDN-Anschluß (S2M oder S0) und ISDN-Endgerät oder ISDN-TK-Anlage geschaltet. Zum ISDN-Anschluß verhält es sich wie ein ISDN-Endgerät und zum ISDN-Endgerät wie ein ISDN-Anschluß. Der D-Kanal-Filter überwacht den ISDN-D-Kanal auf unzulässige Protokollaktionen und ist damit in der Lage, Manipulationsversuche über den D-Kanal zu detektieren und zu verhindern. Der Einsatz des D-Kanal-Filters ist insbesondere dann sinnvoll, wenn mit qualifizierten Angriffen über Remote-Zugriffe (zum Beispiel bei Fernwartung und -administration) zu rechnen ist.

D-Kanal-Filter schränken weiterhin Leistungsmerkmale und Dienste für Rufnummern bestimmter Kommunikationspartner in der Weise ein, daß es unter konkreten Betriebszuständen nicht zu einem Mißbrauch bzw. zur Gefährdung der ISDN-Endeinrichtung kommen kann. Versuche, unberechtigt Leistungsmerkmale und Dienste zu nutzen, werden von D-Kanal-Filtern mit einem Verbindungsabbau (Disconnect, Release) beantwortet und protokolliert. Weitere Informationen zu dieser vom BSI initiierten Technologie können unter der IT-Grundschutz-Hotline nachgefragt werden.

M 4.64 Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen

Vor dem Versenden einer Datei per E-Mail oder Datenträgeraustausch bzw. vor dem Veröffentlichen einer Datei auf einem WWW-Server sollte diese daraufhin überprüft werden, ob sie Restinformationen enthält, die nicht zur Veröffentlichung bestimmt sind. Solche Restinformationen können verschiedenen Ursprungs sein und dementsprechend unterschiedlich können auch die Aktionen sein, die dagegen zu unternehmen sind. Die häufigsten Ursachen für solche Restinformationen sind im folgenden beschrieben.

Generell sollte Standard-Software wie z.B. für Textverarbeitung oder Tabellenkalkulation darauf überprüft werden, welche Zusatzinformationen in damit erstellten Dateien gespeichert werden. Dabei werden einige dieser Informationen mit, andere ohne Wissen des Benutzers gespeichert. Vor der Weitergabe von Dateien sollten diese zumindest stichprobenartig auf unerwünschte Zusatzinformationen überprüft werden. Dazu sollte ein anderer Editor benutzt werden als der, mit dem die Datei erstellt wurde.

Dabei ist darauf zu achten, daß nicht alle Restinformationen einfach gelöscht werden können, ohne das Dateiformat zu zerstören. Wenn z. B. aus einer Textverarbeitungsdatei einige Bytes gelöscht werden, erkennt das Textverarbeitungsprogramm unter Umständen das Dateiformat nicht mehr. Um Restinformationen zu beseitigen,

- kann die Datei in einem anderen Dateiformat abgespeichert werden, z.B. als „Nur-Text“ oder als HTML,

- können die Nutzdaten in eine zweite Instanz derselben Standard-Software kopiert werden, wobei auf dem IT-System keine andere Applikation laufen sollte. Dies empfiehlt sich insbesondere bei Dateien mit einer größeren Änderungshistorie.

Um der Weitergabe von Informationen vorzubeugen, die ursprünglich mit Wissen der Ersteller eingebracht worden sind, wie z.B. als „verborgen" formatierter Text, dessen Vorhandensein dann aber vergessen wurde, kann es sinnvoll sein, die Datei ausdrucken. Dabei sollten dann alle Optionen aktiviert werden, die beim Drucken versteckte Informationen mitausgeben.

Restinformationen/Slack-Bytes
Jedes Betriebssystem hat eine kleinste physikalische Speichereinheit mit festgelegter Größe. Unter DOS ist dies ein Sektor und umfaßt 512 Byte. Bei Unix-Systemen ist dies ein Block, die Größe eines Blocks hängt dabei von der eingesetzten Unix-Variante ab. Unter DOS werden die einzelnen Sektoren einer Partition logisch zu Zuordnungseinheiten (Cluster) zusammengefaßt. Wieviele Sektoren einen Cluster bilden, hängt von der Größe der Partition ab. Wird eine Datei geöffnet, werden ihr ein oder mehrere Cluster zugeordnet. Die letzte Zuordnungseinheit wird dabei nicht vollständig benutzt, wenn die Dateigröße der zu speichernden Datei nicht zufällig ein Vielfaches der Clustergröße ist.
Dies verbraucht zum einen Speicherplatz. Der durchschnittliche Speicherplatzverbrauch hierdurch steigt mit der Clustergröße. Da diese wiederum mit der Partitionsgröße steigt, sollten Partitionen nicht zu groß sein. Hierzu ein Beispiel: Bei einer Partitionsgröße zwischen 1024 und 2047 MB hat ein einzelner Cluster 32 KB. Damit gehen durchschnittlich bei jeder Datei 16 KB Speicherplatz verloren.
Ein anderes Problem hierbei ist, daß (bei DOS-basierten Betriebssystemen) die restlichen Bytes des letzten Clusters bzw. Blocks mit zufällig im Hauptspeicher stehenden Bytes aufgefüllt werden, sogenannten Slack-Bytes. Diese können sinnlose Einträge, Informationen über die Dateistruktur, aber auch Paßwörter enthalten. Auch bei einem Kopiervorgang von einem Datenträger auf den anderen kann die Datei je nach Clustergröße mit Slack-Bytes aufgefüllt werden.
Vor der Weitergabe von Dateien sollte sichergestellt werden, daß diese keine Slack-Bytes mehr enthalten. Dies kann mit Hilfe eines geeigneten Editors (z.B. Hex-Editor) überprüft werden oder mit dem in der BSI-Mailbox verfügbaren Public-Domain-Programm PRUNE, mit dem die Slack-Bytes gezielt überschrieben werden können.
Daneben haben viele Windows-Applikationen das Problem, daß das jeweilige Programm bei der Bearbeitung einer Datei den in Anspruch genommenen Speicherplatz nicht durchgehend mit Applikationsdaten überschreibt, sondern daß Lücken entstehen können, die ebenfalls alte Datenbestände des IT-Systems enthalten.

Verborgener Text / Kommentare
Eine Datei kann Textpassagen enthalten, die als „versteckt" oder „verborgen" formatiert sind. Einige Programme bieten auch die Möglichkeit an, Kommentare hinzuzufügen, die auf dem Ausdruck und oft auch am Bildschirm ausgeblendet sind. Solche Textpassagen können Bemerkungen enthalten, die nicht für den Empfänger bestimmt sind. Daher müssen in Dateien, bevor sie an Externe weitergegeben werden, solche Zusatzinformationen gelöscht werden.

Änderungsmarkierungen
Bei der Bearbeitung von Dateien kann es sinnvoll sein, hierbei Änderungsmarkierungen zu verwenden. Da diese auf dem Ausdruck und am Bildschirm ausgeblendet werden können, muß vor der Weitergabe von Dateien ebenfalls überprüft werden, ob diese Änderungsmarkierungen enthalten.

Versionsführung
Unter Microsoft Word 97 gibt es die Möglichkeit, verschiedene Versionen eines Dokumentes in einer Datei zu speichern. Dies dient dazu, um bei Bedarf auf frühere Überarbeitungsstände zurückgreifen zu können. Dies kann aber sehr schnell zu riesigen Dateien führen, z.B. wenn Graphiken mitgeführt werden. Auf keinen Fall sollte die Option „Version beim Schließen automatisch speichern“ gewählt werden, da hier bei jedem Schließen einer Datei die komplette Vorgängerversion zusätzlich gespeichert wird.

Dateieigenschaften
Als Dateieigenschaften oder Datei-Info werden in der Datei Informationen gespeichert, die bei späteren Suchen helfen sollen, Dateien wiederzufinden. Dabei können je nach Applikation Informationen wie Titel, Verzeichnisstrukturen, Versionsstände, Bearbeiter (nicht nur der Unterschreibende), Kommentare, Bearbeitungszeit, letztes Druckdatum, Dokumentnamen und -beschreibungen enthalten sein. Einige dieser Informationen werden von den Programmen selber angelegt und können nicht durch den Bearbeiter beeinflußt werden. Andere Informationen müssen manuell eingegeben werden. Vor der Weitergabe einer Datei an Externe ist zu überprüfen, welche zusätzlichen Informationen dieser Art die Datei enthält.

Schnellspeicherung
Textverarbeitungsprogramme nutzen die Option der Schnellspeicherung, um nur die Veränderungen seit der letzten Sicherung und nicht das gesamte Dokument speichern zu müssen. Dieser Vorgang nimmt somit weniger Zeit in Anspruch als ein vollständiger Speichervorgang. Ein vollständiger Speichervorgang erfordert jedoch weniger Festplattenspeicher als eine Schnellspeicherung. Der entscheidende Nachteil ist jedoch, daß die Datei unter Umständen Textfragmente enthalten kann, die durch die Überarbeitung hätten beseitigt werden sollen. Grundsätzlich sollten daher Schnellspeicherungsoptionen abgeschaltet werden.
Entscheidet sich der Benutzer trotzdem für die Schnellspeicheroption, sollte er bei folgenden Situationen immer einen vollständigen Speichervorgang durchführen:

- wenn die Bearbeitung eines Dokuments abgeschlossen ist,
- bevor eine weitere Anwendung ausgeführt wird, die viel Speicherplatz in Anspruch nimmt,
- bevor der Dokumenttext in eine andere Anwendung übertragen wird,
- bevor das Dokument in ein anderes Dateiformat konvertiert wird und

- bevor das Dokument per E-Mail oder Datenträgeraustausch versandt wird.

M 4.65 Test neuer Hard- und Software
Vor dem Einsatz neuer Hardwarekomponenten oder neuer Software müssen diese auf speziellen Testsystemen kontrolliert werden. Neben der Lauffähigkeit des Produktes ist dabei insbesondere zu überprüfen, daß der Einsatz neuer Komponten keine negativen Auswirkungen auf die laufenden IT-Systeme hat. Da vor erfolgreichen Tests Schadfunktionen nicht ausgeschlossen werden können und da bei Tests Fehler provoziert werden, sind immer vom Produktionsbetrieb isolierte Testsysteme zu verwenden.
Der Einsatz isolierter Testsysteme ist auch erforderlich, um selbstextrahierende Dateien, die z.B. per E-Mail empfangen wurden, auf Schadfunktionen zu prüfen.
Generelle Verfahrensweisen für die Software-Abnahme und -Freigabe inklusive des Testens sind in [BSI1998] Kap. 9.1 Standardsoftware beschrieben. Erst nach bestandenem Test dürfen neue Komponenten für die Installation auf Produktionssystemen freigegeben werden.

M 4.67 Sperren und Löschen nicht benötigter Datenbank-Accounts
Datenbank-Accounts, die über einen längeren Zeitraum nicht benutzt werden, sollten gesperrt und später - falls möglich - gelöscht werden. Bei der Sperrung bzw. auf jeden Fall vor dem Löschen eines Datenbank-Accounts sollte der betroffene Benutzer informiert werden.
Wenn ein neu einzurichtender Benutzer seinen Datenbank-Account nur für einen befristeten Zeitraum benötigt, sollte dieser auch nur befristet eingerichtet werden, falls die Datenbank eine solche Möglichkeit zur Verfügung stellt. Es kann vorteilhaft sein, Accounts grundsätzlich nur befristet einzurichten und in regelmäßigen Abständen (z.B. jährlich) bei Bedarf zu verlängern.
Ist absehbar, daß ein Benutzer einer Datenbank längere Zeit abwesend ist (durch Urlaub, Krankheit, Abordnung, o.ä.), so sollte sein Account für diese Zeit im Datenbanksystem gesperrt werden, so daß das Arbeiten unter seiner Benutzerkennung für diese Zeit nicht mehr möglich ist.
Es muß sichergestellt sein, daß der Datenbankadministrator alle längeren Abwesenheitszeiträume von Benutzern mitgeteilt bekommt. Sinnvollerweise sollte dies im Rahmen der üblichen Abwesenheitsmeldungen über die Personalstelle erfolgen.
Darüberhinaus sollte die Datenbankadministration schnellstmöglichst über das endgültige Ausscheiden eines Benutzers informiert werden. Spätestens am letzten Arbeitstag des Benutzers ist dessen Account zu sperren.

M 4.68 Sicherstellung einer konsistenten Datenbankverwaltung
Die Datenbankadministrator-Kennung unterliegt prinzipiell keinerlei Beschränkungen bei der Nutzung des Datenbanksystems, was die Gefahr von Fehlern oder Mißbrauch erhöht. Deshalb sollte auch der Datenbankadministrator neben seiner Administrator-Kennung eine normale Benutzer-Kennung erhalten und nur dann unter der Administrator-Kennung arbeiten, wenn es notwendig ist.
Durch Aufgabenteilung, Regelungen und Absprache ist sicherzustellen, daß Administratoren keine inkonsistenten oder unvollständigen Eingriffe vornehmen. Dabei sollten folgende Bedingungen erfüllt sein:

- Die Art und Weise der Durchführung von Änderungen sowie deren Dokumentation ist festzulegen.
- Art, Umfang und Grund der Änderungen sind zu beschreiben.
- Änderungen an Datenbankobjekten oder Daten sind prinzipiell durch den Verantwortlichen der IT-Anwendung genehmigungspflichtig. Handelt es sich dabei um ein zentrales Datenbankobjekt, so erfordert eine Änderung die Zustimmung aller Verantwortlichen der betroffenen IT-Anwendungen.
- Der Zeitpunkt der geplanten Änderungen ist festzulegen und bekanntzugeben.
- Vor der Durchführung von Änderungen muß die Datenbank komplett gesichert werden.

Um den Mißbrauch weitgehend einzuschränken und Inkonsistenzen zu vermeiden, sollten zusätzlich alle Datenbankobjekte einer Anwendung unter die Verwaltung einer eigens für die jeweilige Anwendung eingerichteten Benutzerkennung gestellt werden. Änderungen an den Datenbankobjekten bleiben somit diesen speziellen Benutzer-Kennungen vorbehalten, so daß selbst unter der Administrator-Kennung der Datenbank keine Modifikationen vorgenommen werden können. Kenntnis über das Paßwort dieser speziellen Benutzer-Kennungen sollte nur derjenige Datenbankadministrator haben, der für die Administration der entsprechenden anwendungsspezifischen Belange verantwortlich ist.

Beispiel:
In einer Datenbank werden die Daten von drei Anwendungen A, B und C verwaltet. Alle Datenbankobjekte, die ausschließlich der Anwendung A zuzuordnen sind, werden unter der Datenbank-Benutzerkennung AnwA eingerichtet und nur über diese Kennung verwaltet. Analog wird mit den Datenbankobjekten der anderen beiden Anwendungen verfahren. Auf diese Weise können an den Datenbankobjekten der drei Anwendungen nur mittels der jeweiligen Datenbank-Benutzerkennung Modifikationen vorgenommen werden (unter der Voraussetzung, daß die Zugriffsrechte entsprechend restriktiv definiert wurden).
Datenbankobjekte, die von mindestens zwei der drei Anwendungen benötigt werden, sollten unter einer zentralen Datenbank-Kennung eingerichtet und verwaltet werden.
Das entsprechende Paßwort der drei anwendungsspezifischen Kennungen ist nur demjenigen Administrator bekannt, der für die Verwaltung und Pflege der Datenbankobjekte der jeweiligen Anwendung verantwortlich ist. Das Paßwort für die Datenbank-Kennung, über die die zentralen Datenbankobjekte verwaltet wird, ist dagegen keinem dieser Administratoren bekannt, sondern unterliegt der Obhut eines weiteren Administrators. Auf diese Weise kann verhindert werden, daß die Administratoren der jeweiligen Anwendungen Modifikationen an zentralen Datenbankobjekten vornehmen können, die unter Umständen die Funktionalität der anderen Anwendungen beeinträchtigen könnte.

M 4.69 Regelmäßiger Sicherheitscheck der Datenbank

Der Datenbankadministrator sollte regelmäßig, jedoch mindestens einmal monatlich einen Sicherheitscheck des Datenbanksystems durchführen. Folgende Punkte sollten dabei u.a. geprüft

werden, wobei die mit (*) markierten Punkte meist durch entsprechende Skripte automatisiert werden können:

- Sind die erforderlichen und geplanten Sicherungs- und Sicherheitsmechanismen aktiv und greifen sie auch?
- Gibt es Datenbank-Benutzer ohne Paßwort? (*)
- Gibt es Benutzer, die längere Zeit das Datenbanksystem nicht mehr benutzt haben?
- Wer darf bzw. kann außer dem Datenbank-Administrator auf die Dateien der Datenbank-Software bzw. auf die Dateien der Datenbank auf Betriebssystemebene zugreifen? (*)
- Wer hat außer dem Datenbank-Administrator Zugriff auf die System-Tabellen?
- Wer darf mit einem interaktiven SQL-Editor auf die Datenbank zugreifen?
- Welche Benutzerkennungen haben modifizierende Zugriffsrechte auf die Datenbankobjekte der Anwendungen? (*)
- Welche Benutzerkennungen haben lesende und / oder modifizierende Zugriffsrechte auf die Daten der Anwendungen? (*)
- Welche Benutzer besitzen die gleichen Rechte wie der Datenbank-Administrator? (*)
- Verfügt das Datenbanksystem über ausreichend freie Ressourcen? (*)

Anmerkung:
System-Tabellen sind die Tabellen, mittels derer die Datenbank selbst verwaltet wird. In diesen Tabellen werden beispielsweise die einzelnen Datenbankobjekte, die Datenbankkennungen, die Zugriffsberechtigungen sowie die Zuordnungen von Dateien zu Speichermedien verwaltet. Die System-Tabellen werden vom DBMS selbst bei der Erstellung einer Datenbank erzeugt. Eine Modifikation dieser Tabelleninhalte ist prinzipiell immer mit Datenbankkennungen möglich, die Administratorrechte besitzen. Werden die Daten der System-Tabellen durch UPDATE-, INSERT- oder DELETE-Kommandos modifiziert, besteht ein hohes Risiko, daß die Datenbank zerstört wird. Aus diesem Grund sollte man auf die Vergabe von modifizierenden Rechten auf die System-Tabellen verzichten. Selbst ein lesender Zugriff sollte beschränkt werden, da über die System-Tabellen alle Informationen der Datenbank ermittelt werden können.

M 4.70 Durchführung einer Datenbanküberwachung

Um die Verfügbarkeit, die Datenbankintegrität und die Vertraulichkeit der Daten gewährleisten zu können, ist eine regelmäßige Datenbanküberwachung erforderlich. Die wesentlichen Punkte, die es dabei zu beachten gilt, werden im folgenden kurz erläutert.
Die Datenbank ist in regelmäßigen Zeitabständen hinsichtlich einer möglichen Fragmentierung zu überprüfen, um gegebenenfalls Maßnahmen wie z.B. eine Reorganisation der Datenbank planen und durchführen zu können.

Datenbanksysteme verwalten den ihnen zur Verfügung gestellten Speicherplatz in der Regel in der Form von Blöcken fester Größe. Wenn Sätze in eine leere Tabelle eingefügt werden, werden neue Blöcke für diese Tabelle reserviert und mit den Datensätzen gefüllt. Bei diesem Neuanlegen ist es möglich, die Blöcke (mit Ausnahme des letzten) fast vollständig zu nutzen.
Werden im späteren Betrieb Datensätze gelöscht, wird der von ihnen belegte Speicherplatz in den Blöcken freigegeben. Dieser Platz kann dann grundsätzlich für andere Datensätze genutzt werden. Da die Datensätze aber alle unterschiedliche Längen haben, kann in der Regel ein freier Speicherbereich nicht zu 100 % ausgenutzt werden. Dadurch entsteht durch die Datenänderungen im Laufe der Zeit eine immer größere Anzahl kleiner Lücken in den Blöcken der Datenbank, die meist nicht mehr genutzt werden können. Diese Lücken entstehen nicht nur durch DELETE- und INSERT-Operationen, sondern auch durch UPDATEs, da ein Datensatz nicht mehr an derselben Stelle gespeichert werden kann, wenn sich seine Länge geändert hat.
Das Vorhandensein solcher Lücken erhöht nicht nur den Speicherbedarf, sondern verlangsamt auch Datenbankoperationen, da Datensätze oder freier Speicherplatz erst in einem größeren Plattenbereich gesucht werden müssen.
Der Grad der Fragmentierung in den Blöcken einer Tabelle kann durch den Vergleich zwischen der Menge der Daten in den Datensätzen in der Tabelle und dem von den Blöcken der Tabelle belegtem Speicherplatz festgestellt werden. Auswertungen über den Fragmentierungsgrad werden für einige DBMSe auch von der mitgelieferten Administrationssoftware oder von Zusatzprodukten unterstützt.

Sollte die Fragmentierung der Datenbank aufgrund einer der oben genannten Gründe zu groß werden, muß eine Reorganisation durchgeführt werden. Dies kann z.B. manuell erfolgen, in dem zuerst alle Daten der Datenbank exportiert, dann alle Tabellen neu berechnet und angelegt und schließlich alle Daten in die neue Datenbank wieder importiert werden. Für manche DBMSe sind auch Hilfsprogramme zum Defragmentieren von Tabellen erhältlich. Ebenso sind die Datenbankdateien regelmäßig hinsichtlich ihres Füllgrades zu überprüfen, um rechtzeitig Maßnahmen wie z.B. eine Erweiterung der Speicherkapazitäten planen und durchführen zu können. Manche DBMSe erlauben es dem Administrator durch Definition bestimmter Parameter bereits beim Anlegen der Tabellen einer zu starken und zu raschen Fragmentierung vorzubeugen. So kann für eine Tabelle von vornherein eine bestimmte Menge zusammenhängender Blöcke reserviert werden, in denen zusätzlich bereits freier Platz für Änderungen im Betrieb bereitgehalten wird.

Beispiel:
Bei einer Oracle Datenbank wird jeder Tabelle eine feste Anzahl von Extents zugeordnet. Der Begriff Extent wird im Oracle Sprachgebrauch als logische Größeneinheit verwendet. Die Daten einer Tabelle werden in mindestens einem Extent abgelegt. Sobald die Kapazität eines Extents ausgeschöpft ist, legt das DBMS automatisch ein weiteres Extent an. Beim Erstellen einer Tabelle können dabei folgende Werte definiert werden:

- Größe des ersten Extent in Bytes
- Größe des zweiten Extents in Bytes

- Wachstum aller weiteren Extents in Prozent, wobei diese Zahl in Relation zur Größe des zweiten Extents steht.
- Maximale Anzahl an Extents, die für die Tabelle angelegt werden dürfen.
- Mit dem Parameter PCTFREE wird festgelegt, wieviel Prozent der neuen Blöcke für spätere Änderungen freigehalten werden.

Es muß ebenfalls regelmäßig überprüft werden, ob das Datenvolumen tatsächlich in dem Maße anwächst wie es ursprünglich angenommen wurde. Wächst es langsamer, werden unnötige Speicherressourcen gebunden, die anderweitig verwendet werden könnten. Wächst es schneller, kann es unter Umständen zu Speicherengpässen kommen.
Darüber hinaus ist die Auslastung der Datenbank ist regelmäßig zu prüfen, insbesondere im Hinblick auf die eingestellten Obergrenzen (siehe M 4.73 - Festlegung von Obergrenzen).

Welche Informationen für eine konkrete Datenbanküberwachung relevant sind, hängt von deren spezieller Funktionsweise, also von der eingesetzten Datenbank-Standardsoftware ab. Dementsprechend sind auch individuelle Maßnahmen einzuleiten, die die Datenbankkonfiguration dahingehend modifizieren, daß sie den Anforderungen hinsichtlich Zugriffsgeschwindigkeiten, durchzuführender Transaktionen usw. gerecht wird.
Eine Automatisierung der Datenbanküberwachung kann mittels Skripten durchgeführt werden. Eine Voraussetzung ist allerdings, daß die Informationen in auswertbarer Form von der eingesetzten Datenbanksoftware zur Verfügung gestellt werden.

M 4.71 Restriktive Handhabung von Datenbank-Links
Über sogenannte Datenbank-Links (DB-Links) besteht die Möglichkeit, von einer Datenbank aus auf die Daten einer anderen Datenbank zuzugreifen. Um einen angemessenen Schutz der Daten zu gewährleisten, sollte diese Technik jedoch nur dann verwendet werden, wenn dies unbedingt notwendig ist. Um die Berechtigungen eines Benutzers bei der Verwendung von DB-Links kontrollieren zu können, ist ein entsprechendes Konzept hinsichtlich der Definition von Benutzer-Kennungen erforderlich. So erhält ein Benutzer prinzipiell die Möglichkeit, auf eine fremde Datenbank zuzugreifen, wenn dort die gleiche Benutzer-Kennung existiert, mit der sich der Benutzer an der lokalen Datenbank anmeldet. Einen weitergehenderen Schutz erhält man durch die Möglichkeit, einen DB-Link mit expliziter Angabe einer Benutzer-Kennung und eines Paßwortes zu erstellen.

Prinzipiell ist zunächst einmal jeder Benutzer der Datenbank befugt, solche DB-Links zu erstellen (unter der Voraussetzung, daß er in der Lage ist, das entsprechende CREATE-Kommando auszuführen). Im allgemeinen sollte jedoch nur der Administrator das Recht besitzen, DB-Links zu erstellen. Insbesondere gilt dies für DB-Links, die von allen Datenbankbenutzern genutzt werden dürfen (sogenannte PUBLIC DB-Links). Die Berechtigung zur Erstellung von DB-Links sollte dagegen für normale Benutzerkennungen explizit nicht vergeben werden.
Weiterhin sollte die Anzahl von parallel nutzbaren DB-Links eines Benutzers begrenzt werden, um die Belastung der Datenbankserver unter Kontrolle halten zu können. Ansonsten kann ein

Angreifer dies ausnutzen, um die Verfügbarkeit der Datenbankserver zu reduzieren oder diese sogar vollständig lahmzulegen.

Eine Dokumentation der vom Administrator angelegten DB-Links ist unabdingbar. Die Dokumentation sollte neben der Verbindungsart (über eine spezielle Benutzerkennung oder unter der Voraussetzung, daß die jeweilige aktuelle Datenbankkennung ebenfalls für die verbundene Datenbank angelegt wurde) auch beinhalten, welcher Benutzerkreis in der Lage ist, den entsprechenden DB-Link zu nutzen. Wie bereits erwähnt, steht ein DB-Link, der als PUBLIC definiert wurde, allen Datenbankkennungen zur Verfügung.

M 4.72 Datenbank-Verschlüsselung
In Abhängigkeit von der Art der in einer Datenbank gespeicherten Informationen und den sich daraus ergebenden Anforderungen an deren Vertraulichkeit und Integrität kann es notwendig werden, diese Daten zu verschlüsseln. Dabei kann zwischen einer Online- und einer Offline-Verschlüsselung unterschieden werden:

- Bei einer Online-Verschlüsselung werden die Daten während des laufenden Betriebs ver- und entschlüsselt, ohne daß die betroffenen Benutzer davon etwas merken. Dafür können Tools eingesetzt werden, mit denen entweder auf Betriebssystemebene die gesamte Festplatte verschlüsselt wird, oder solche, mit denen nur die Anwendungsdaten der Datenbank verschlüsselt werden.

- Bei einer Offline-Verschlüsselung werden die Daten erst nach ihrer Bearbeitung verschlüsselt und vor ihrer Weiterverarbeitung wieder entschlüsselt. Dies wird im allgemeinen mit Tools durchgeführt, die nicht in das Datenbanksystem integriert sind, und kann insbesondere für Datensicherungen oder Datenübertragungen sinnvoll sein. Dabei ist zu beachten, daß genügend Platz auf der Festplatte vorhanden ist, da die Ver- bzw. Entschlüsselung nur dann erfolgreich ausgeführt werden kann, wenn auf der Festplatte genügend Platz für das Original und die verschlüsselte Version der Datenbank verfügbar ist.

Darüber hinaus besteht die Möglichkeit, Daten weiterhin im Klartext in der Datenbank abzuspeichern, beim Zugriff über ein Netz jedoch eine verschlüsselte Datenübertragung zu realisieren. Dies kann z.B. durch die Secure Network Services der Oracle SQL*Net Produktfamilie durchgeführt werden.

Welche Daten mit welchem Verfahren zu verschlüsseln sind, ist am besten bereits bei der Auswahl der Datenbank-Standardsoftware festzustellen (siehe M 2.124 - Geeignete Auswahl einer Datenbank-Software). Dabei sollten die Anforderungen hinsichtlich der Verschlüsselung von Datenbeständen mit den entsprechenden Leistungsmerkmalen der Datenbank-Software verglichen werden. Als Mindestanforderung sollte sie in jedem Fall sicherstellen, daß die Paßwörter der Benutzer-Kennungen der Datenbank verschlüsselt abgelegt sind.
Falls die Anforderungen durch keine der am Markt verfügbaren Datenbank-Standardsoftware abgedeckt werden können, sollte man den Einsatz von Zusatzprodukten prüfen, um die entsprechende Sicherheitslücke zu schließen. Falls auch keine Zusatzprodukte erhältlich sind, muß

ein Konzept für die Umsetzung einer Verschlüsselungsstrategie erstellt werden, das im Unternehmen bzw. in der Behörde umgesetzt wird.

M 4.73 Festlegung von Obergrenzen
Um den Zugriff auf ein Datenbanksystem besser kontrollieren zu können und um die Performance zu verbessern, ist die Festlegung von Obergrenzen für bestimmte Parameter sinnvoll. Dabei sind vor allem die folgenden Punkte zu beachten:

Festlegung von Obergrenzen für selektierbare Datensätze
Insbesondere wenn große Datenmengen in einer Datenbank abgelegt wurden, sollte eine maximale Anzahl von Datensätzen definiert werden, die im Rahmen eines Datenzugriffs selektiert werden können.
Existieren solche Obergrenzen nicht, so kann ein Benutzer gezielt oder unbeabsichtigt beliebig umfangreiche Selects durchführen. Dies behindert nicht nur den einzelnen Benutzer in seiner Arbeit, sondern führt auch bei allen anderen Benutzern der Datenbank zu langen Wartezeiten. Werden die Datensätze dabei selektiert, um diese zu modifizieren, so sind sie solange für alle anderen Benutzer gesperrt, bis diese Transaktion beendet ist. Die Obergrenzen müssen im Rahmen der Anwendungen definiert werden, die auf die Datenbank zugreifen. Dabei müssen geeignete Kontrollen bzw. Sperren realisiert werden, die die Einhaltung der Obergrenzen überwachen. Stellt eine Anwendung Suchfunktionalitäten bereit, so sollte die uneingeschränkte Suche generell abgelehnt und die Eingabe von Suchkriterien gefordert werden.

Festlegung von Ressourcenbeschränkungen
Eine weitere Möglichkeit, die von einigen Herstellern angeboten wird, ist die Unterstützung von Ressourcenbeschränkungen in Bezug auf die Benutzung einer Datenbank. So können beispielsweise die Anzahl von Anmeldungen pro Benutzerkennung, der maximale Anspruch auf CPU-Zeit pro Anmeldung, die Gesamtdauer einer Datenbankverbindung, die maximal zulässige inaktive Zeit während einer Anmeldung und vieles mehr definiert werden.

Beispiele:
Mit folgendem Kommando wird in einer Oracle-Datenbank für die Datenbankkennung „Meier“ der temporäre Tablespace „Temp“ auf 100 MB begrenzt:
ALTER USER Meier TEMPORARY TABLESPACE Temp QUOTA 100M ON Temp;
Mit dem nachfolgenden Befehl wird ein Profile „Tester“ erstellt, das die Anzahl der Sessions, die maximale CPU-Zeit pro Session, die maximale Zeit einer Datenbankverbindung und die maximale Leerlaufzeit (IDLE) begrenzt. Dieses Profile kann dann einzelnen Benutzern zugeordnet werden.

```
CREATE PROFILE Tester LIMIT
SESSIONS PER USER 2,
CPU_PER_SESSION 6000,
IDLE_TIME 30,
CONNECT_TIME 500;
```

Eine Ingres-Datenbank erlaubt beispielsweise für Benutzer und Gruppen das Setzen von Grenzen für die maximale Ein- und Ausgabe je Abfrage oder für die Anzahl von Sätzen pro Abfrage. Weiterhin kann auch die Anzahl der Benutzer beschränkt werden, die gleichzeitig auf die Datenbank zugreifen dürfen. Durch deren Begrenzung mittels Parametereinstellungen im DBMS kann gewährleistet werden, daß die maximal zur Verfügung stehende Zahl an Lizenzen für die Datenbank-Software nicht überschritten wird. Außerdem verursachen viele parallel zugreifende Benutzer eine hohe Arbeitslast, dem der Datenbankserver eventuell nicht gewachsen ist, wodurch sich die durchschnittliche Dauer einer Transaktion verlängert. Ist in diesem Fall aus bestimmten Gründen eine Erweiterung der Ressourcen des Datenbanksystems nicht möglich oder nicht gewünscht, schafft hier eine Begrenzung der maximal möglichen parallelen Benutzerzugriffe ebenfalls Abhilfe.
Die diesbezüglichen Anforderungen sollten bereits während der Auswahl einer Datenbank-Standardsoftware geklärt werden, um gegebenenfalls ein Konzept zur Umsetzung der Ressourcenbeschränkungen zu erstellen (siehe M 2.124 Geeignete Auswahl einer Datenbank-Software).

M 4.74 Vernetzte Windows 95 Rechner
Werden Windows 95 Rechner in einem Netz betrieben (Novell Netware oder Windows NT), so sollte die Möglichkeit genutzt werden, die jeweiligen Systemrichtlinien auf Netzservern zu speichern und diese dort zentral zu verwalten.
Mit Hilfe der SYSTEMSTEUERUNG unter NETZWERK wird hierbei die primäre Netzwerkanmeldung, d.h. der Pfad für die Systemrichtlinien festgelegt. Standardmäßig werden die Benutzerprofile auf einem Novell Netware Server unter SYS:PUBLIC abgelegt. Erfolgt die primäre Netzanmeldung an einem Windows NT Rechner, so werden die Benutzerprofile standardmäßig unter NETLOGON
(%SystemRoot%\SYSTEM32\REPL\IMPORT\SCRIPTS\) abgelegt.
Die Aktivierung der Benutzerprofile wird mit Hilfe der SYSTEMSTEUERUNG-KENNWÖRTER-BENUTZERPROFILE sichergestellt.

Weiterhin sollte zudem der Betrieb von Windows 95 ohne Netzwerkanmeldung gesperrt werden um eine Umgehung der Systemrichtlinien auf lokaler Basis zu verhindern. Hierzu sollte mit Hilfe von POLEDIT.EXE unter lokaler Computer-Netzwerk-Anmeldung die Option NETZWERK-BESTÄTIGUNG FÜR WINDOWS ZUGRIFF FORDERN aktiviert werden.

Die Verwaltung der Systemrichtlinien sollte aus Gründen der Einheitlichkeit überwiegend über die Einrichtung von Benutzergruppen erfolgen. Gruppenrichtlinien werden unter Windows 95 über SYSTEMSTEUERUNG-SOFTWARE-WINDOWS-SETUP installiert und befinden sich standardmäßig in dem Verzeichnis ADMIN\APPTOOLS\POLEDIT\GROUPPOL.INF.
Die Namen der jeweiligen Benutzergruppen müssen hierbei den eingerichteten Benutzergruppen unter Novell Netware bzw. Windows NT entsprechen. Um den ordnungsgemäßen IT-Betrieb sicherzustellen, sollte zusätzlich beachtet werden, daß das Programm POLEDIT.EXE nicht auf dem lokalen Windows 95 Rechner installiert werden darf, da mit diesem Programm die gültigen Systemrichtlinien von jederman dauerhaft verändert werden können. Ebenso sollte in der

Datei MS DOS.SYS der Wert BootKeys verändert werden (BootKeys=1) um den Start von Windows 95 im „abgesicherten Modus“ zu unterbinden. Dies verhindert, daß die Systemrichtlinien nicht zur Anwendung kommen.
Das BIOS des Computers sollte zudem einen Systemboot über Diskette verhindern, sowie das Diskettenlaufwerk mit einem Schloß versperrt werden, um Einsatz von nichtautorisierter Software zu erschweren.

M 4.75 Schutz der Registrierung unter Windows NT
In der Registrierung eines Windows NT Systems werden alle wichtigen Konfigurations- und Initialisierungsinformationen gespeichert. Dort wird u. a. auch die SAM-Datenbank verwaltet, die die Benutzer- und Computerkonten enthält.
Die Registrierung eines Windows NT Systems besteht aus mehreren Dateien, die sich in dem Verzeichnis %Systemroot%\SYSTEM32\Config befinden. Aus diesem Grund sollten die Zugriffsrechte auf dieses Verzeichnis und die darin enthaltenen Dateien so gesetzt werden, wie dies in M 4.53 - Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT vorgeschlagen wurde.
Zur Erhöhung des Schutzes sollten unmittelbar nach der Installation des Betriebssystems die folgenden sicherheitsrelevanten Teile der Registrierung durch expliziten Eintrag von Zugriffsrechten mit Hilfe des Registrierungs-Editors (des Programms REGEDT32.EXE im Windows-Systemverzeichnis %SystemRoot%\SYSTEM32) besonders geschützt werden, so daß die Gruppe „Jeder“ für diese Teile nur über die Zugriffsrechte „Wert einsehen“, „Teilschlüssel auflisten“, „Benachrichtigen“ und „Zugriff lesen“ verfügt:

- im Bereich HKEY_LOCAL_MACHINE:
  \Software\Microsoft\RPC (mit allen Unterschlüsseln)
  \Software\Microsoft\Windows NT\CurrentVersion
  unter dem Schlüssel \Software\Microsoft\Windows NT\CurrentVersion\:
  + Profile List
  + AeDebug
  + Compatibility
  + Drivers
  + Embedding
  + Fonts
  + FontSubstitutes
  + GRE_Initialize
  + MCI
  + MCI Extensions
  + Port (mit allen Unterschlüsseln)
  + WOW (mit allen Unterschlüsseln)
  + Windows3.1MigrationStatus (mit allen Unterschlüsseln)

- im Bereich HKEY_CLASSES_ROOT:
  \HKEY_CLASSES_ROOT (mit allen Unterschlüsseln)

Dabei ist sorgfältig vorzugehen, da fehlerhafte Einstellungen in der Registrierung dazu führen können, daß das System nicht mehr lauffähig ist und nach dem nächsten Starten eventuell nicht mehr hochläuft. Die hier genannten Einstellungen sollten daher zunächst an einem eigenen Testsystem angewendet und auf ihre Lauffähigkeit in der aktuellen Umgebung kritisch geprüft werden, ehe sie allgemein eingesetzt werden.

Netzzugriff auf die Registrierung
Sofern diese Funktionalität nicht unbedingt gebraucht wird, sollte auch der Zugriff über das Netz auf die Registrierung gesperrt werden. Dies ist ab der Version 4.0 möglich, indem der Eintrag „winreg“ im Schlüssel
\System\CurrentControlSet\Control\SecurePipeServers im Bereich HKEY_LOCAL_MACHINE auf den Wert REG_DWORD = 1 gesetzt wird.
In der Version 3.x besteht die Möglichkeit der expliziten Sperrung von Netzzugriffen auf die Registrierung nicht. Hier kann man sich damit behelfen, daß die Zugriffsberechtigung für „Jeder“ auf die Wurzel des Bereiches HKEY_LOCAL_MACHINE (nicht jedoch auf die darunterliegenden Schlüssel!) entfernt wird, so daß nur noch Administratoren auf diesen Bereich Zugriff haben. Diese Änderung ist unbedingt auf einem Testsystem zu überprüfen, da sie zur Folge haben kann, daß einige Anwendungen nicht mehr lauffähig sind. Es ist zu beachten, daß diese Änderung nur bis zum nächsten Systemstart bestehen bleibt.

M 4.76 Sichere Systemversion von Windows NT
Vor der Beschaffung des Betriebssystem Windows NT muß entschieden werden, ob die englische oder die deutsche Version beschafft werden soll. Es ist nicht möglich, eine eindeutige Empfehlung abzugeben. Daher soll hier nur aufgezeigt werden, welche spezifischen Vor- und Nachteile die Entscheidung für die eine oder andere Version mit sich bringt.
Die englische Version von Windows NT ist stärker verbreitet als die deutsche Version. Dies führt dazu, daß Tools, Service Packs und Hot Fixes für die englische Version schneller verfügbar sind. Es gibt auch Tools, die nur mit der englischen Version von Windows NT einsetzbar sind. Es ist auch möglich, die englische Version von Windows NT so zu konfigurieren, daß Fehlermeldungen in deutscher Sprache ausgegeben werden. Andererseits ergibt sich die gleiche Situation hinsichtlich der Verfügbarkeit bei den Schadprogrammen. Auch diese werden für die englische Version schneller entwickelt und sind teilweise für die deutsche Version überhaupt nicht verfügbar.
Windows NT kann nur dann sicher betrieben werden, wenn mindestens die Version 3.51 oder 4.0 installiert sind. Weiterhin ist die Installation des jeweils aktuellen Service Packs erforderlich. Zum Zeitpunkt der Drucklegung ist dies für die Version 3.51 das Service Pack 5 und für die Version 4.0 das Service Pack 3. Die installierte Systemversion und der ggf. installierte Service Pack werden beim Systemstart angezeigt. Außerdem werden durch Microsoft sogenannte Hot Fixes zur Verfügung gestellt, die Updates zu dem jeweils aktuellen Service Pack darstellen. Die jeweils aktuellen Hot Fixes sollten ebenfalls installiert werden, soweit sie Funktionen des installierten Systems betreffen. Der Systemverwalter muß sich daher regelmäßig darüber informieren, welches Service Pack und welche Hot Fixes für sein System aktuell sind.
Die einmalige Installation eines Service Packs oder eines Hot Fixes reicht nicht für die Sicher-

stellung der Systemintegrität. Jede Änderung der Systemkonfiguration, die einen Zugriff auf die Installations-CD-ROM erforderlich macht oder bei der neue Gerätetreiber inst- alliert werden müssen, bedingt eine erneute Installation des aktuellen Service Packs und der notwendigen Hot Fixes. Wird dies unterlassen, besteht die Gefahr, daß Systemdateien, die aus dem jeweiligen Service-Pack oder dem Hot Fix stammen, durch eine ältere Version ersetzt werden, was im schlimmsten Fall dazu führen kann, daß ein Windows NT System nicht mehr in Betrieb genommen werden kann.
Nach der Installation eines Service Packs oder eines Hot Fixes sollten die Notfalldisketten aktualisiert werden (siehe M 6.42 - Erstellung von Rettungsdisketten für Windows NT). Außerdem sollte die Sicherheitskonfiguration des betroffenen Rechners überprüft werden.

M 4.77 Schutz der Administratorkonten unter Windows NT
Bei jeder Installation eines jeden Windows NT Systems wird ein Administratorkonto angelegt. Auf Windows NT Rechnern, die als Workstation oder als Server ohne Domänencontrollerfunktion installiert werden, ist dieses vordefinierte Administratorkonto Mitglied der Gruppe „Administratoren“ . Auf Servern, die unter dem Betriebssystem Windows NT als Primäre Domänenkontroller installiert werden, wird das vordefinierte Administratorkonto bei der Installation Mitglied der Gruppen „Administratoren“ , „Domänen-Admins“ und „Domänen-Benutzer“ . Es ist weiterhin möglich, beliebige auf einem Windows NT Rechner definierte Benutzerkonten den Gruppen „Administratoren“ oder „Domänen-Admins“ hinzuzufügen. Das vordefinierte Administratorkonto und die nach der Installation den Gruppen „Administratoren“ bzw. „Domänen-Admins“ hinzugefügten Benutzerkonten erhalten die Rechte und Berechtigungen, die der oder den Gruppen erteilt wurden, in denen sie Mitglied sind. Diese Konten werden von den Personen verwendet, welche die Gesamtkonfiguration der Arbeitsstation oder des Servers verwalteten. Administratoren besitzen mehr Kontrollmöglichkeiten über den Windows NT Computer als jeder andere Benutzer.

Das vordefinierte Administratorkonto unterscheidet sich aber in wesentlichen Punkten von allen anderen Konten unter Windows NT: Es kann nicht gelöscht werden und es ist von der automatischen Sperre bei wiederholten Anmeldeversuchen mit falschem Paßwort ausgenommen. Außerdem kann es auf Windows NT Workstations und auf Windows NT Servern ohne Domänencontrollerfunktionalität nicht aus der Gruppe „Administratoren“ entfernt werden. Auf Windows NT Domänencontroller ist es nicht möglich, das vordefinierte Administratorkonto sowohl aus der Gruppe „Administratoren“ als auch aus der Gruppe „Domänen-Admin“ zu entfernen. Die Entfernung aus einer dieser beiden Gruppen ist aber möglich. Damit wird verhindert, daß ein Administrator zeitweise oder vollständig aus dem System ausgesperrt wird. Andererseits führt dieser Mechanismus zu einem erhöhten Einbruchsrisiko. An dieser Stelle muß ausdrücklich darauf hingewiesen werden, daß alle nachträglich angelegten Benutzerkonten, die durch Aufnahme in die Gruppen „Administratoren“ bzw. „Domänen-Admins“ Administratorrechte erlangt haben, selbstverständlich durch andere Administratoren gesperrt und gelöscht bzw. aus den o.g. Gruppen wieder entfernt werden können. Auch ist die automatische Sperre bei wiederholten Anmeldeversuchen mit falschen Paßwort wirksam, sofern diese in den Kontenrichtlinien definiert wurde.

Auf allen Windows NT Computern sollte das vordefinierte Administratorkonto auf einen nicht leicht erratbaren Namen umbenannt werden. Es sollte bereits bei der Installation mit einem sicheren Paßwort (siehe M 2.11 - Regelung des Paßwortgebrauchs) versehen werden. Das Paßwort sollte möglichst die maximale Länge von 14 Zeichen ausnutzen. Es ist sicher zu hinterlegen. Es ist sinnvoll für die tägliche Administration nicht das vordefinierte Administratorkonto zu benutzen, sondern Benutzerkonten, die der Gruppe „Administrator“ oder „Domänen-Admins“ hinzugefügt wurden. Die Paßwortlänge dieser Konten sollte mindestens 8 Zeichen betragen. Das vordefinierte Administratorkonto sollte lediglich für den Fall benutzt werden, daß ein Zugriff über die nachträglich angelegten Konten mit Administratorrechten nicht möglich ist, z.B. weil diese Konten wegen wiederholten Anmeldeversuchen mit falschem Paßwort gesperrt sind. Auch ist es sinnvoll, danach ein neues Konto mit dem Namen „Administrator“ anzulegen, dieses mit einem Paßwort zu versehen, es zu deaktivieren und dieses Konto nur in der Gruppe „Gäste“ aufzunehmen. Diesem Konto dürfen keine besonderen Systemrechte zugewiesen werden, da es lediglich dazu dient, einen potentiellen Angreifer auf eine falsche Spur zu führen.
Weiterhin sollte das Sicherheitsprotokoll regelmäßig auf Anmeldeversuche mit Konten, die über Administratorrechte verfügen, überprüft werden (siehe M 4.54 - Protokollierung unter Windows NT).
Es existiert eine spezielle Schadsoftware, mit der ein lokal angemeldeter Benutzer der Gruppe „Administratoren“ beliebige Benutzerkonten hinzufügen kann. Um dies zu verhindern, sollte auf allen Computern unter dem Betriebssystem Windows NT der Hot Fix „getadmin-fix“ installiert werden, der durch Microsoft kostenlos zur Verfügung gestellt wird.
Um ein Extrahieren des Administratorpaßwortes zu verhindern, sollten außerdem die Rechte auf die Verzeichnisse
%Systemroot%\SYSTEM32\Config und %Systemroot%\SYSTEM32\Repair so gesetzt werden, wie dies in M 4.53 - Restriktive Vergabe von Zugriffsrechten vorgeschlagen wurde. Auch müssen Notstartdisketten und evtl. vorhandene Bandsicherungen unter Verschluß gehalten werden.
Abhängig vom Schutzbedarf der Daten, die mit Windows NT Workstations verarbeitet werden, ist zu entscheiden, ob für alle lokalen Administratorenkonten das gleiche Paßwort benutzt wird. Eine generelle Empfehlung kann nicht gegeben werden, es sollte jedoch bei einer Entscheidung zugunsten des gleichen Paßwortes für alle Workstations bedacht werden, daß ein Angreifer im Falle der Kompromittierung dieses Paßwortes auf allen betroffenen Workstations Administratorrechte hat.

Bei Windows NT Servern sollten noch folgende weitere Maßnahmen getroffen werden. Es sollten die Administratorenkonten auf den verschiedenen Servern nicht alle mit dem gleichen Paßwort versehen werden. Weiterhin sollte möglichst nicht über das Netz fernadministriert werden. Dies wird erreicht, indem der Gruppe „Administratoren“ das Recht „Zugriff auf diesen Computer vom Netz“ entzogen wird. Dort, wo auf eine Fernadministration z.B. aufgrund räumlicher Gegebenheiten nicht verzichtet werden kann, sollten die Angriffsmöglichkeiten, die sich dadurch eröffnen, so gering wie möglich gehalten werden. Dazu gehört, daß eine Anmeldung über das Netz für Benutzerkonten mit Administratorrechten nur über in den Kontenrichtlinen festgelegte Rechner, die unter dem Betriebssystem Windows NT betrieben werden, erlaubt wird. Diese

Rechner sollten möglichst in gesicherten Bereichen aufgestellt werden. Auf diesen Rechnern sollte zwingend die LAN-Manager-Kompatibilität abgeschaltet werden, um so zu vermeiden, daß Paßwörter von Benutzerkonten mit Administratorrechten unverschlüsselt über das Netz gesandt werden. Dazu ist es erforderlich, den Hot Fix „lm-fix", der ein installiertes Service Pack 3 voraussetzt, zu installieren und in der Registrierung der folgenden Schlüssel zu ergänzen: HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\Lsa um den Eintrag „LM-CompatibilityLevel" vom Typ „REG_DWORD" und dem Wert „2".

Ein so modifizierter Windows NT Rechner ist danach nicht mehr in der Lage auf Ressourcen zuzugreifen, die sich auf Rechnern befinden, die das Windows NT Authentisierungsschema nicht beherrschen. Dies sind u.a. alle Rechner, die unter dem Betriebssystem Windows 95 betrieben werden. Auf Domänencontrollern reicht es nicht aus, der Gruppe „Administratoren" das Recht „Zugriff auf diesen Computer vom Netz" zu entziehen, weil auf Domänencontrollern das vordefinierte Administratorkonto automatisch Mitglied in den Gruppen „Domänen-Admins" und „Domänen-Benutzer" geworden ist. Das vordefinierte Administratorkonto sollte daher aus der Gruppe der „Domänen-Admins" entfernt werden. Dies ist möglich, solange diese Konto Mitglied der Gruppe „Administratoren" bleibt. Außerdem sollte das vordefinierte Administratorkonto aus der Gruppe „Domänen-Benutzer" entfernt werden. Dies ist allerdings nicht ohne weiteres möglich, da es die primäre Gruppe dieses Kontos ist. Es muß daher eine beliebige globale Gruppe angelegt werden, die nicht über das Recht „Zugriff auf diesen Computer vom Netz" verfügt. Das vordefinierte Administratorkonto ist dieser Gruppe hinzuzufügen und es ist einzustellen, daß dies nunmehr die primäre Gruppe des Kontos sein soll. Erst danach kann das vordefinierte Administratorkonto aus der Gruppe „Domänen-Benutzer" entfernt werden.

M 4.78 Sorgfältige Durchführung von Konfigurationsänderungen

Die Durchführung von Änderungen an einem IT-System im Echtbetrieb ist immer als kritisch einzustufen und entsprechend sorgfältig muß hierbei vorgegangen werden.
Bevor mit Änderungen am System begonnen wird, muß als erstes die alte Konfiguration gesichert werden, so daß sie schnell verfügbar ist, wenn Probleme mit der neuen Konfiguration auftreten.
Bei vernetzten IT-Systemen müssen die Benutzer rechtzeitig über die Durchführung von Wartungsarbeiten informiert werden, damit sie zum einen ihre Planung auf eine zeitweise Systemabschaltung einrichten können, und damit sie zum anderen nach Änderungen auftretende Probleme richtig zuordnen können.

Die Konfigurationsänderungen sollten immer nur schrittweise durchgeführt werden. Zwischendurch sollte immer wieder überprüft werden, ob die Änderungen korrekt durchgeführt wurden und das IT-System sowie die betroffenen Applikationen noch lauffähig sind.
Bei Änderungen an Systemdateien ist anschließend ein Neustart durchzuführen, um zu überprüfen, ob sich das IT-System korrekt starten läßt. Für Problemfälle sind alle für einen Notstart benötigten Datenträger vorrätig zu halten, z.B. Boot-Disketten, Start-CD-ROM.
Komplexere Konfigurationsänderungen sollten möglichst nicht in den Originaldateien vorgenommen werden, sondern in Kopien. Alle durchgeführten Änderungen sollten von einem Kol-

legen überprüft werden, bevor sie in den Echtbetrieb übernommen werden.
Bei IT-Systemen mit hohen Verfügbarkeitsanforderungen ist auf Ersatzsysteme zurückzugreifen bzw. zumindest ein eingeschränkter IT-Betrieb zu gewährleisten. Das Vorgehen kann sich dabei idealerweise nach dem Notfall-Handbuch richten.
Die durchgeführten Konfigurationsänderungen sollten Schritt für Schritt notiert werden, so daß bei auftretenden Problemen das IT-System durch sukzessive Rücknahme der Änderungen wieder in einen lauffähigen Zustand gebracht werden kann (siehe auch M 2.34 - Dokumentation der Veränderungen an einem bestehenden System).

M 4.79 Sichere Zugriffsmechanismen bei lokaler Administration
Bei einigen aktiven Komponenten kann über einen lokalen Zugriff die Administration der Komponenten erfolgen. Solch ein lokaler Zugriff ist zumeist über einen seriellen Anschluß (üblicherweise eine V.24 bzw. EIA-232-E Schnittstelle) realisiert. Für einen sicheren lokalen Zugriff sind die folgenden Maßnahmen zu beachten:

- Die aktiven Netzkomponenten und ihre Peripheriegeräte, wie z.B. angeschlossene Terminals, müssen sicher aufgestellt werden (siehe M 1.29 - Geeignete Aufstellung eines IT-Systems),
- der lokale Zugriff zur Administration der lokalen Komponenten muß softwaretechnisch und/oder mechanisch gesperrt werden,
- eine eventuell vorhandenes Standardpaßwort des lokalen Zugriffs muß sofort nach Inbetriebnahme geändert werden (zur Auswahl des neuen Paßwortes siehe M 2.11 - Regelung des Paßwortgebrauchs),
- die Sicherheitseigenschaften dauerhaft angeschlossener Terminals oder Rechner, wie z.B. automatische Bildschirmsperre oder Auto-Logout, sind zu aktivieren (siehe M 5.11 - Konsolen der Server und aktiven Netzkomponenten sperren).

Eine lokale Administration bietet folgende Vorteile:

- Die Gefahr des Abhörens von Paßwörtern wird reduziert.
- Auch bei einem Ausfall des Netzsegmentes, in dem sich die aktive Komponente befindet, oder bei einem Ausfall des gesamten Netzes ist eine Administration weiterhin möglich.

Eine lokale Administration bietet allerdings auch folgende Nachteile:

- Aktive Netzkomponenten können im allgemeinen so konfiguriert werden, daß eine lokale oder eine zentrale Administration der aktiven Netzkomponenten möglich ist. Für die Auswahl der Konfigurationsmethode kann jedoch keine generelle Empfehlung gegeben werden. Zu berücksichtigen ist jedoch, daß bei der Konfiguration für eine ausschließlich lokale Administration keine zentrale Administration der aktiven Netzkomponenten mehr möglich ist. Diese muß dann immer vor Ort direkt an den entsprechenden Komponenten vorgenommen werden. In diesem Fall erhöht sich auch die Reaktionszeit im Störungsfall, da unter Umständen längere Wege bis zum Standort der Komponente zurückzulegen sind.

- Der lokale Zugriff ist durch die Realisierung über eine V.24 bzw. EIA-232-E Schnittstelle im allgemeinen langsamer als ein Fernzugriff über das Netz.

H.5 Maßnahmenkatalog Kommunikation

M 5.1 Entfernen oder Kurzschließen und Erden nicht benötigter Leitungen
Nicht mehr benötigte Leitungen sollten nach Möglichkeit entfernt werden. Ist dies aufgrund der damit verbundenen Beeinträchtigung des Dienstbetriebes (Öffnen von Decken, Fensterbank- und Fußbodenkanälen) nicht möglich, sind folgende Maßnahmen sinnvoll:

- Kennzeichnen der nicht benötigten Leitungen in der Revisionsdokumentation und Löschen der Eintragungen in der im Verteiler befindlichen Dokumentation,
- Auftrennen aller Rangierungen und Verbindungen der freien Leitungen in den Verteilern (soweit möglich),
- Kurzschließen der freien Leitungen an beiden Kabelenden und in allen berührten Verteilern,
- Auflegen der freien Leitungen auf Erde (Masse) an beiden Kabelenden und in allen berührten Verteilern; bei dadurch entstehenden Masse-Brumm-Schleifen ist nur einseitig zu erden,
- Gewährleisten, daß nicht mehr benötigte Leitungen bei ohnehin anstehenden Arbeiten im Netz entfernt werden.

M 5.2 Auswahl einer geeigneten Netz-Topographie
Unter der Topographie eines Netzes wird die rein physikalische Struktur eines Netzes in Form der Kabelführung verstanden. Im Gegensatz dazu handelt es sich bei der Netz-Topologie um die logische Struktur eines Netzes. Die Topographie und Topologie eines Netzes sind nicht notwendig identisch. Die Topographie orientiert sich naturgemäß fast immer an den räumlichen Verhältnissen, unter denen das Netz aufgebaut wird. Dies sind u.a.:

- Standorte der Netzteilnehmer,
- verfügbarer Platz für Trassen und Kabel (M 1.21 - Ausreichende Trassendimensionierung),
- erforderliche Kabeltypen (M 1.20 - Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht),
- Anforderungen an den Schutz von Kabeln (M 1.22 - Materielle Sicherung von Leitungen und Verteilern).

Nachfolgend werden die Vor- und Nachteile möglicher Topographien aufgeführt. Weitere denkbare Topographien, die an dieser Stelle nicht genannt sind, können als Spezialfall der betrachteten Strukturen aufgefaßt werden. Im allgemeinen können zwei Grundformen unterschieden werden: der Stern und der Bus. Daraus lassen sich als Erweiterungen aus dem Stern eine baumförmige Struktur und aus dem Bus eine ringförmige Struktur ableiten. Diese vier Formen werden im folgenden kurz dargestellt:

Stern
Bei einem Stern sind alle Teilnehmer des Netzes über eine dedizierte Leitung mit einem zentralen Knoten verbunden. Die häufig anzutreffende Token-Ring-Architektur wird topographisch als Stern verkabelt, bildet topologisch jedoch einen Ring.
Die Vorteile:

- Die Beschädigung einer Leitung beeinträchtigt nur den Betrieb des daran angeschlossenen Systems.
- Änderungen der Zuordnung von Netzteilnehmern zum Anschlußpunkt am zentralen Knoten sowie Trennungen einzelner Teilnehmer lassen sich zentral durchführen.
- Mit einer Sternverkabelung können alle denkbaren logischen Topologien nachgebildet werden.

Die Nachteile:

- Bei einem Ausfall des zentralen Knotens fallen alle angeschlossenen IT-Systeme aus.
- Durch die Einzelanbindung jedes Teilnehmers an den zentralen Knoten ist ein hoher Kabelaufwand erforderlich.
- Mit zunehmender Zahl individueller Leitungen wächst die Gefahr des Übersprechens.
- Durch die sternförmige Verkabelung können Reichweitenprobleme in Abhängigkeit vom verwendeten Kabeltyp und vom eingesetzten Protokoll auftreten (vgl. M 5.3 Auswahl geeigneter Kabeltypen aus kommunikationstechnischer Sicht). In diesem Fall können Verstärker (Repeater) eingesetzt werden, was jedoch u.U. bei einer hohen Zahl von Leitungen sehr kostenintensiv ist. Hinzu kommt, daß nicht beliebig viele Verstärker in eine Leitung geschaltet werden dürfen. Dies ist ebenfalls vom verwendeten Protokoll abhängig. Eine andere Möglichkeit ist hier der Übergang zu einer baumförmigen Struktur.

Baum
Eine Baumstruktur entsteht durch die Verbindung mehrerer Sterne. In diesem Fall werden die Netzteilnehmer zu Gruppen zusammengefaßt, die an dezentrale Netzknoten sternförmig angeschlossen werden. Diese dezentralen Netzknoten sind wiederum über eine Leitung oder mehrere dedizierte Leitungen miteinander verbunden. Unter Umständen werden auch alle dezentralen Netzknoten an einem zentralen Netzknoten zusammengeführt.
Die Vorteile:

- Für den Anschluß der Systeme an die dezentralen Netzknoten gelten die gleichen Vorteile wie beim Stern.
- Für neue Teilnehmer muß nur im Bereich des dezentralen Netzknotens neu verkabelt werden.
- Bei entsprechender Auslegung der dezentralen Netzknoten ist ein Datenaustausch zwischen den Teilnehmern eines solchen Knotens auch bei einem Ausfall der anderen Knoten möglich.
- Durch die Verbindung der dezentralen Knoten untereinander über eine Leitung reduziert sich der Verkabelungsaufwand.
- Zur Überwindung großer Entfernungen zwischen den Knoten reicht die Verstärkung auf einer Leitung (Kostenersparnis).
- Für die Verbindung der Knoten ist der Einsatz hochwertigerer (meist teurerer) Kabel sinnvoll, mit denen auch größere Distanzen ohne zusätzliche Verstärkung überwunden werden können. Das bringt gegenüber den sonst notwendigen Verstärkern Vorteile in bezug auf Ausfallsicherheit und Kostenreduzierung.
- Baumstruktur ermöglicht es, durch Vermaschung der einzelnen Knoten redundante Verbindungen aufzubauen.

Die Nachteile:

- Bei Störung eines Übergangs zu einem anderen dezentralen Netzknoten wird der Betrieb mit allen daran angeschlossenen Teilnehmern unterbrochen.

Bus
Bei einem Bus werden alle Netzteilnehmer an eine gemeinsame Leitung angeschlossen. Dies geschieht im allgemeinen durch ein zentrales Kabel, an das mit Stichleitungen die einzelnen Teilnehmer angebunden werden. Die Vorteile:

- Die Verkabelung reduziert sich auf ein Kabel, hinzu kommen evtl. notwendige Stichleitungen.
- Die Nachinstallation neuer Teilnehmer erfordert im allgemeinen nur geringen Verkabelungsaufwand. Sie werden einfach an das vorhandene Buskabel angeschlossen.
- Der Bus ist durch den Einsatz von Verstärkern einfach verlängerbar. Dabei sind jedoch die Längenrestriktionen aufgrund des eingesetzten Kabeltyps und des verwendeten Protokolls zu beachten (vgl. M 5.3 Auswahl geeigneter Kabeltypen aus kommunikationstechnischer Sicht).
- Ressourcen können an nahezu beliebigen Stellen am Bus angeschlossen werden.

- Eine Busverkabelung erfordert durch das zentrale Kabel deutlich weniger Platz als eine vergleichbare Sternverkabelung mit TP-Kabel.

Die Nachteile:

- Störungen, die auf das Kabel wirken, beeinträchtigen den gesamten Bus.
- Unterbrechungen des Buskabels bringen den gesamten Datenverkehr zum Erliegen.
- Ab einer gewissen maximalen Länge und einer bestimmten Anzahl von Teilnehmern ist keine einfache Erweiterung des Busses mehr möglich.
- Abhängig vom Kabeltyp müssen Restriktionen beim Anschluß neuer Teilnehmer beachtet werden (z.B. der Mindestabstand zwischen zwei Teilnehmern).

Ring
Der Ring ist aus topographischer Sicht ein Bus, dessen beide Enden miteinander verbunden sind. Eine Sonderform des Rings besteht in der doppelten Ausführung als Doppelring, wie sie z.B. bei FDDI Verwendung findet.
Die Vorteile:

- Der Ring kann bei einer Leitungsunterbrechung mit gewissen Beeinträchtigungen weiterarbeiten. Die Art der Beeinträchtigung hängt vom für den Ring verwendeten Netzzugangsprotokoll ab. Beeinträchtigungen können z.B. Bandbreitenverluste sein.
- Die mögliche Ausführung als Doppelring ermöglicht eine zusätzliche Redundanz bzw. Fehlertoleranz.

Die Nachteile:

- Die verfügbaren Protokolle für Ring- und Doppelringsysteme sind beschränkt, d.h. es können nicht alle Protokolle auf diesen eingesetzt werden. Dies kann sich für die zukünftige Weiterentwicklung des Netzes nachteilig auswirken.

Collapsed und Distributed Backbone
Ein Collapsed Backbone ist eine spezielle Ausprägung eines Netzknotens, der innerhalb seiner Backplane (eine lokale Hochgeschwindigkeitsverbindung innerhalb eines Gerätes) eine der o.g. Strukturen oder eine Mischform daraus realisiert. Bei einem Collapsed Backbone werden alle Kabel zentral zu einem Netzknoten geführt, so daß es sich im Prinzip um eine Sternverkabelung handelt. Innerhalb des Netzknotens können nun die unterschiedlichsten Strukturen unterstützt werden. So werden beispielsweise bei einer Baumstruktur die nötigen Verbindungswege zwischen den dezentralen Sternen durch sehr kurze Verbindungen innerhalb des Netzknotens realisiert.

Die Vorteile:

- Alle Kabelanschlüsse können zentral kontrolliert und verwaltet werden.

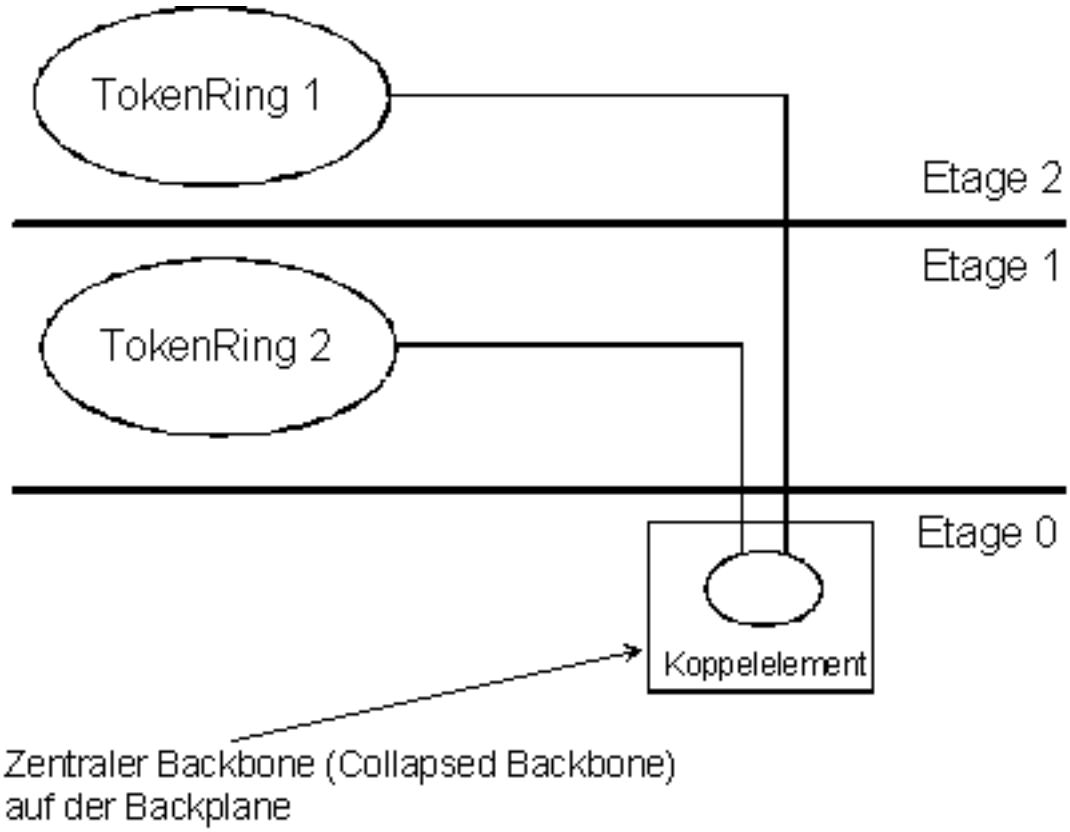

Abbildung H.1: Collapsed und Distributed Backbone

- Es werden im allgemeinen hohe Übertragungsraten in der Backplane erreicht. Hierdurch steht, je nach Produkt, zwischen den Segmenten die volle Netzbandbreite zur Verfügung.

Die Nachteile:

- Bei einem Ausfall des Collapsed Backbones fallen alle Netzzugänge aus.

Bei einem Distributed Backbone sind die einzelnen Netzkomponenten, die zum Backbone gehören, räumlich verteilt und werden durch die normale Netzinfrastruktur gekoppelt. Topographische Bäume werden beispielsweise im allgemeinen durch einen Distributed Backbone realisiert. Die Vorteile:

- Bei einem Ausfall einer Netzkomponente sind nicht unbedingt alle IT-Systeme betroffen.

Die Nachteile:

- Die Kopplung der Backbone-Komponenten erfolgt über die im Vergleich zum Collapsed Backbone relativ langsame normale Netzverkabelung.
- Es ist keine zentrale Administration der Backbone-Anschlüsse möglich.

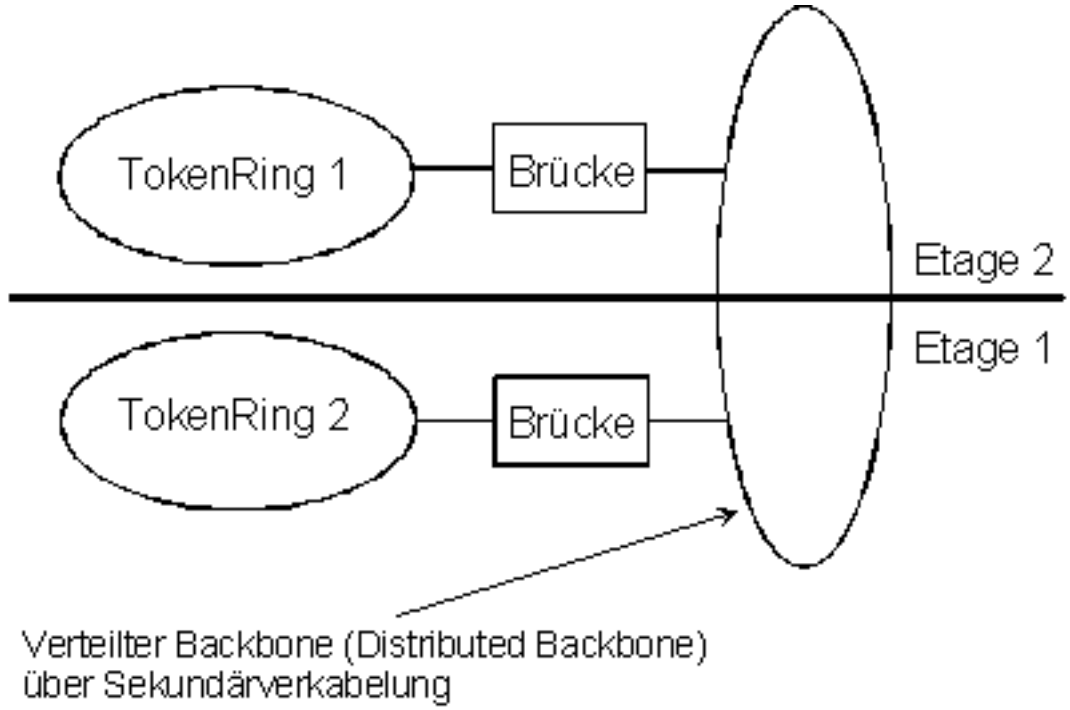

Abbildung H.2: Verteilter Backbone

Bei der Auswahl einer geeigneten Netztopographie kann, wie bereits eingangs erwähnt, keine allgemeingültige Empfehlung gegeben werden. Solch eine Entscheidung wird u. a. immer stark durch bauliche Gegebenheiten beeinflußt. Allgemein üblich ist heute bei Neuinstallationen eine strukturierte Verkabelung in Stern- oder Baumform. Hierbei ist es sinnvoll, im Backbone-Bereich (Primär- und Sekundärbereich) Lichtwellenleiter und für die Etagenverkabelung (Tertiärbereich) Twisted-Pair-Kabel mind. der Kategorie 5 zu verwenden. Mit Primärbereich wird dabei der Bereich der Kabelführung, der Gebäude miteinander verbindet, bezeichnet und mit Sekundärbereich die Verkabelung zur Verbindung der aktiven Netzkomponenten einzelner Abschnitte innerhalb eines Gebäudes (z.B. zur Verbindung von Stockwerken).
Die Wahl dieser Medien für die einzelnen Bereiche gewährleistet aus heutiger Sicht eine zukunftssichere Verkabelung, die auch höheren Bandbreitenanforderungen v.a. im Backbone-Bereich gerecht wird. Im Einzelfall ist jedoch auch zu prüfen, ob es sinnvoll oder notwendig ist, eine Mischform aus Stern- und Ringverkabelung zu installieren. Hier bietet sich häufig die Möglichkeit, die Primärverkabelung zwischen Gebäuden als FDDI-Doppelring und die Sekundär- und Tertiärverkabelung wie o.g. als Stern- oder Baum auszuführen.

M 5.3 Auswahl geeigneter Kabeltypen unter kommunikationstechnischer Sicht
Die Auswahl des Kabels wird durch die erforderliche Übertragungsrate bestimmt und davon, welche Entfernungen ohne Verstärker zu überwinden sind. Vor- und Nachteile werden nachfolgend unter IT-Sicherheitsgesichtspunkten beschrieben. Drei Kabelgrundtypen stehen zur Verfügung:

Ungeschirmtes Kupferkabel
Die vom Kupferkabel bewältigte Bandbreite reicht heute, abhängig vom Kabelaufbau und Schirmung, bis 100 MHz, wobei die maximalen Übertragungsstrecken mit zunehmender Frequenz abnehmen (von 3 km bis zu 100m). Im Entwurf der DIN EN 50 173 sind in Kapitel 6.1 die wesentlichen Unterschiede dargestellt. Es reicht für Telefonie und einen Großteil heute betriebener Datennetze aus.
Vorteile:

- Das Kabel ist (noch) billiger als die anderen Kabel.
- Die Installation erfordert bei niedrigen Frequenzen (kHz-Bereich, Klasse A- und B-Kabel) keine Spezialkenntnisse.
- Oft können vorhandene Telefonnetze genutzt werden.

Nachteile:

- Übertragungsfrequenzen über 150 MHz sind nur mit sehr teueren Kabelaufbauten möglich. Eine Übertragung höherer Frequenzen ist technisch nicht mehr sinnvoll realisierbar.
- Im oberen MHz Bereich (Klasse C- und D-Kabel) erfordert die Installation Spezialkenntnisse (Hochfrequenztechnik!).
- Durch einfach zu realisierende galvanische Ankopplung läßt sich das Kupferkabel leicht abhören.
- Umrangierungen und Ankopplungen sind meßtechnisch, wenn überhaupt, nur sehr schwierig erkennbar.
- Mit zunehmender Bandbreitenforderung sinkt die maximale unverstärkte Übertragungsstrecke auf ca. 100 m (Klasse D, Kat-5-Kabel).
- Bei hochpaarigen Kabeln kann es zum Übersprechen kommen.
- Ungeschirmte Kupferkabel sind sehr empfindlich gegenüber elektrischen, elektrostatischen und induktiven Störungen.

Koaxial-Kabel
Es wird im MHz-Bereich u.a. in Breitbandverteilnetzen (Kabelfernsehen) und in der Bus-Technik (z.B. Ethernet) angewendet.
Vorteile:

- Die Bandbreite und die unverstärkte Übertragungsstrecke sind deutlich höher als beim Kupferkabel.
- Übersprechen tritt nicht auf.

- Die unverstärkte Übertragungsstrecke beträgt je nach Kabeltyp bis zu 400 m.

Nachteile:

- Das Koaxialkabel ist deutlich teurer als das Kupferkabel.
- Verlegung und Installation erfordern Kenntnis und Erfahrung.
- Koaxialkabel erfordern deutlich mehr Platz als alle anderen Kabeltypen.
- Das Kabel ist mit mäßigem Aufwand abhörbar.
- Das Koaxialkabel ist durch elektrische, elektrostatische und induktive Störungen beeinflußbar.

Das Lichtwellenleiterkabel (LWL-Kabel)
Es wird für die Datenfernübertragung in allen Netzen und zunehmend für LANs, insbesondere aber zur Realisierung von Backbone-Ringen, verwendet.
Vorteile:

- Die Bandbreite und die unverstärkte Reichweite ist deutlich höher als bei allen anderen Kabeln (je nach Typ bis zu ca. 1 GHz und 10 km).
- Abhören ist nur mit hohem technischen Aufwand möglich.
- Unzulässige Umrangierungen sind durch verfügbare Technik einfach zu erkennen.
- LWL-Kabel sind unempfindlich gegenüber allen nicht zerstörenden Umfeldbedingungen. Dadurch ist es nahezu überall einsetzbar.
- LWL-Kabel brauchen von allen Kabeln am wenigsten Platz.

Nachteile:

- Der Preis liegt (noch) etwas über dem der hochwertigsten Kupferkabel (Klasse D, Kat-5-Kabel).
- Die Verlegung erfordert Kenntnis und Erfahrung, die Herstellung von Spleißen und Steckanschlüssen erfordert Spezialkenntnisse und Sonderwerkzeuge.

M 5.4 Dokumentation und Kennzeichnung der Verkabelung
Für Wartung, Fehlersuche, Instandsetzung und für erfolgreiche Überprüfung der Verkabelung ist eine gute Dokumentation und eindeutige Kennzeichnung aller Kabel erforderlich. Die Güte dieser Revisionsdokumentation ist abhängig von der Vollständigkeit, der Aktualität und der Lesbarkeit.
In dieser Dokumentation (auch Bestandsplan genannt) sind alle das Netz betreffenden Sachverhalte aufzunehmen:

- genauer Kabeltyp,

- nutzungsorientierte Kabelkennzeichnung,
- Standorte von Zentralen und Verteilern mit genauen Bezeichnungen,
- genaue Führung von Kabeln und Trassen in der Liegenschaft (Einzeichnung in bemaßte Grundriß- und Lagepläne),
- Trassendimensionierung und -belegung,
- Belegungspläne aller Rangierungen und Verteiler,
- Nutzung aller Leitungen, Nennung der daran angeschlossenen Netzteilnehmer,
- technische Daten von Anschlußpunkten,
- Gefahrenpunkte,
- vorhandene und zu prüfende Schutzmaßnahmen.

Es muß möglich sein, sich anhand dieser Dokumentation einfach und schnell ein genaues Bild über die Verkabelung zu machen.
Da es mit zunehmender Größe eines Netzes nicht möglich ist, alle Informationen in einem Plan unterzubringen, ist eine Aufteilung der Informationen sinnvoll. Tatsächliche Lageinformationen sind immer in maßstäbliche Pläne einzuzeichnen. Andere Informationen können in Tabellenform geführt werden. Wichtig dabei ist eine eindeutige Zuordnung aller Angaben untereinander.
Um die Aktualität der Dokumentation zu gewährleisten, ist sicherzustellen, daß alle Arbeiten am Netz rechtzeitig und vollständig demjenigen bekannt werden, der die Dokumentation führt. Es ist z.B. denkbar, die Ausgabe von Material, die Vergabe von Fremdaufträgen oder die Freigabe gesicherter Bereiche von der Mitzeichnung dieser Person abhängig zu machen.
Da diese Dokumentation schutzwürdige Informationen beinhaltet, ist sie sicher aufzubewahren und der Zugriff zu regeln.

M 5.5 Schadensmindernde Kabelführung
Bei der Planung von Kabeltrassen ist darauf zu achten, daß erkennbare Gefahrenquellen umgangen werden. Grundsätzlich sollen Trassen nur in den Bereichen verlegt werden, die ausschließlich dem Benutzer zugänglich sind. Ein übersichtlicher Aufbau der Trassen erleichtert die Kontrolle. Trassen und einzelne Kabel sollen immer so verlegt werden, daß sie vor direkten Beschädigungen durch Personen, Fahrzeuge und Maschinen geschützt sind.
Der Standort von Geräten sollte so gewählt werden, daß Kabel nicht im Lauf- oder Fahrbereich liegen. Ist dies nicht zu vermeiden, sind die Kabel den zu erwartenden Belastungen entsprechend durch geeignete Kanalsysteme zu schützen.
Grundsätzlich ist bei Geräteanschlußleitungen auf eine ausreichende Zugentlastung der Kabel in den Steckern zu achten. Bisweilen kann es sinnvoll sein, auf die vorgesehene Verschraubung von Steckern zu verzichten. Bei Zugbelastung werden nur Steckverbindungen auseinandergerissen und nicht die Stecker-Kabel- oder Stecker-Geräte-Verlötung.
Tiefgaragen stellen ein großes Problem für eine schadensmindernde Kabelführung dar. Durch

die Sicherheitsschaltungen und die langen Offenzeiten von Einfahrtstoren ist der Zutritt von Fremdpersonen zu Tiefgaragen nie auszuschließen. Durch die in der Regel geringen Deckenhöhen ist es mit einfachen Mitteln möglich, sich Zugriff zu dort verlaufenden Trassen zu verschaffen. Durch Trassen im Fahrbereich kann die zulässige Fahrzeughöhe unterschritten werden. Beschädigungen oder Zerstörungen der Trassen und Kabel durch Fahrzeuge sind dann nicht auszuschließen.
Bei gemeinsam mit Dritten genutzten Gebäuden ist darauf zu achten, daß Kabel nicht in Fußbodenkanälen durch deren Bereiche führen. Fußboden- und Fensterbank-Kanalsysteme sind gegenüber den fremdgenutzten Bereichen mechanisch fest zu verschließen. Besser ist es, sie an den Bereichsgrenzen enden zu lassen.
Bereiche mit hoher Brandgefahr sind zu meiden. Ist dies nicht möglich und ist der Betriebserhalt aller auf der Trasse liegenden Kabel erforderlich, ist der entsprechende Trassenbereich mit Brandabschottung zu versehen. Ist der Betriebserhalt nur für einzelne Kabel erforderlich, ist dafür ein entsprechendes Kabel zu wählen.
In Produktionbetrieben ist mit hohen induktiven Lasten und daraus resultierenden Störfeldern zu rechnen. Auch diese sind bei der Trassen- und Kabelverlegung zu berücksichtigen. Für den Schutz der Kabel gilt sinngemäß das gleiche wie bei der Brandabschottung. Bei Erdtrassen ist ca. 10 cm über der Trasse ein Warnband zu verlegen. Bei einzelnen Kabeln (ohne Rohr) ist der Einbau von Kabelabdeckungen sinnvoll.

M 5.6 Obligatorischer Einsatz eines Netzpaßwortes Standardmäßig sollte jeder Benutzer (und auch die Administratoren) in einem lokalen Netz mit einem Benutzer-Paßwort ausgestattet werden. Für den korrekten Umgang mit dem Paßwort sind die Bedingungen aus Maßnahme M 2.11 - Regelung des Paßwortgebrauchs einzuhalten.

M 5.7 Netzverwaltung
Netze können zentral oder lokal an den einzelnen Knoten verwaltet werden. Das ist neben den technischen Möglichkeiten davon abhängig, wer den Netzknoten administriert. In jedem Fall ist eine zentrale Koordinierung aller Netzaktivitäten einer Behörde oder eines Unternehmens notwendig, damit Redundanzen vermieden werden. Zentral gesteuert werden sollten:

- die Auswahl und Verlegung der Kabel,
- die Auswahl der eingesetzten IT-Systeme und Anwendungen, um Unverträglichkeiten zu vermeiden,
- die zentrale Vergabe von Netzadressen und Benutzer-IDs,
- die organisatorische Zuteilung von Netzkomponenten z.B. zu Abteilungen.

Die einzelnen Netzknoten und die dort angeschlossenen IT-Systeme können auch lokal verwaltet werden. Die Aufgaben- und Verantwortungsbereiche der Systemverwalter müssen dabei klar spezifiziert und eindeutig geregelt sein (siehe auch M 2.26 - Ernennung eines Administrators und eines Vertreters).

M 5.8 Monatlicher Sicherheitscheck des Netzes
Der Netzadministrator sollte regelmäßig, mindestens monatlich, einen Sicherheitscheck des Netzes durchführen. Einige Netzbetriebssysteme bieten Programme an, mit denen diese Untersuchung automatisiert durchgeführt werden kann. Ein Beispiel ist das Programm SECURITY im Verzeichnis SYS:SYSTEM bei Novell 3.11. Folgende Parameter werden u.a. geprüft:

- Gibt es Benutzer ohne Paßwort?
- Gibt es Benutzer, die längere Zeit das Netz nicht mehr benutzt haben?
- Gibt es Benutzer, deren Paßwort nicht die erforderlichen Bedingungen einhält?
- Welche Benutzer besitzen die gleichen Rechte wie der Supervisor?

M 5.9 Protokollierung am Server
Die am Netz-Server mögliche Protokollierung ist in einem sinnvollen Umfang zu aktivieren. In regelmäßigen Abständen muß der Netzadministrator die Protokolldateien des Netz-Servers überprüfen. Dabei sind insbesondere folgende Vorkommnisse von Interesse:

- falsche Paßworteingabe für eine Benutzerkennung bis hin zur Sperrung der Benutzerkennung bei Erreichen der Fehlversuchsgrenze,
- Versuche von unberechtigten Zugriffen,
- Stromausfall,
- Daten zur Netzauslastung und -überlastung.

Da diese Log-Dateien mit der Zeit sehr umfangreich werden können, sollten die Auswertungsintervalle so kurz gewählt werden, daß eine sinnvolle Auswertung möglich ist.

M 5.10 Restriktive Rechtevergabe
Zugriffsrechte auf Dateien, die auf der Festplatte des Netz-Servers gespeichert sind, müssen restriktiv vergeben werden. Jeder Benutzer erhält nur auf die Dateien ein Zugriffsrecht, die er für seine Aufgabenerfüllung benötigt. Das Zugriffsrecht selbst wiederum wird auf die notwendige Zugriffsart beschränkt (Dazu siehe auch M 2.5 - Aufgabenverteilung und Funktionstrennung, M 2.7 - Vergabe von Zugangsberechtigungen und M 2.8 - Vergabe von Zugriffsrechten). So ist es zum Beispiel in den seltensten Fällen notwendig, ein Schreibrecht auf Programmdateien zu vergeben.
Meist darf über die Vererbung von Rechten auf Dateien in Unterverzeichnissen zugegriffen werden, wenn ein Zugriffsrecht auf das übergeordnete Verzeichnis bestand. Daraus ergibt sich, daß Zugriffsrechte auf höchster Ebene (Volume-Ebene) nur sehr eingeschränkt erteilt werden sollten. Insbesondere ist bei der Installation neuer Sof
twareprodukte die Rechtevergabe erneut zu überprüfen. Sind die PCs mit Diskettenlaufwerken ausgestattet, so ist auf restriktive Rechtevergabe besonderen Wert zu legen.

Sollte der Speicherplatz des Netz-Servers gering ausgelegt sein, kann eine Beschränkung der maximalen Speicherkapazität, die ein Benutzer auf dem Netz-Server belegen darf, eingestellt werden.

M 5.13 Geeigneter Einsatz von Elementen zur Netzkopplung

Geräte zur Netzkopplung wie Router, Bridges oder Gateways verbinden nicht nur Netze, sie können auch zur physikalischen oder logischen Segmentierung von Netzen benutzt werden. Durch die Aufteilung von großen Netzen in Teilnetze kann z.B. die Verfügbarkeit verbessert werden, da ein Fehler nur einen begrenzten Bereich des Netzes betrifft und dort schneller lokalisiert werden kann. Bei zunehmender Anzahl von Netzstationen können Antwortzeiten unakzeptabel und eine Teilnetzbildung zur Lasttrennung notwendig werden. Der Schutz von sensitiven Informationen kann ein weiterer Grund zur Segmentierung von Netzen sein, so daß diese nicht auf dem Gesamtnetz verfügbar sind. Um sich vor externen Angreifern zu schützen, kann es sinnvoll sein, einen Transfer von Paketen nur vom sicheren ins unsichere Netz zuzulassen, zum Schutz von vertraulichen Daten kann es andererseits sinnvoll sein, keinen Transfer von Paketen vom sicheren ins unsichere Netz zuzulassen.
Die Aufteilung in Netzsegmente bzw. die Netzkopplung kann auf verschiedenen Schichten nach dem OSI-Modell erfolgen. Netzkoppelkomponenten auf der physikalischen Schicht (Schicht 1) des OSI-Modells sind z.B. Repeater, auf der Sicherungsschicht (Schicht 2) z.B. Bridges, auf der Vermittlungsschicht (Schicht 3) z.B. Router und auf der Anwendungsschicht (Schicht 7) im allgemeinen Gateways. Zum besseren Verständnis ist das OSI-Modell in der folgenden Abbildung dargestellt.

Das OSI/ISO Referenzmodell

Eine Verbindung mit einem anderen Netz auf einer höheren Schicht (ab Schicht 3) des OSI-Modells ermöglicht es z. B. den Datenfluß nach Sicherheitsanforderungen zu reglementieren und somit zu schützende und unsichere Netze kontrolliert zu verbinden.
Andererseits kann das Trennen von Netzen erforderlich sein, wenn diese vor Zugriffen aus dem jeweils anderen Netz geschützt werden sollen oder um die Verfügbarkeit der Netze im Fehlerfall zu erhöhen bzw. die Netzlast in den jeweiligen Netzsegmenten zu verringern.
Um Manipulationen zu verhindern, müssen alle Geräte zur Netzkopplung so aufgestellt werden, daß nur Berechtigte physikalischen Zugang haben.

Repeater

Repeater arbeiten auf der Schicht 1 des OSI-Modells und sind einfache Signalverstärker. Dadurch erlauben sie es, die maximale Kabellänge eines bestehenden Netzsegmentes zu verlängern bzw. mehrere Netzsegmente zu verbinden. Beispielsweise kann mit ihnen beim Einsatz von Ethernet auf Koaxialkabelbasis die maximale Kabellänge auf über 185 m bzw. auf über 500 m (für Thin- bzw. Thick-Ethernetkabel) verlängert werden. Zu beachten sind hierbei die Konfigurationsregeln für Repeater, die die Anzahl und Anordnung von Repeatern beschränken.
Im Fall einer Twisted-Pair-Verkabelung werden Repeater häufig als zentraler oder dezentraler Netzknoten zur Verbindung der einzelnen Netzteilnehmer eingesetzt. Da hierfür mehrere Repeater in einem Gerät miteinander verbunden werden müssen, werden diese Geräte auch

Multiport-Repeater genannt. Multiport-Repeater werden häufig auch als Hubs bzw. als Mini-Hubs bezeichnet.
Durch die somit erreichte Trennung auf der Schicht 1 des Netzes werden elektrische Fehler auf ein Segment beschränkt. Dies gilt jedoch nicht für Fehler in höheren Schichten (z.B. zu häufige Kollisionen oder ein Broadcast-Sturm). Von einigen Herstellern gibt es inzwischen auch Multiport-Repeater, die Informationen aus Schicht 2 auswerten (aber noch keine Bridges sind) und dadurch z.B. die Implementation von Zugriffsbeschränkungen erlauben. Mit solchen Geräten läßt sich beispielsweise einstellen, daß nur bestimmte Netzteilnehmer Zugang zum Netz bekommen.

Bridge
Die Verbindung von Netzen auf der Ebene 2 des ISO-OSI-Referenzmodells erfolgt über Bridges. Eine Bridge verbindet zwei Netze, die in der Regel dasselbe Logical Link Control (LLC) Protokoll benutzen, aber unterschiedliche Medium Access Control (MAC) Protokolle. Eine Bridge kann z.B. ein Ethernet mit einem Token-Ring-Netz verbinden. Eine solche Bridge wird dann Translation-Bridge oder T-Bridge genannt.
Hierdurch ergeben sich drei wesentliche Vorteile:

- Die Bridge trennt Collision-Domains, d.h. performanceverringernde Kollisionen bei CSMA/CD-basierten Netzen gelangen nicht in das andere Segment.

- Eine Bridge leitet nur diejenigen Datenpakete in ein anderes Segment, die dort auch ihre Zieladresse haben. Hierdurch bleibt der Datenverkehr auf das jeweils notwendige Segment beschränkt, wodurch die Abhörsicherheit steigt.

- Schließlich steigt dadurch auch der Datendurchsatz in jedem Segment, da auf jeder Seite der Bridge unabhängig Daten übertragen werden können und somit eine Lasttrennung erfolgt.

Switch (Ethernet, Token-Ring, ATM)
Ein Switch ist eine Variante einer Brücke, die mehrere logische LAN-Segmente verbindet (Multiport-Brücke), arbeitet also auf Schicht 2 des OSI-Modells. Einige neuere Produkte implementieren zusätzlich auch Switching-Funktionalität auf der Schicht 3 des OSI-Modells, erlauben also hiermit auch eine Schicht 3 Segmentierung.
Ein Ethernet-Switch besteht aus mehreren Bridges, die auf geeignete Weise intern miteinander verbunden sind (z.B. über eine sogenannte Switching-Matrix).
Ein Ethernet-Switch bietet die Vorteile einer Bridge für mehrere Anschlüsse (üblich sind derzeit 8 bis 32 Anschlüsse pro Switch), d.h. jeder Netzteilnehmer bzw. jedes Segment an einem Switchanschluß bildet eine eigene Collision-Domain und der Verbindungsaufbau beruht auf den tatsächlichen Erfordernissen. Damit kann jedes angeschlossene Segment mit allen anderen unbeeinflußt von dem Verkehr und der Last der anderen Segmente kommunizieren, solange das entsprechende Segment nicht bereits anderweitig belegt ist. Switches bieten sich vor allem zur Lasttrennung und als zentrale Kopplungskomponente von mehreren Teilsegmenten an. Durch die Kaskadierung von Switches, d.h. durch den Anschluß von nachgeordneten Switches an einen

zentralen Switch, lassen sich bei geeigneter Wahl der logischen Netzstruktur sehr leistungsfähige Netze bilden.
Ethernet-Switches, die nach der IEEE-Norm für Bridges arbeiten, benutzen die Store-and-Forward-Technik. Bei dieser Technik wird zunächst das gesamte Ethernet-Paket des Quellports eingelesen und auf Korrektheit überprüft. Nur korrekt und vollständig empfangene Pakete werden an das Zielsegment weitergeschickt. Die Verzögerungszeit solcher Switches ist relativ hoch, sie garantieren aber auch, daß keine fehlerhaften Pakete in andere Segmente übertragen werden. Der Einsatz solcher Store-and-Forward-Switche ist dann zu empfehlen, wenn Wert auf maximale Verfügbarkeit und Integrität und nicht so sehr auf Bandbreite gelegt wird.
Im Gegensatz dazu wurden alternativ Techniken entwickelt, die den Durchsatz eines Ethernet-Switches erhöhen, also die Verzögerungszeit zu verkleinern, die ein zu verarbeitendes Datenpaket erfährt. Hierzu wird die On-the-Fly-Technik (auch Cut-Through genannt) eingesetzt, die nicht mehr das gesamte Paket einliest und überprüft, sondern lediglich die Zieladresse des Paketes auswertet und daraufhin sofort das gesamte Paket an diese Adresse schickt. On-the-Fly-Switches sind damit maximal um den Faktor 20 schneller als Store-and-Forward-Switches. Allerdings leiten sie auch fehlerhafte Pakete in das andere Segment, wodurch die Bandbreite und damit u.U. die Verfügbarkeit der einzelnen Segmente beeinträchtigt werden kann. On-the-fly-Switches sollten also in Netzen eingesetzt werden, in denen wenig fehlerhafte Pakete auftreten können und in denen es auf maximalen Durchsatz ankommt. Die meisten Hersteller bieten heute Switches an, die beide Techniken beherrschen und entsprechend konfiguriert werden können.
Von einigen Produkten wird inzwischen auch ein Switching auf der Schicht 3 des OSI-Modells unterstützt. Dabei werden die Netzteilnehmer nicht mehr nach ihrer MAC-Adresse unterschieden (Layer-2-Switching), sondern nach den Adressen der Schicht 3 (für den TCP/IP-Protokollstapel ist dies die IP-Adresse). Ein Layer-3-Switching kann weitere Performancevorteile bedeuten, in diesem Fall muß aber der Switch, analog zu einem Router, die auf der Schicht 3 verwendeten Protokolle verarbeiten können.
Switches für ATM oder Token-Ring sind funktional einem Ethernet-Switch sehr ähnlich, d.h. auch ein Switch für diese Protokolle ermöglicht es, daß zwei Netzteilnehmer oder Netzbereiche unabhängig von den anderen kommunizieren können. Für ATM-Netze ist durch die zugrundeliegende Konzeption der Einsatz eines Switches sogar zwingend.
Bei der Auswahl von Switches, mit denen ein Collapsed Backbone realisiert werden soll, muß die zur Verfügung gestellte Portdichte berücksichtigt werden. Bei einem „Collapsed backbone“ sollte es vermieden werden, mehrere Switches einsetzen zu müssen, die nicht über eine gemeinsame (Hochgeschwindigkeits-) Backplane verfügen (vgl. M 5.2 - Auswahl einer geeigneten Netz-Topographie).

Router
Router trennen bzw. verbinden Netze auf der Schicht 3 des OSI-Modells. Damit arbeiten Router nicht mehr protokolltransparent (wie z.B. Repeater oder Bridges), sondern müssen die im Einsatz befindlichen Protokolle auf der Vermittlungsschicht auch verarbeiten können. Dadurch verlangsamen Router den Datenverkehr zwischen zwei verbundenen Teilnetzen merklich, da der Router jedes Paket auf der Schicht 3 auswerten muß.

Aufgrund ihrer Fähigkeit, Protokolle zu verarbeiten und diese umzusetzen, werden Router vor allem zur LAN-LAN-Kopplung und zur Anbindung eines LANs an ein WAN genutzt. Ein Router kann beispielsweise zwei LANs über eine ISDN-Leitung miteinander verbinden. Hierbei wird das LAN-Protokoll unverändert in das WAN-Protokoll eingekapselt (encapsulation) und übertragen. Ein anderes Protokoll, das hier beispielsweise zum Einsatz kommen kann, ist das X.25-Protokoll. In großen Netzen, in denen viele Teilnetze durch Router verbunden sind, ist eine wesentliche Aufgabe des Routers die Wegewahl (Routing) zwischen den Teilnetzen. Hierbei können prinzipiell zwei Verfahren unterschieden werden:

- Das statische Routing, bei dem die Wegewahl manuell angegeben wird.
- Das dynamische Routing, bei dem die Wegewahl durch die Router bestimmt und laufend aktualisiert wird. Hierzu stehen mehrere Algorithmen bzw. Protokolle zur Verfügung, die auch den Abgleich der Router untereinander gewährleisten. Die bekanntesten Protokolle sind RIP (Routing Information Protocol), OSPF (Open Shortest Path First) und IGRP (Interior Gateway Routing Protocol). Für die Auswahl eines geeigneten Routing-Protokolls ist auch M 4.82 - Sichere Konfiguration der aktiven Netzkomponenten zu beachten.

Weiterhin kann durch den Einsatz von Filtern eine Zugriffskontrolle gewährleistet werden, d.h. welche Systeme mit welchen Protokollen über den Router in welche Richtung miteinander kommunizieren dürfen.

Konzentratoren und Hubs
Unter einem Hub wird eine Komponente verstanden, die eine oder mehrere aktive Netzkoppelkomponenten aufnimmt und eine Kommunikation dieser Komponenten untereinander über eine interne Backplane (siehe auch M 5.2 Auswahl einer geeigneten Netz-Topographie) ermöglicht. Hubs, die bei Bedarf mehrere Netzkoppelkomponenten aufnehmen können, werden als modulare Hubs bezeichnet. Entsprechend werden Hubs, die nur aus einer Koppelkomponente bestehen und nicht zur Aufnahme weiterer Komponenten bestimmt sind, als nicht modulare Hubs bezeichnet. Wenn es möglich ist, die Backplanes mehrerer Hubs miteinander zu verbinden, werden diese Hubs als stackable Hubs bezeichnet. Durch den Einsatz eines Hubs oder eines Konzentrators erfolgt die Leitungsführung zumindest zum Teil sternförmig zu den Endgeräten, aus diesem Grund werden Hubs oder Konzentratoren auch Sternkoppler genannt.
Wie bereits bei den Repeatern erwähnt ist die kleinste Form eines Konzentrators bzw. eines Hubs ein Multiport-Repeater. Modulare Hubs dagegen erlauben die Aufnahme verschiedener Koppelelemente, die selbst wiederum auf verschiedenen Schichten arbeiten können (z.B. Repeater, Bridges und Router). Durch diese Konzentration der Netzkoppelkomponenten an einem Ort ergeben sich Vorteile in der einfacheren Administration des Netzes, allerdings beeinflußt der Ausfall eines solchen zentralen Hubs auch das gesamte Netz. Für diesen Fall sind geeignete Vorsorge-Maßnahmen zu treffen, wie z.B. die redundante Auslegung der Netzkomponenten (siehe M 6.53 Redundante Auslegung der Netzkomponenten).

Gateway
Ein Gateway verbindet zwei Netze auf der Anwendungsschicht (Schicht 7) des OSI-Modells.

Daher erfüllt er nicht nur die Aufgabe, ein Netzprotokoll zu konvertieren, sondern auch Daten auf Anwendungsebene zu transportieren, gegebenenfalls zu modifizieren und unter Sicherheitsgesichtspunkten auszuwerten. Ein typisches Einsatzfeld eines Gateways ist die Kommunikation von Systemen in einem TCP/IP-Netz mit einem SNA-Host. In diesem Fall besteht das Gateway aus einer Kombination von Hard- und Software. Es gibt jedoch auch Gateways, die nur durch Software realisiert sind. Dies sind z.B. Mail-Gateways, die unterschiedliche Mailformate verstehen und konvertieren können.

M 5.14 Absicherung interner Remote-Zugänge
Die Remote-Zugänge bei TK-Anlagen werden für Fernwartungs-, Fernadministrations- und Netzmanagementaufgaben genutzt. Ferner können noch Remote-Zugänge für die Anlagennutzer (Dial-In-Optionen) existieren.
Grundsätzlich läßt sich zwischen

- einem Remote-Zugang im eigenen TK-Anlagenverbund (interner Zugang) und
- einem Remote-Zugang aus anderen Netzen (externer Zugang)

unterscheiden.
Beim internen Remote-Zugang wird die Absicherung einer Fernwartung innerhalb eines TK-Anlagenverbundes betrachtet. Unter Anlagenverbund wird hierbei eine aus mehreren separaten Anlagenteilen bestehende Gesamtanlage verstanden, welche über ein eigenes Leitungsnetz miteinander verbunden ist. Sollte diese Verbindung über öffentliche Vermittlungseinrichtungen geführt sein, so sind zusätzlich die unter M 5.15 Absicherung externer Remote Zugänge beschriebenen Maßnahmen zu realisieren. Bei Vernetzung über geschlossene Benutzergruppen innerhalb öffentlicher Netze oder über virtuelle private Netze (VPN) sollten die Maßnahmen für interne Remote Zugänge und nach Möglichkeit die mit * gekennzeichneten Punkte aus den Maßnahmen für externe Remote-Zugänge umgesetzt werden.
Der wichtigste Aspekt bei der Absicherung des internen Remote-Zugangesïst der, Eindringversuche aus externen Netzen wirksam zu unterbinden und gegebenenfalls auch erkennen zu können. Desweiteren sollen die Zugänge aus dem eigenen Netz auf die berechtigten Stellen und Personen eingeschränkt werden können. Je nach Art der Zugangstechnik existieren hierfür unterschiedliche Methoden.

Absicherung eines internen Remote-Zuganges via Modem
Die nachfolgende Abbildung stellt ein typisches Szenario eines internen Remote-Zugangs zu einem Fernadministrationsport via Modem dar. Die TK-Anlage PBX 1 wird vom Wartungsplatz aus direkt über die V.24-Wartungsschnittstelle administriert. Die TK-Anlage PBX 2 wird vom Wartungsplatz aus über Modem 1 - PBX 1 - PBX 2 - Modem 2 - V.24-Wartungsschnittstelle administiert.

In einem solchem Fall können folgende Maßnahmen zur Abschottung gegenüber Zugängen aus externen Netzen ergriffen werden:

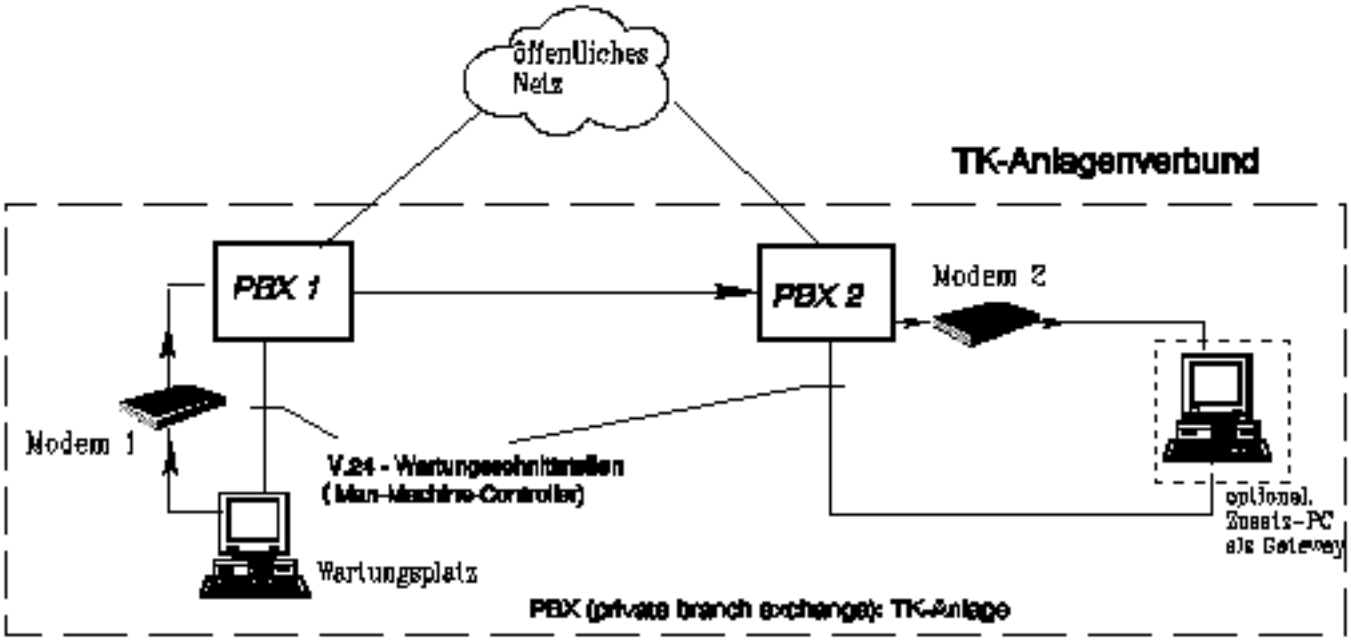

Abbildung H.3: Aufbau einer Fernadministration via Modem

- Keine Amtsberechtigung für den Modemanschluß
  Der Modemanschluß, über den der Zugang zum Administrationsport der Anlage geführt wird, sollte in jedem Fall nicht-amtsberechtigt sein! Diese Minimalanforderung sollte als erstes überprüft werden. Hiermit wird vermieden, daß das Modem von außerhalb direkt angewählt werden kann.

- Geheimhaltung der Rufnummer des Wartungsports (Modem)
  Um Mißbrauch von vornherein zu erschweren, sollte die Rufnummer des Wartungsapparates nicht in Telefonverzeichnissen veröffentlicht werden. Ihre Kenntnis sollte den sie unmittelbar benötigenden Personen vorbehalten bleiben.

- Verwendung von Standleitungen (optional)
  Die Verwendung von eigenen Standleitungen für die Remote-Verbindungen, die nicht über Vermittlungseinrichtungen geführt werden, ist eine der sichersten Methoden, einen externen Zugriff auf die Remote-Zugänge zu unterbinden. Da dieses Verfahren in der Regel sehr teuer ist, wird es nur in Ausnahmefällen Anwendung finden können. Um sicherzustellen, daß nur die berechtigten Stellen innerhalb des eigenen Netzes auf die Remote-Zugänge zugreifen können, müssen folgende Maßnahmen umgesetzt werden:

- Bildung geschlossener Benutzergruppen (Closed User Group, CUG)
  In einigen TK-Anlagen lassen sich auch anlagenübergreifend CUGs einrichten. Diese geschlossenen Benutzergruppen stellen eine Art Netz im Netz dar. Alle benötigten Remote-Zugänge sollten daher mit den jeweils zugangsberechtigten Stellen in solchen CUGs zusammengefaßt werden.

- Automatischer Rückruf (Callback)
  Die Callback-Option der Modems sollte genutzt werden (vgl. M 5.30 - Aktivierung einer vorhandenen Callback-Option). Wird ein PC-Gateway eingesetzt, so sollte das Callback von dort gestartet werden.

- Beschränkung der Rechte des Remote-Ports (optional)
  Sollte die TK-Anlage eine Rechteverwaltung für verschiedene Ports unterstützen, so kann diese genutzt werden, um sicherheitskritische Aktionen über Remote-Zugänge zu unterbinden und nur vor Ort zuzulassen. Viele TK-Anlagen besitzen diese Option jedoch nicht. In solchen Fällen können durch Zusatzprodukte, z.B. Portcontroller, die über einen Port ausführbahren Transaktionen beschränkt werden.

Um sicherzustellen, daß nur die berechtigten Personen innerhalb des eigenen Netzes auf die Remote-Zugänge zugreifen können, müssen folgende Maßnahmen umgesetzt werden:

- Identifikation und Authentisierung,

- Challenge-Response-Verfahren zur Authentikation (optional).

Absicherung eines internen Remote-Zugriffes via ISDN-Vernetzung
Aus Pratikabilitätsgründen bietet es sich teilweise an, die PCs mit Netzmanagementaufgaben mit ISDN-Karten auszurüsten. In einem solchen Fall sollte eine geschlossene Benutzergruppe gebildet werden. Hierzu kann die Rufnummer des rufenden Teilnehmers genutzt werden (Calling Line Identification and Presentation, CLIP). Dies könnte vom Endgerät selbst unter Zuhilfenahme der vom Netz zur Verfügung gestellten Rufnummer des anrufenden Gerätes (CLIP) realisiert werden.

Absicherung direkter Systemzugänge (Direct Inward System Access, DISA)
Direkte Systemzugänge sollten nach Möglichkeit gesperrt werden. Ist dies nicht möglich, so sollten die Berechtigungen so gesetzt werden, daß der direkte Systemzugang nur über einen dedizierten Port erfolgen kann. Auf diese Weise wird es möglich, den DISA-Zugang über ein Gateway zu führen. Ein Beispiel einer solchen Absicherung ist in der folgenden Abbildung dargestellt:

Einrichtung und Unterbringung eines Netzmanagementzentrums
Der Vorteil eines zentralen Netzmanagementes ist, neben einer komfortablen Abwicklungsmöglichkeit der Systemadministration, daß für die alltäglichen Administrationsarbeiten kein physikalischer Zutritt zu den TK-Anlagen mehr notwendig ist.
Sollte die Einrichtung eines zentralen Netzmanagementes erwogen werden, so ist dies in einem gesicherten Bereich unterzubringen. Der Zutritt zu diesem Zentrum ist durch organisatorische Maßnahmen zu regeln. Entsprechende Vorgaben können dem Kapitel 4.3.2 - Serverraum entnommen werden. Die Managementrechner, von welchem die Arbeiten durchgeführt werden können, sollten auch mit geeigneten Maßnahmen abgesichert werden. Beispiele finden sich in den Kapiteln 5.1 - DOS-PC (ein Benutzer) und 5.2 - Unix-System.

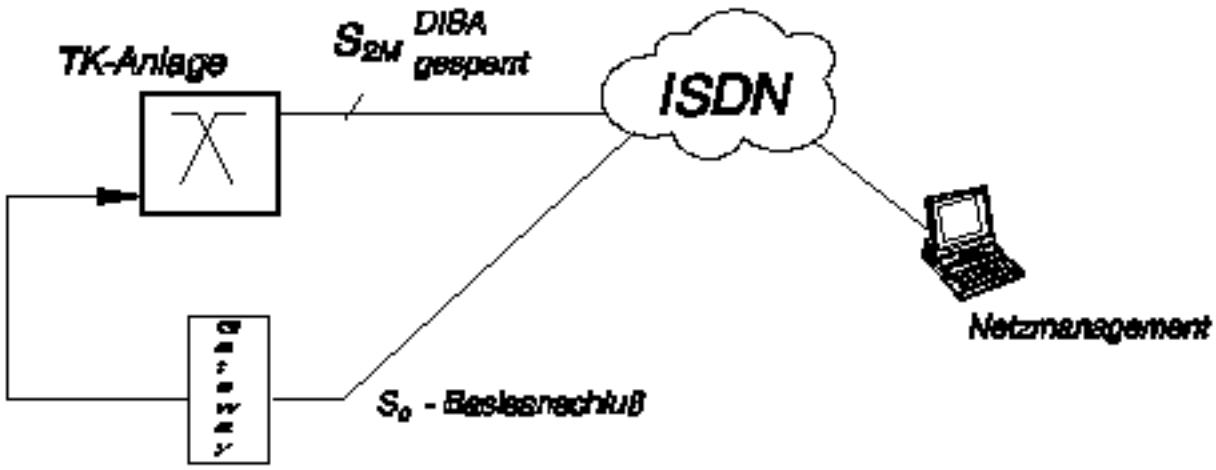

Abbildung H.4: Absicherung eines direkten Systemzuganges

Protokollierung von Wartungsmaßnahmen
Die momentane Anlagenkonfiguration, d.h. vergebene Rufnummern und Berechtigungen, aktivierte und deaktivierte Leistungsmerkmale, eingerichtete Heranholgruppen etc., muß jederzeit nachvollziehbar sein. Hierzu ist es notwendig, vorgenommene Veränderungen zu protokollieren. Eine elegante Methode ist die Zwangsprotokollierung mit Hilfe eines PC-Gateways.

M 5.15 Absicherung externer Remote-Zugänge
Als externer Remote-Zugang wird hierbei jeder Zugriff über den Wartungseingang der TK-Anlage via öffentliche Vermittlungssysteme angesehen. Dies kann entweder dadurch notwendig werden, daß die einzelnen Anlagen des Verbundes nicht oder nicht nur1) über Standleitungen verbunden sind oder daß auf eine schnelle Unterstützung des Herstellers in Notfällen nicht verzichtet werden kann. In diesen Fällen muß der Wartungsport (Modem) die volle Amtsberechtigung besitzen.
Die nachfolgende Abbildung stellt ein typisches Szenario eines externen Remote-Zugangs zur einem Fernadministrationsport via Modem dar. Die TK-Anlage wird vom externen Wartungsplatz aus über Modem 1 - öffentliches Netz - PBX 1 - Modem 2 - V.24-Wartungsschnittstelle administriert.

Aus Sicherheitsgründen ist es sinnvoll, auf externe Fernwartung zu verzichten. Ist dies nicht möglich, so sind - neben den Maßnahmen für interne Remote Zugänge - zusätzliche Sicherungsmaßnahmen unumgänglich.

PC-Gateway
Zwischen Wartungsport und Modem sollte ein PC-Gateway geschaltet werden. Dieser muß die folgenden Sicherheitsfunktionen realisieren:

- Identifikation und Authentisierung des Bedieners,

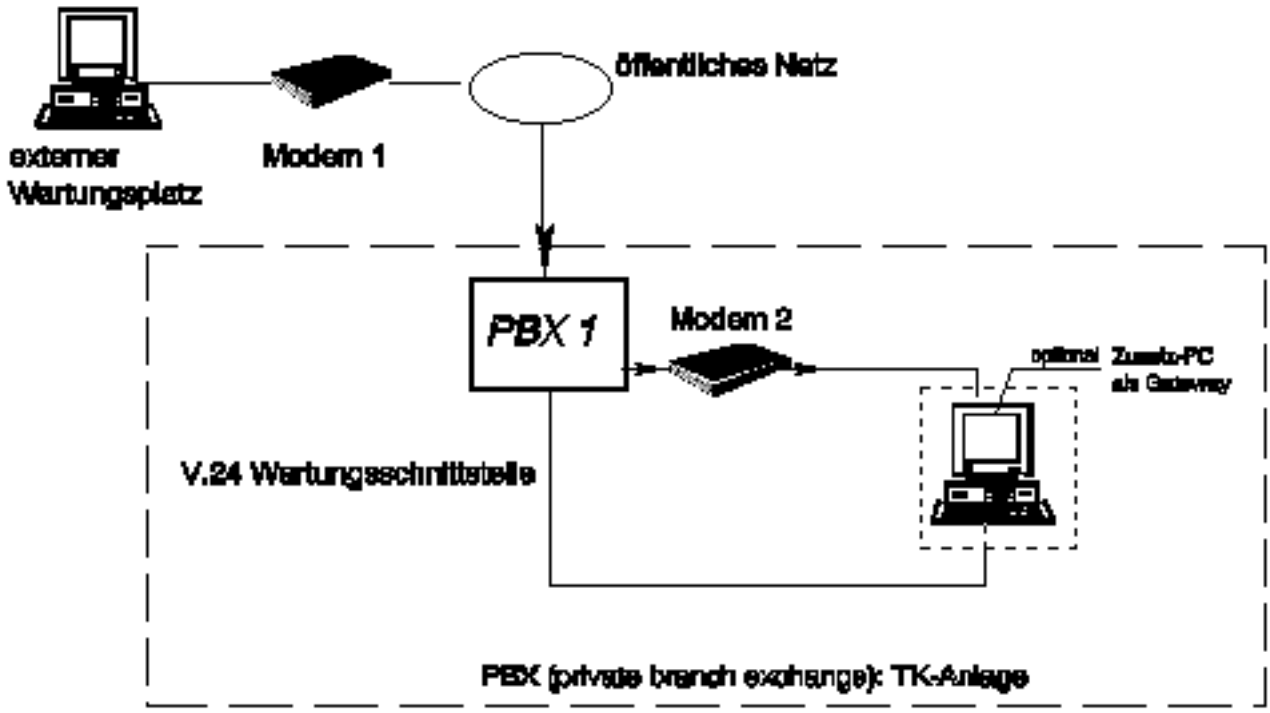

Abbildung H.5: Aufbau einer externen Fernadministration über Modem

- Abbruch der Verbindung bei sicherheitskritischen Ereignissen,
- Automatischer Rückruf (call back) und
- Protokollierung aller Tätigkeiten.

Darüber hinaus können noch weitere Funktionalitäten implementiert werden:

- Verhängen einer Zeitsperre bei fehlerhaften Zugangsversuchen,
- Sperren der Fernwartung im Normalbetrieb und explizite Freigabe für eine genau definierte Zeitspanne; dies ist sinnvoll, um in Notfall dem Hersteller oder einem anderen Wartungsunternehmen einen Eingriff zu ermöglichen,
- Einschränkung der Rechte des Wartungspersonals; über eine auf dem Wartungs-PC installierte Zusatzsoftware kann der Benutzer in seinem Handlungsspielraum eingeengt werden, um eine abgestufte Rechteverwaltung zu realisieren,
- SZwangslogout"bei Leitungsunterbrechung; wird die Verbindung zwischen Fernwartungsstelle und PC-Gateway auf irgendeine Weise unterbrochen, so muß der Zugriff auf das System durch ein SZwangslogout"beendet werden.

Physikalische Abschaltung des Fernwartungszuganges
Sollte im Normalfall keine Fernwartung benötigt und nur im Bedarfsfall eine solche ermöglicht

werden, so empfiehlt sich die physikalische Abschaltung des Zuganges. Im Bedarfsfall kann dieser, eventuell nach telefonischer Rücksprache mit dem Hersteller oder der Wartungsfirma, kurzfristig aktiviert werden.

Geschlossene Benutzergruppen (Closed User Group, CUG)
In öffentlichen ISDN- und X.25-Netzen wird das Leistungsmerkmal der Bildung von CUG angeboten. Auf diese Weise wird für einen Benutzer vom Netzbetreiber ein virtuelles Netz-im-Netzßur Verfügung gestellt. Die geschlossenen Benutzergruppen können beim Netzbetreiber gegen entsprechende Entgelte beantragt werden.
Alternativ kann überlegt werden, die geschlossenen Benutzergruppen durch Nutzung der ISDN-Hilfsdienste Calling Line Identification and Presentation (CLIP) und Connected Line Identification and Presentation (COLP) selbst zu realisieren. Dies kann, wenn möglich, durch entsprechende Konfiguration der eigenen TK-Anlage oder aber durch entsprechende Auslegung eines PC-Gateways geschehen.

Vermeidung bzw. Kontrolle direkter Einwahlmöglichkeiten (Dial-In)
Eine direkte Einwahlmöglichkeit, z.B. aus anderen Netzen über Nachwahl im Mehrfrequenzwahlverfahren, in die TK-Anlage sollte nach Möglichkeit unterbunden werden. Solche Verfahren werden oft für den Zugang zu Serverdiensten genutzt. Sollte ein Unterbinden aus betrieblichen Gründen nicht vermeidbar sein, so empfiehlt sich das vollständige Aktivieren der möglichen Schutzmechanismen und eine regelmäßige Kontrolle auf möglichen Mißbrauch.

M 5.16 Übersicht über Netzdienste

Bevor unter Unix mit der Sicherheitsüberprüfung einzelner Netzdienste und -prozesse begonnen wird, sollte zunächst eine Übersicht darüber erstellt werden, welche Dienste überhaupt zur Verfügung gestellt werden müssen und welche Dienste u. U. schon installiert sind. Für letzteres ist es hilfreich, mit Hilfe des Befehls ps und entsprechenden Optionen eine Liste aller Netzprozesse zu erzeugen. Dann sollte man sich über die Aufgabe von jedem dieser Prozesse und darüber, wo er mit welchen Optionen gestartet wird, informieren. Häufig geschieht dies in den Dateien /etc/rc, /etc/rc.net, /etc/rc.local, die beim Booten des Systems gelesen werden.
Besonders wichtig ist der inetd-Daemon, da dieser alle Prozesse, die in der Datei /etc/inetd.conf aufgeführt sind, starten kann. Auch Konfigurationsdateien wie /etc/services, /etc/protocols, /etc/hosts, /etc/gated.conf und andere müssen überprüft werden.

M 5.17 Einsatz der Sicherheitsmechanismen von NFS

NFS (Network File System) erlaubt die gemeinsame Benutzung von Dateien auf einem Server von allen Rechnern (Clients) aus, die im selben Netz eingebunden sind und auf dem Server die Rechte dazu bekommen haben. Jeder Server läßt sich auch als Client betreiben und umgekehrt, so daß sichergestellt werden muß, daß jeder Rechner nur mit der für ihn vorgesehenen Funktionalität arbeitet. So ist es z. B. unnötig, den Mount-Daemon mountd oder den NFS-Daemon nfsd auf einem NFS-Client zu starten.

- Auf einem NFS-Server muß in einer Datei (z. B. /etc/exports oder /etc/dfs/dfstab) jedes Dateisystem bzw. Verzeichnis eingetragen werden, das von anderen Rechnern gemountet

werden können soll. Für sie muß folgendes gelten:

- Es sollten nur Dateisysteme exportiert werden, die unbedingt notwendig sind.
- Mit den Schlüsselwörtern root= und access= lassen sich die Rechner genau spezifizieren, für die Dateisysteme zum Export freigegeben werden sollen. Fehlt die Angabe spezieller Rechner, so ist das Dateisystem für alle Rechner freigegeben, was auf keinen Fall geschehen darf!
- Für Dateisysteme, die nur gelesen werden sollen, und hierzu gehören alle ausführbaren Dateien, sollte die Option ro (read only) benutzt werden.
- Normalerweise wird die Benutzernummer de Systemadministrators (UID 0) bei NFS-Anfragen auf die Nummer des Benutzers nobody (UID -2 bzw. 65534) umgesetzt, so daß auf Dateien mit der UID 0 über NFS nicht zugegriffen werden kann. Dies gilt nicht für Dateien, die anderen privilegierten Benutzern gehören, wie z.B. bin oder daemon, was auch in Zusammenhang mit der Aufteilung der Administrationstätigkeiten (M 2.32 - Einrichtung einer eingeschränkten Benutzerumgebung) bedacht werden muß, d.h. Dateisysteme mit Dateien dieser Benutzer dürfen nicht exportiert werden. Da jeder Rechner im Netz jede IP annehmen kann und z.B. jeder PC-Benutzer unter DOS root-Privilegien hat, sollte also die Umsetzung von root auf nobody nicht abgeschaltet werden, und es sollte sichergestellt werden, daß ein Eintrag $nobody : * : -2 : -2 : anonymoususer ::$ in der /etc/passwd existiert und wirksam ist. In diesem Zusammenhang muß auch beachtet werden, daß jeder Benutzer, der auf einem Netzrechner root-Privilegien hat (z.B. als PC-Benutzer) über NFS auch jede Gruppenkennung annehmen kann, so daß also kein exportiertes Verzeichnis und keine exportierte Datei Gruppenschreibrechte besitzen sollte und Lese- und Ausführungsrechte nur, soweit dies unumgänglich ist. Außerdem sollte beachtet werden, daß nicht nur einzelne Dateien, sondern alle darüberliegenden Verzeichnisse geschützt werden müssen!
- Die Option anon=-1 sollte benutzt werden, damit anonyme Anfragen verhindert werden. anon=0 (root) sollte niemals benutzt werden, da hierdurch jedem Benutzer Dateizugriffe mit root-Rechten möglich werden.
- In Dateien wie z.B. /etc/fstab oder /etc/vfstab sind die Dateisysteme eingetragen, die durch einen Befehl wie z.B. mount -a oder mountall gemountet werden können. Dies kann u.U. auch ohne Rückfrage beim Booten geschehen. Diese Datei muß deshalb rechtzeitig auf Korrektheit überprüft werden.
- /etc/exports und /etc/fstab (bzw. analoge Dateien auf anderen Systemen) sind Systemdateien, auf die nur der Systemadministrator Zugriff haben darf.
- Zu exportierende Dateisysteme sollten auf einer separaten Platte oder Partition eingerichtet werden, damit z.B. das unbefugte Vollschreiben der Systemplatte durch einenBenutzer von einem anderen Rechner aus verhindert wird.

- Beim Mounten exportierter Dateisysteme muß die Option nosuid benutzt werden, um die Ausführung von suid-Programmen auf dem Client zu verhindern.
- Wenn möglich, sollte der NFS-Daemon so konfiguriert werden, daß er automatisch eine Überprüfung der Portnummern durchführt, um sicherzustellen, daß Pakete nur von den privilegierten Ports 0 - 1023 akzeptiert werden.
- Zur Kennzeichnung von Dateien werden zwischen Client und Server sogenannte File-Handles benutzt, die sic sehr leicht erraten lassen. Sie sollten deshalb mit Hilfe des Programms fsirand randomisiert werden.
- Wenn vorhanden, sollte SECURE-NFS benutzt werden, so daß die Daten verschlüsselt übertragen werden. Dabei sind folgende Schritte wichtig:
- Erzeugung von Schlüsseln für alle NFS-Benutzer,
- Löschen des public key für den Benutzer nobody,
- auf dem NIS-Masterserver darf rpc.ypupdated nicht laufen,
- Übertragung der public key map auf alle Rechner, bevor SECURE-NFS gestartet wird,
- Benutzung von keylogin und keylogout zur Erzeugung von private keys beim Ein- und Ausloggen,
- auf jedem Client muß der keyserv-Daemon laufen,
- beim Mounten muß die Option secure benutzt werden,
- die Uhren auf allen Rechnern müssen synchronisiert werden, da die übertragenen Pakete mit Zeitmarken versehen werden, um das Wiedereinspielen von Nachrichten zu verhindern.

M 5.18 Einsatz der Sicherheitsmechanismen von NIS

NIS (Network Information Service) läßt sich nicht ohne schwerwiegende Sicherheitslücken betreiben und sollte deshalb nur in einer sicheren Umgebung eingesetzt werden.
Für einen NIS-Server gilt folgendes:

- In der Paßwortdatei /etc/passwd darf der Eintrag +::0:0::: nicht enthalten sein, da sonst ein Zugang mit dem Namen ´+´ ohne Paßwort existiert. Sollte der Eintrag notwendig sein, muß das Paßwort durch ein ´*´ ersetzt werden (überprüfen, ob der Zugang wirklich gesperrt ist !). Trotzdem bleibt die Gefahr, daß bei einer versehentlichen Löschung der ersten Spalte (das ´+´) ein privilegierter Zugang ohne Paßwort und ohne Benutzername möglich ist!
- Analoges gilt für die Gruppendatei /etc/group und alle anderen sicherheitsrelevanten Dateien, die über NIS netzweit zugänglich gemacht werden sollen, wie z. B. /etc/hosts, /etc/group oder /etc/bootparams.

- Der Server-Prozeß ypserv sollte nur Anfragen von vorher festgelegten Rechnern beantworten.

Für einen NIS-Client gilt folgendes:

- Der Eintrag +:*:0:0::: in der Paßwortdatei /etc/passwd sollte dokumentiert werden (siehe M 2.31 - Dokumentation der zugelassenen Benutzer und Rechteprofile), und es muß auf jeden Fall ein Eintrag im Paßwortfeld vorhanden sein, damit nicht im Falle einer (beabsichtigten oder nicht beabsichtigten) Nichtbenutzung von NIS versehentlich ein Zugang mit dem Benutzernamen ´+´ ohne Paßwort geschaffen wird.

- Analoges gilt für die Gruppendatei /etc/group und alle anderen sicherheitsrelevanten Dateien, die über NIS netzweit zugänglich gemacht werden sollen.

- Der Client-Prozeß ypbind sollte nur Daten akzeptieren, die von einem privilegierten Port kommen, da ansonsten er Daten (auch Paßwörter !) von jedem beliebigen Prozeß, der sich als Server ausgibt, bekommen könnte.

- Um zu verhindern, daß der NIS-Administrator auf allen NIS-Clients root-Rechte hat, sollte auf jedem NIS-Client ein lokaler Benutzer mit der UID 0 eingerichtet werden.

- Es muß beachtet werden, daß NIS zunächst die lokalen Dateien nach passenden Einträgen absucht, so daß z.B. die Einträge root::0:0:::
  +:*:0:0:::
  in der /etc/passwd dazu führen, daß nicht das root-Paßwort aus der NIS-Map benutzt wird, sondern der erste Eintrag ohne Paßwort.

M 5.19 Einsatz der Sicherheitsmechanismen von sendmail

Da die Übertragung von Mails die wohl am meisten verbreitete Anwendung in Netzen ist, sind die dafür zuständigen Prozesse von besonderer Bedeutung und einer der häufigsten Angriffspunkte in einem System. Hinzu kommt, daß diese Prozesse häufig das suid-Bit gesetzt haben und einem privilegierten Benutzer gehören (z.B. root oder bin). Ein Fehler in sendmail war z.B. einer der Wege, über die sich der Internet-Wurm ausgebreitet hat.

- Beim Starten von sendmail lassen sich sehr viele Optionen angeben, die zu Sicherheitsproblemen führen würden, wenn sie mit root-Rechten abliefen. Wenn sendmail von beliebigen Benutzern aufgerufen werden kann, sollte deshalb überprüft werden, ob es beim Start mit einer dieser Optionen das gesetzte suid-Bit ignoriert und mit der UID des Benutzers abläuft. Um Sicherheitsprobleme zu vermeiden, sollte der Administrator sicherstellen, daß sendmail nur mit den folgenden Optionen bei gesetztem suid-root-Bit von unprivilegierten Benutzern gestartet werden kann: 7, b, C, d, e, E, i, j, L, m, o, p, r, s und v.

- Aufgrund der in der Vergangenheit aufgedeckten Sicherheitsdefizite des Programms sendmail muß stets die aktuellste Programmversion eingesetzt werden. Informationen über die aktuellen Versionen erteilen die in M 2.35 - Informationsbeschaffung über Sicherheitslücken des Systems angegebenen Stellen wie BSI, CERT, DFN-CERT.

- Der sendmail-Prozeß darf nicht im Debug-Modus betrieben werden können, da es sonst möglich wird, root-Rechte zu erlangen. Man kann dies testen, indem man den Befehl
  telnet localhost 25
  eingibt, wobei localhost der zu überprüfende Rechnername sein kann und 25 die Portnummer, mit der der sendmail-Prozeß angesprochen wird. Der Rechner bzw. der sendmail-Prozeß meldet sich dann mit

  Trying 123.45.67.8...
  Connected to xxx.yy.de.
  Escape character is '^]'.
  220 xxx Sendmail 4.1/SMI-4.1 ready at Wed, 13 Apr 94 10:04:43 +0200

  Wenn Sie nun den Befehl debug, showq oder bei sehr alten Versionen wizard eingeben, sollte dies der Prozeß mit

  500 Command unrecognized

  ablehnen. Sie können dann mit dem Befehl quit die Verbindung wieder beenden.

- Die Befehle vrfy und expn dürfen nicht verfügbar sein, da sie zu einem Mailnamen den zugehörigen Login-Namen ausgeben, so daß sich dann durch Probieren evtl. das zugehörige Paßwort herausfinden läßt. Bei Version 8 von sendmail lassen sich diese Befehle z.B. durch die Option p (privacy) beim Starten abschalten. Ob diese Befehle verfügbar sind, läßt sich wie im vorigen Punkt beschrieben feststellen, also z.B. durch Eingabe des Befehl vrfy useralias.

- Die Konfigurationsdatei sendmail.cf sollte root gehören und auch nur für root les- und schreibbar sein. Dasselbe gilt für die darüber stehenden Verzeichnisse, da sich sonst durch ein einfaches Umbenennen dieser Verzeichnisse eine neue sendmail.cf Datei erzeugen läßt.

- Die Angabe von ausführbaren Programmen oder von Dateien als gültige Adressen für Empfänger oder Absender muß durch die Konfiguration von sendmail.cf verhindert werden oder durch geeignete Maßnahmen auf bestimmte, unbedenkliche Programme und Dateien eingeschränkt werden.

- Das F-Kommando (also z.B. FX/path [^#]), mit dessen Hilfe Klassen definiert werden, sollte in der Konfigurationsdatei (sendmail.cf) nur benutzt werden, um Dateien zu lesen, die sowieso systemweit lesbar sind, da es sonst möglich sein kann, daß sicherheitsrelevante Informationen aus geschützten Dateien frei verfügbar werden. Die Programmform des F-Kommandos (z.B. FX|/tmp/prg) sollte nicht benutzt werden!

- Bei der Definition des Delivery Agents (z.B. Mlocal) dürfen nur absolute Pfade angegeben werden (z.B. P=/bin/mail). Außerdem sollte das Flag S (suid) nur gesetzt werden, wenn die damit evtl. verbundenen Sicherheitsprobleme geklärt sind.

- Jede Datei, in die sendmail schreiben könnte, wie z.B. sendmail.st für eine Statistik, sollte nur von root beschreibbar sein und auch nur in root gehörenden Verzeichnissen stehen. Dasselbe gilt für Dateien, die von sendmail ausgewertet werden wie z.B. :include: in Mailing Listen.

- Privilegierte Benutzer wie bin oder root sollten keine .forward Datei besitzen. Sind nämlich die Benutzer- oder Gruppenschreibrechte für diese Datei falsch gesetzt oder gelingt es einem Benutzer, in eine privilegierte Gruppe zu gelangen, kann er sich eine Shell mit der privilegierten Benutzerkennung erzeugen.
  Für normale Benutzer sollte die .forward-Datei nur von dem Besitzer beschreibbar sein und muß sich in einem Verzeichnis befinden, das dem Besitzer gehört.
  Falls ein Heimatverzeichnis systemweit beschreibbar sein muß, wie z.B. uucp, läßt sich auf folgende Weise verhindern, daß eine schädliche .forward-Datei angelegt werden kann: Es muß ein Verzeichnis mit dem Namen .forward, den Rechten 000 und dem Besitzer root angelegt werden und in diesem eine Datei ebenfalls mit den Rechten 000 und dem Besitzer root, so daß niemand außer root diese Datei verändern oder löschen kann. Das Homedirectory von uucp sollte dann ebenfalls root gehören und mit dem Sticky-Bit (t) versehen sein. Eine analoge Vorgehensweise empfiehlt sich auch für andere Konfigurationsdateien (z.B. .login, .cshrc) in systemweit beschreibbaren Verzeichnissen.

- Aus der Alias-Datei sollte jedes ausführbare Programm entfernt werden, insbesondere auch uudecode. Außerdem sollte die Alias-Datei und die zugehörige Datenbank root gehören und auch nur für root beschreibbar sein.

- Es muß beachtet werden, daß jede empfangene Mail verfälscht sein kann. Dies kann entweder in der Mailqueue geschehen oder durch ein Einloggen auf Port 25. Ersteres läßt sich vermeiden, wenn das Mailqueue-Verzeichnis root gehört und die Rechte 0700 besitzt. Die Queue-Dateien sollten die Berechtigung 0600 haben. Die Veränderung einer Mail während ihres Transportes läßt sich nicht vermeiden, so daß die Benutzer darüber aufgeklärt werden müssen, daß z.B. eine Mail von root, in der sie dazu aufgefordert werden, ihr Paßwort zu ändern, gefälscht sein kann.

M 5.20 Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp

Mit dem Programm rlogin bzw. dem zugehörigen Daemon rlogind ist es möglich, sich über eine Netzverbindung auf einem anderen Rechner einzuloggen, wobei allerdings nur das Paßwort abgefragt wird, da der Benutzername direkt übergeben wird. Mit den Kommandos rsh bzw. rcp und dem Daemon rshd ist es möglich, auf einem anderen Rechner ein Kommando ausführen zu lassen. Für beide Befehle gibt es die Möglichkeit, Trusted-Hosts zu definieren und zwar entweder benutzerspezifisch im Heimatverzeichnis in der Datei $HOME/.rhosts oder systemweit in der Datei /etc/hosts.equiv. Jeder Rechner, der in einer dieser Dateien eingetragen ist, wird als vertrauenswürdig angesehen, so daß ein Einloggen (mit rlogin) bzw. die Ausführung eines Befehles (mit rsh) von ihm aus ohne Angabe eines Paßwortes möglich ist. Da es, insbesondere von einem PC aus, sehr leicht ist, jeden beliebigen Rechnernamen vorzutäuschen, muß

sichergestellt werden, daß die Dateien $HOME/.rhosts und /etc/hosts.equiv nicht vorhanden sind oder daß sie leer sind und der Benutzer keine Zugriffsrechte auf sie hat. Hierzu sollten regelmäßig die Heimatverzeichnisse der Benutzer untersucht werden, oder es sollte verhindert werden, daß die Daemons rlogind und rshd gestartet werden können (siehe hierzu die Datei /etc/inetd.conf und Maßnahme M 5.16 - Übersicht über Netzdienste). Sollte die Benutzung der Datei /etc/hosts.equiv unumgänglich sein, muß sichergestellt sein, daß kein Eintrag '+' vorhanden ist, da hierdurch jeder Rechner vertrauenswürdig würde.

M 5.21 Sicherer Einsatz von telnet, ftp, tftp und rexec

Das Kommando telnet hostname ermöglicht es, sich nach Eingabe eines Benutzernamens und des zugehörigen Paßwortes auf dem Rechner hostname einzuloggen. Mit ftp ist es möglich, größere Datenmengen zu kopieren, und rexec erlaubt die Ausführung von Kommandos auf einem anderen Rechner ohne ein vorhergehendes Anmelden. Bei allen drei Programmen werden die eingegebenen Benutzernamen und Paßwörter unverschlüsselt über das Netz übertragen, so daß sie nur benutzt werden dürfen, wenn sichergestellt ist, daß das Netz nicht abgehört werden kann (siehe G 5.7). Alle Aufrufe von sind telnet, ftp und rexec zu protokollieren. Insbesondere ist auf fehlgeschlagene Verbindungsversuche von externen IT-Systemen zu achten.
Beim Einsatz des Daemons ftpd muß beachtet werden, daß ähnlich wie bei sendmail (siehe M 5.19 - Einsatz der Sicherheitsmechanismen von sendmail) immer wieder neue schwerwiegende Sicherheitslücken festgestellt werden, die es u.U. ermöglichen, ohne Paßwort Administratorrechte zu bekommen (siehe hierzu die CERT-Mitteilung 94-08 vom 14.4.94). Es sollten keine ftp-Versionen eingesetzt werden, die älter sind als die dort beschriebenen.
Weiterhin sollten in die Datei /etc/ftpusers alle Benutzernamen eingetragen werden, für die ein ftp-Zugang nicht erlaubt werden soll. Hierzu gehören z.B. root, uucp und bin. Bei der Einrichtung von neuen Benutzern ist darauf zu achten, diese in /etc/ftpusers einzutragen, wenn sie gemäß ihrem Rechteprofil keinen ftp-Zugang haben dürfen (siehe auch M 2.30 - Regelung für die Einrichtung von Benutzern / Benutzergruppen).
Mit Hilfe von .netrc-Dateien werden automatische FTP-Zugriffe auf entfernten IT-Systemen erlaubt.
Es muß sichergestellt werden, daß keine .netrc-Dateien vorhanden sind oder daß sie leer sind und der Benutzer keine Zugriffsrechte auf diese hat. Der Einsatz des Daemons tftpd, rexd und rexecd muß verhindert werden (z.B. durch Entfernen des entsprechenden Eintrags in der Datei /etc/inetd.conf), oder es muß zumindest sichergestellt sein, daß beim Einsatz von tftp den Benutzern aus dem Login-Verzeichnis nur eingeschränkte Dateizugriffe möglich sind (siehe auch M 2.32 - Einrichtung einer eingeschränkten Benutzerumgebung). Dies läßt sich überprüfen, indem man folgendes eingibt: tftp hostname
tftp>get /etc/passwd /tmp/txt
Meldet sich der tftp-Daemon nicht mit einer Fehlermeldung, muß seine Benutzung verhindert werden.

M 5.22 Kompatibilitätsprüfung des Sender- und Empfängersystems

Abhängig vom Grad der Kompatibilität von Empfänger- und Sendersystem lassen sich Informationen mehr oder weniger zuverlässig per Datenträgeraustausch übertragen. Dabei sind je

nach Komplexität auszutauschender Daten unterschiedliche Anforderungen an die Kompatibilität zu stellen. Vor Einrichtung eines regelmäßigen Datenträgeraustausches sollte daher die Übereinstimmung folgender Eigenschaften überprüft werden, um im Vorfeld Inkompatibilitäten festzustellen und ggf. Abhilfe zu schaffen:

- Physikalisches Lesemedium:
  Notwendige Voraussetzung ist die Übereinstimmung der physikalischen Lesemedien von Empfänger- und Sendersystem. Dabei reicht aber mechanische Äquivalenz noch nicht aus, denn die Nichtübereinstimmung von Parametern wie Geschwindigkeit bei Bändern oder Kapazität bei Disketten kann zu Problemen führen.

- Zeichencode (z.B. ASCII oder EBCDIC):
  Stimmen Sender- und Empfängersystem im verwendeten Zeichencode überein, so sind mit Hilfe des physikalischen Lesens einzelne Sektoren/Blöcke im Klartext lesbar, die unzusammenhängend auf dem Datenträger verteilt sein können. Stimmen die verwendeten Zeichencodes nicht überein, werden die übertragenen Daten falsch interpretiert.

- Formatierung des Betriebs- bzw. Dateisystem des Datenträgers:
  Verfügen beide Systeme darüber hinaus über das gleiche Betriebs- und Dateisystem oder sieht das Empfängerbetriebssystem vor, Formatierungen anderer Betriebssystem zu lesen (einige Unix-Betriebssysteme können DOS-Disketten einlesen), dann können alle Dateien, wie sie beim Absender vorlagen, wiederhergestellt werden. Dies ist für Informationen ausreichend, die keiner weiteren Formatierung, wie sie von den meisten Anwendungsprogrammen (z.B. Textverarbeitungsprogrammen) vorgenommen werden, unterliegen.

- Anwendungssoftware:
  Wurden Anwendungsprogramme zur Erzeugung der zu übermittelten Dateien verwendet, ist auf Versionsgleichheit dieser Programme zu achten, da die Dateiformate evtl. unterschiedlich sein können. Die Versionsgleichheit muß nicht bestehen, wenn die Programmversionen aufwärts- bzw. abwärtskompatibel sind.

- IT-Sicherheitssoftware und IT-Sicherheitsparameter:
  Werden darüber hinaus IT-Sicherheitsprodukte oder Schutzmechanismen bestimmter Anwendungsprogramme (siehe M 4.30 - Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen) verwendet, so ist die Kompatibilität dieser Produkte sicherzustellen. Über die verwendeten Schlüssel oder Paßworte müssen sich Absender und Empfänger auf geeignetem Wege verständigen.

Treten Inkompatibilitäten auf, so sind zusätzliche Vorkehrungen bzw. Produkte bereitzustellen, die eine entsprechende Konvertierung vorsehen, oder die Absender- und Empfängersysteme sind identisch auszustatten.

M 5.23 Auswahl einer geeigneten Versandart für den Datenträger

Neben den in M 2.3 - Datenträgerverwaltung dargestellten Umsetzungshinweisen sollte sich die Versandart der Datenträger am Gefährdungspotential orientieren. Hinsichtlich Verfügbarkeit

ist die Versandart derart auszuwählen, daß eine rechtzeitige Zustellung garantiert werden kann. Je mehr Personen mit der Beförderung befaßt und je länger die Zeiten sind, in denen der Datenträger unbeaufsichtigt bleibt, desto weniger kann im allgemeinen die Vertraulichkeit und Integrität garantiert werden. Dementsprechend sind angemessene Versandarten auszuwählen. Man kann dabei z.B. zwischen folgenden Versandarten wählen:

- Deutsche Post AG,
- Deutsche Bahn AG,
- Kurierdienste,
- persönlicher Kurier und
- persönliche Übergabe.

M 5.24 Nutzung eines geeigneten Fax-Vorblattes
Um einen geordneten und nachvollziehbaren Fax-Austausch zu erzielen, ist die Nutzung eines standardisierten Fax-Vorblattes vorzusehen. Damit kann insbesondere geprüft werden, ob eine erhaltene Fax-Sendung vollständig empfangen und ausgedruckt wurde.
Das Fax-Vorblatt sollte beinhalten:

- Rufnummer des Fax-Gerätes,
- Name des Absenders (mit Telefonnummer und vollständiger Adresse),
- Telefonnummer eines Ansprechpartners bei Übertragungsproblemen,
- Name des Empfängers (mit Rufnummer des Fax-Gerätes und ggf. vollständiger Adresse),
- Seitenzahl einschließlich Fax-Vorblatt,
- ggf. Dringlichkeitsvermerk (evtl. gestuft) und
- Unterschrift des Absenders.

Die Bitte, fehlgeleitete Sendungen weiterzuleiten oder den Absender zu informieren, ist sinnvoll.

M 5.25 Nutzung von Sende- und Empfangsprotokollen
Listenmäßige Protokolle von Übertragungsvorgängen, die automatisch vom Fax-Gerät geführt werden (Kommunikationsjournal), sind regelmäßig auszudrucken. Es bedarf einer Festlegung, wer diese Ausdrucke veranlaßt, wo und wie lange sie aufbewahrt werden und in welcher Weise sie stichprobenartigen Prüfungen auf Unregelmäßigkeiten unterzogen werden. Auf die Erfordernisse des BDSG ist Rücksicht zu nehmen. Insbesondere ist der Zugriff Unbefugter zu verhindern. Es sollte zusätzlich ein Fax-Tagebuch geführt werden, aus dem ersichtlich wird, wer wann ein Fax an wen versandt hat. Optional kann darüber hinaus ein Fax-Eingangsbuch geführt werden. Es sei darauf hingewiesen, daß eine weitere Kontrollmöglichkeit besteht, wenn das Fax-Gerät an

eine moderne TK-Anlage angeschlossen ist. Dann ist es u.U. möglich, die Gebührendatensätze der Fax-Rufnummer in der TK-Anlage auszuwerten (vgl. auch M 2.40 - Rechtzeitige Beteiligung des Personal- / Betriebsrates).

M 5.26 Telefonische Ankündigung einer Fax-Sendung
Wichtige Fax-Sendungen mit vertraulichen oder finanzwirksamen Inhalten (z.B. Angebote) oder termingebundene Fax-Sendungen sollten vor Absendung beim Empfänger (zum Beispiel per Telefon) angemeldet werden. Der Empfänger hat dann die Möglichkeit, zum entsprechenden Fax-Gerät zu gehen und dort das für ihn eingehende Fax direkt entgegenzunehmen, so daß kein anderer das Fax entnehmen kann.
Die Benutzer sollten von Vorgesetzten angewiesen werden, vertrauliche oder wichtige Fax-Sendungen anzukündigen.

M 5.27 Telefonische Rückversicherung über korrekten Fax-Empfang
Bei wichtigen Fax-Sendungen sollte beim Empfänger nachgefragt werden, ob die Fax-Sendung vollständig empfangen, ausgedruckt und ihm übergeben wurde. Die Mitarbeiter sollten hierzu angewiesen werden. Die telefonische Bestätigung kann auch auf dem Fax-Vordruck erbeten werden.
Hilfreich sind in diesem Zusammenhang die von einigen Fax-Geräten als Leistungsmerkmal angebotenen Einzelsendeberichte, die Fehler beim Versand anzeigen können.

M 5.28 Telefonische Rückversicherung über korrekten Fax-Absender
Bei wichtigen oder ungewöhnlichen Fax-Sendungen sollte in Erwägung gezogen werden, sich beim Fax-Absender zu vergewissern, daß das Fax von ihm abgesandt und nicht von einem Dritten gefälscht wurde. Dies kann auf einfache Weise durch einen telefonischen Rückruf erfolgen. Die erforderliche Rufnummer ist i. allg. auf dem Fax-Vorblatt dokumentiert, sollte aber, da sie gefälscht sein könnte, verifiziert werden.

M 5.29 Gelegentliche Kontrolle programmierter Zieladressen und Protokolle
Bei programmierbaren Kurzwahltasten oder Zieladressenspeicherung sollte gelegentlich überprüft werden, ob die gewünschte mit der einprogrammierten Fax-Nummer übereinstimmt und ob sie noch benötigt wird. Damit wird verhindert, daß eine von einem Unberechtigten eingegebene fremde Fax-Nummer längere Zeit statt der korrekten Nummer genutzt wird. Außerdem werden eventuell übersehene Änderungen der gewünschten Zielrufnummern frühzeitig entdeckt.

M 5.30 Aktivierung einer vorhandenen Callback-Option
Viele Modems bieten die Option automatischer Rückruf (Callback). Ist diese Option aktiviert, trennt das Modem, wenn es einen Anruf erhält, sofort nach dem erfolgreichen Verbindungsaufbau die Leitung und ruft eine voreingestellte Nummer zurück. Dadurch wird verhindert, daß ein nicht autorisierter Anrufer diesen Modemzugang mißbrauchen kann, solange er nicht unter der voreingestellten Nummer erreichbar ist. Callback ist immer dann einzusetzen, wenn ein fester Kommunikationspartner sich automatisch einwählen können soll. Zu beachten ist, daß mit dem automatischen Rückruf auch die Kosten der Datenübertragung übernommen werden.

Das erforderliche Kommando ist der Bedienungsanleitung zu entnehmen, üblicherweise wird das Kommando AT%S benutzt. Vor der Aktivierung der Callback-Option ist festzulegen, welche Nummer zurückgerufen werden soll.
Manche Modems bieten auch die Möglichkeit, einen automatischen Rückruf mit einer Paßwortabfrage zu verbinden. Das angerufene Modem fordert dabei nach dem Verbindungsaufbau das anrufende Modem zu einer Paßworteingabe auf. Im angerufenen Modem wird die Gültigkeit des Paßwortes überprüft. Jedem gültigen Paßwort ist eine Rufnummer zugeordnet, die dann zurückgerufen wird. Dabei kann meist eine Liste von Rückrufnummern im lokalen Modem angelegt werden, so daß von verschiedenen Orten aus Verbindung mit dem lokalen Modem aufgebaut werden kann.
Es ist darauf zu achten, daß der automatische Rückruf nur auf einer Seite aktiviert ist, da der Mechanismus sonst in eine Endlosschleife führt. Callback sollte auf der passiven Seite aktiviert sein, also auf der Seite, von der Dateien abgerufen oder auf der Dateien eingespielt werden. Ein typisches Beispiel ist der Außendienstmitarbeiter, der mit einem IT-System in seiner Organisation in Verbindung treten will. Hier muß Callback auf dem organisationsinternen Modem aktiviert sein.
Es sollte sichergestellt sein, daß die voreingestellten Rufnummern des Callback sporadisch kontrolliert und aktualisiert werden. Ein Callback kann außer durch das Modem auch von der Applikation ausgelöst werden. Wenn die eingesetzte Applikation diese Option bietet, sollte das Callback von der Applikation und nicht vom Modem ausgelöst werden. Wenn das Modem ein Callback auslöst, kann ein Angreifer versuchen, in dem Moment, wenn das Modem den Callback starten will, dieses anzuwählen und damit den Callback abzufangen. Wenn die Applikation den Callback durchführt, ist es für einen Angreifer wesentlich schwieriger, den richtigen Moment abzupassen.

M 5.31 Geeignete Modem-Konfiguration

Die meisten Modems arbeiten nach dem Hayes-Standard (auch AT-Standard genannt, da die Kommandos mit „AT“ beginnen). Dies ist ein nicht normierter, herstellerabhängiger Standard. Die Basis-Befehlssätze der verschiedenen Modems stimmen größtenteils überein. Größere Abweichungen gibt es in den erweiterten Befehlssätzen. Es ist wichtig, den Befehlssatz des eingesetzten Modems daraufhin zu überprüfen, wie die im folgenden beschriebenen Funktionen umgesetzt sind und ob durch fehlerhafte Konfiguration Sicherheitslücken entstehen können.
Die gewählten Einstellungen sollten im nichtflüchtigen Speicher des Modems gespeichert werden (siehe auch M 1.38 - Geeignete Aufstellung eines Modems). Außerdem sollten sie auf Papier ausgedruckt werden, so daß sie jederzeit mit der aktuellen Einstellung verglichen werden können. Nachfolgend werden einige sicherheitsrelevante Konfigurationen vorgestellt:

Auto-Answer
Über das Register S0 kann eingestellt werden, daß das Modem einen ankommenden Ruf automatisch nach einer einzustellenden Anzahl von Klingelzeichen entgegennimmt. Mit der Einstellung S0=0 wird dies verhindert und erzwungen, daß Anrufe manuell entgegengenommen werden müssen. Diese Einstellung sollte gewählt werden, wenn verhindert werden soll, daß von außen unbemerkt eine Verbindung aufgebaut werden kann. Ansonsten ist ein Callback-Mechanismus

einzusetzen (siehe M 5.30 -Aktivierung einer vorhandenen Callback-Option).

Fernkonfiguration des Modems
Manche Modems können so eingestellt werden, daß sie von entfernten Modems fernkonfiguriert werden können. Es ist darauf zu achten, daß diese Möglichkeit ausgeschaltet ist.
Zum Problem der Fernwartung über Modems siehe M 5.33 - Absicherung der per Modem durchgeführten Fernwartung.

Paßwortgeschützte Speicherung von (Rückruf-)Nummern
Bei der Speicherung von Telefonnummern oder Rückrufnummern im nichtflüchtigen Speicher des Modems können diese bei vielen Modellen durch ein Paßwort geschützt werden. Wenn diese Möglichkeit vorhanden ist, sollte sie genutzt und die Paßwörter entsprechend M 2.11 - Regelung des Paßwortgebrauchs gewählt werden. Bei einigen Modems wird nach Eingabe eines bestimmten Befehls eine Liste der Rufnummern mit den zugehörigen Paßwörtern angezeigt. Daher sollte der Zugang zum Modem nur befugten Personen möglich sein (vgl. M 1.38 - Geeignete Aufstellung eines Modems).

M 5.32 Sicherer Einsatz von Kommunikationssoftware
Die Sicherheit des Rechnerzugangs über Modem hängt entscheidend von der eingesetzten Kommunikationssoftware ab.
Fast jede Kommunikationssoftware bietet die Möglichkeit, Telefonnummern und andere Daten von Kommunikationspartnern zu speichern. Dies sind personenbezogene Daten, die entsprechend geschützt werden müssen.
Paßwörter für den Zugang auf andere Rechner oder Modems sollten nicht in der Kommunikationssoftware gespeichert werden, auch wenn das komfortabel erscheinen mag. Jeder, der Zugang zum IT-System und der Kommunikationssoftware hat, kann dann unter fremdem Benutzernamen Zugang in andere Systeme erlangen (siehe auch M 1.38 - Geeignete Aufstellung eines Modems und M 2.8 - Vergabe von Zugriffsrechten).
Etliche Kommunikationsprogramme bieten die Möglichkeit, die Datenübertragung im Hintergrund und damit unbeobachtet laufen zu lassen, z.B. unter Windows. Dies sollte nur bei vertrauenswürdigen Kommunikationspartnern genutzt werden, da hierbei ein Kommunikationspartner die Dateiübertragung abbrechen und u.U. andere Daten als abgesprochen vom oder zum lokalen Rechner übertragen könnte. Damit könnten beispielsweise Computer-Viren auf den lokalen Rechner eingeschleust oder vertrauliche Daten kopiert werden. Es gibt außerdem auch Übertragungsprotokolle, die eine Vollduplex-Übertragung, also gleichzeitiges Senden und Empfangen zulassen. Solche Übertragungsprotokolle sollten nur mit vertrauenswürdigen Kommunikationspartnern benutzt werden, da dies einer Datenübertragung im Hintergrund entspricht.
Verfügt die Kommunikationssoftware über eine Paßwortabsicherung oder über Protokollierungsfunktionen, muß sie aktiviert werden.

M 5.33 Absicherung der per Modem durchgeführten Fernwartung
Die Fernwartung von IT-Systemen über ein Modem birgt besondere Sicherheitsrisiken. Aus

Sicherheitsgründen ist es sinnvoll, auf externe Fernwartung zu verzichten. Ist dies nicht möglich, so sind zusätzliche Sicherungsmaßnahmen unumgänglich. Das zu wartende IT-System einschließlich des eingesetzten Modems muß die folgenden Sicherheitsfunktionen realisieren:

- Der Aufbau der Verbindung für eine Fernwartung sollte immer vom lokalen IT-System initiiert werden. Dies kann durch Anruf des zu wartenden IT-System bei der Fernwartungsstelle oder über einen automatischen Rückruf (Callback) realisiert werden.

- Das externe Wartungspersonal muß sich zu Beginn der Wartung authentisieren. Werden dabei Paßwörter unverschlüsselt übertragen, sollten Einmalpaßwörter benutzt werden (siehe M 5.34 - Einsatz von Einmalpaßwörtern).

- Alle Tätigkeiten bei der Durchführung der Fernwartung müssen auf dem zu wartenden IT-System protokolliert werden. Darüber hinaus können am zu wartenden IT-System noch weitere Funktionalitäten implementiert werden:

- Verhängen einer Zeitsperre bei fehlerhaften Zugangsversuchen,

- Sperren der Fernwartung im Normalbetrieb und explizite Freigabe für eine genau definierte Zeitspanne,

- Einschränkung der Rechte des Wartungspersonals; das Wartungspersonal sollte nicht die vollen Administrator-Rechte besitzen; bei DOS-PCs sollte über eine Zusatzsoftware eine abgestufte Rechteverwaltung realisiert werden; bei Unix-Systemen ist außerdem M 2.33 - Aufteilung der Administrationstätigkeiten unter Unix zu beachten, bei PC-Netzen M 2.38 - Aufteilung der Administrationstätigkeiten, (Das Wartungspersonal sollte nur auf die Daten und Verzeichnisse Zugriff haben, die aktuell von der Wartung betroffen sind.)

- auf dem IT-System sollte für das Wartungspersonal eine eigene Benutzerkennung existieren, unter der möglichst alle Wartungsarbeiten durchgeführt werden,

- wird die Verbindung zur Fernwartungsstelle auf irgendeine Weise unterbrochen, so muß der Zugriff auf das System durch einen SZwangslogout"beendet werden.

Die Fernwartung sollte lokal durch IT-Experten beobachtet werden. Auch wenn die Fernwartung eingesetzt wird, weil intern das Know-How oder die Kapazität nicht verfügbar ist, kann das Wartungspersonal nicht unbeaufsichtigt gelassen werden (siehe auch M 2.4 - Regelungen für Wartungs- und Reparaturarbeiten). Bei Unklarheiten über die Vorgänge sollte der lokale IT-Experte sofort nachfragen. Es muß jederzeit die Möglichkeit geben, die Fernwartung lokal abzubrechen.
Werden während der Wartung Daten oder Programme auf dem lokalen IT-System angelegt, so muß dies deutlich erkennbar und nachvollziehbar sein, also z.B. darf dies nur in besonders markierten Verzeichnissen oder unter bestimmten Benutzerkennungen erfolgen.
Entsprechend M 3.2 - Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen sind auch mit externem Wartungspersonal vertragliche Regelungen über die Geheimhaltung von Daten zu treffen. Insbesondere ist festzulegen, daß Daten, die

im Rahmen der Wartung extern gespeichert wurden, nach Abschluß der Arbeiten sorgfältig gelöscht werden. Ebenso sind die Pflichten und Kompetenzen des externen Wartungspersonals sorgfältig festzulegen.

M 5.34 Einsatz von Einmalpaßwörtern

In Netzen, in denen Paßwörter unverschlüsselt übertragen werden, können diese relativ einfach abgehört werden. Außerdem können Implementierungs- oder Protokollfehler in Betriebssystemen und Applikationssoftware dazu führen, daß auch verschlüsselte Paßwörter kompromittiert werden können. Daher empfiehlt sich die Verwendung von Einmalpaßwörtern, also Paßwörtern, die nach einmaligem Gebrauch gewechselt werden müssen. Einmalpaßwörter können software- oder hardwaregestützt erzeugt werden.

Bei der Verwendung von Einmalpaßwörtern muß der Benutzer das Einmalpaßwort auf dem lokalen IT-System oder über ein Token generieren oder aus einer Liste einlesen, die vom entfernten IT-System generiert worden ist und die sicher aufzubewahren ist. Das entfernte IT-System muß dann das Einmalpaßwort verifizieren.

Für den Einsatz von Einmalpaßwörtern können z.B. Public-Domain-Programme wie OPIE bzw. S/Key benutzt werden. OPIE (One-time Passwords in Everything) ist die Public-Domain-Weiterentwicklung von S/Key, das mittlerweile als kommerzielles Produkt vertrieben wird.

S/Key benutzt im Gegensatz zu OPIE noch standardmäßig den MD4-Algorithmus zum Erzeugen und Verifizieren der Einmalpaßwörter. Wegen der bekannten Schwachstellen des MD4-Algorithmus sollte der im Lieferumfang enthaltene MD5-Algorithmus benutzt werden.

OPIE bzw. S/Key bestehen aus einem Programmteil auf dem Server zum Verifizieren der eingegebenen Paßwörter und einem Programmteil auf dem IT-System des Benutzers. Ein Benutzer bekommt beim Login auf dem entfernten IT-System nach Eingabe seines Benutzernamens die Sequenznummer des einzugebenden Einmalpaßwortes und eine Kennung angezeigt. Mit diesen beiden Angaben und einem geheimzuhaltenden Paßwort berechnen OPIE bzw. S/Key auf dem lokalen IT-System das Einmalpaßwort für diese Sitzung. Steht dem Benutzer zur Berechnung der Einmalpaßwörter lokal kein Programm zur Verfügung, kann vom entfernten System eine Liste mit Einmalpaßwörtern erzeugt werden, die dann entsprechend sicher zu verwahren ist.

Einmalpaßwörter können auch über Token erzeugt werden, die die Generierung übernehmen. Dies können entweder Chipkarten oder taschenrechnerähnliche Geräte sein. Der Benutzer muß sich zunächst gegenüber dem Token authentisieren. Nach erfolgter Benutzerauthentisierung authentisiert sich dann entweder der Token selbständig gegenüber dem Server oder er zeigt dem Benutzer an einem Display das am Client einzugebende Einmalpaßwort an.

Nachdem immer mehr sensible Informationen nur durch Paßwörter vor Fremdzugriff geschützt sind, kommt Einmalpaßwortsystemen und hardwarebasierten Authentifikationsmethoden ein wachsender Stellenwert zu. Wo der Einsatz von softwarebasierten Einmalpaßwortsystemen wie S/Key auf Akzeptanzprobleme stößt, sollten hardwarebasierte Systeme eingesetzt werden. Viele hardwarebasierte Systeme bieten darüber hinaus auch die Möglichkeit, „Single-Sign-On"-Lösungen aufzubauen. Über „Single-Sign-On"-Verfahren wird erreicht, daß sich Benutzer nicht an jedem IT-System mit einem anderen Paßwort ausweisen müssen, sondern daß sie sich auch bei großen heterogen Netzen ausschließlich am ersten benutzten IT-System authentisieren müssen, das diese Informationen dann an alle weiteren IT-Systeme weiterreicht.

Durch hardwarebasierte Einmalpaßwortsysteme werden außerdem viele der unter M 2.11 - Regelung des Paßwortgebrauchs aufgeführten Regelungen, die die einzelnen Benutzer beachten müssen, überflüssig, da dies von den Einmalpaßwortsystemen übernommen wird.

M 5.35 Einsatz der Sicherheitsmechanismen von UUCP
Das im Standardumfang von Unix-Systemen enthaltene und ebenfalls für andere Betriebssysteme verfügbare Programmpaket UUCP (Unix-to-Unix Copy) erlaubt den Datenaustausch zwischen IT-Systemen und die Ausführung von Kommandos auf entfernten IT-Systemen. Voraussetzung ist lediglich die Kompatibilität der uucico-Programme auf den beiden beteiligten Systemen. UUCP ist stark verbreitet, auch wenn seine Bedeutung zurückgegangen ist z. B. durch die Möglichkeit, Rechner über ISDN mittels TCP/IP zu verbinden.
UUCP wird in der Regel zum Austausch von E-Mail und News zwischen Rechnern benutzt (uucp). Es ermöglicht auch das Einloggen (cu) und das Ausführen von Programmen (uux) auf fremden Rechnern.
Es gibt verschiedene UUCP-Varianten: Neben der Implementation von Peter Honeyman, David Nowitz und Brian E. Redman von 1983 (HoneyDanBer UUCP) werden auch häufig das ursprüngliche UUCP-System der AT&T UNIX Version 7, dessen zweite Version aktuell ist (diese UUCP-Implementation wird daher auch Version 2 UUCP genannt) oder das Tahoe-UUCP (das mit BSD 4.3 ausgeliefert wurde) eingesetzt.
Die eingesetzte UUCP-Variante kann an den Dateien im Verzeichnis /usr/lib/uucp (auf einigen Systemen /etc/uucp) erkannt werden: Bei Version 2 UUCP findet sich hier die Datei L.sys, beim HoneyDanBer UUCP die Datei Systems.
Version 2 UUCP hat gravierende Sicherheitsprobleme (Fehler in uucico, Gefahr fehlerhafter Konfiguration durch die komplizierte Form der sicherheitsrelevanten Administrationsdateien). Sie sollte daher nicht benutzt werden, stattdessen sollte das HoneyDanBer UUCP eingesetzt werden.
Allgemein sollten folgende Sicherheitsfragen beim Einsatz von UUCP bedacht werden:

- Die Administration von UUCP setzt eine intensive Beschäftigung mit den Konfigurationsmöglichkeiten und den zugehörigen Dateien voraus. Es muß berücksichtigt werden, daß es zwischen den UUCP-Paketen der verschiedenen Unix-Derivate Abweichungen geben kann, auch wenn diese auf dem HoneyDanBer UUCP basieren.

- Für die Administration der UUCP-Dateien, -Programme und -Verzeichnisse gelten dieselben Anforderungen wie für die Administration von Systemdateien und -verzeichnissen (siehe M 2.25 - Dokumentation der Systemkonfiguration, M 2.31 - Dokumentation der zugelassenen Benutzer und Rechteprofile, M 4.19 - Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen).

- Auf den meisten Systemen gibt es einen Benutzer namens uucp. Diesem Benutzer gehören die UUCP-Dateien, -Programme und -Verzeichnisse. Es ist sicherzustellen, daß dieser Account ein Paßwort gemäß den Vorgaben der Maßnahme M 2.11 - Regelung des Paßwortgebrauchs hat. Das Heimatverzeichnis für den Benutzer uucp darf nicht das öffentliche Verzeichnis /usr/spool/uucppublic sein, sondern ein eigenes, auf das nur der

Benutzer uucp Zugriff hat.

- Für jedes IT-System, das sich per UUCP am lokalen IT-System anmelden können soll, muß in der /etc/passwd eine eigene Benutzerkennung und ein Paßwort eingetragen werden. Als UID darf nicht die des Benutzers uucp gewählt werden, sondern für jedes entfernte IT-System eine beliebige individuelle UID.

- UUCP-Paßwörter werden bei Kommunikationsanforderungen unverschlüsselt übertragen und sind in der entsprechenden UUCP-Konfigurationsdatei für Anforderungen an entfernte Rechner unverschlüsselt gespeichert. Je nach Anwendung und Umgebung (insbesondere bei Benutzung von Weitverkehrsnetzen) sind entsprechende Sicherheitsmaßnahmen wie z.B. der Einsatz von Einmalpaßwörtern zu ergreifen.

Für die Benutzung von UUCP müssen verschiedene Konfigurationsdateien eingerichtet werden. Alle Einstellungen sollten dokumentiert und Abweichungen der im folgenden vorgeschlagenen Einstellungen kurz begründet werden, damit später nachvollziehbar ist, wozu diese Änderung notwendig war.
Die Verwaltung der folgenden Dateien muß besonders sorgfältig gehandhabt werden, da sie sicherheitskritische Informationen enthalten. Sie befinden sich im Verzeichnis /usr/lib/uucp bzw. /etc/uucp). Auf diese Verzeichnisse darf nur der Benutzer uucp schreibenden Zugriff haben.

- Systems: Diese Datei enthält die für einen Verbindungsaufbau mit entfernten IT-Systemen benötigten Informationen. Hier können für jedes einzelne IT-System die Zeiträume festgelegt werden, in denen die Übertragung per UUCP zugelassen ist. Diese Zeiträume sind möglichst eng zu fassen. Die Datei enthält außerdem die Telefonnummern und Login-Sequenzen der IT-Systeme, zu denen per UUCP eine Verbindung aufgebaut werden kann. Auf Systems darf nur der Eigentümer uucp lesenden Zugriff haben, da hier auch die Paßwörter für die entfernten IT-Systeme eingetragen sind.

- Permissions: Hier werden Zugriffsrechte für entfernte Systeme festgelegt. Bei Auslieferung sind in Permissions keine IT-Systeme eingetragen, d. h. über UUCP sind keine Zugriffe möglich. Für jeden Rechner, der anrufen und sich einloggen darf, und für jeden Rechner, der angerufen werden darf, müssen hier Einstellungen zur Festlegung der jeweilig notwendigen Zugriffsrechte und anderer Bedingungen vorgenommen werden. Die Zugriffsrechte für die IT-Systeme, die vom lokalen IT-System angerufen werden, werden unter den auf MACHINE folgenden Einträgen spezifiziert, die für die anrufenden IT-System unter den auf LOGNAME folgenden. Durch Ausnutzung dieser Konfigurationsmöglichkeiten kann die Sicherheit beachtlich erhöht werden. Mit dem Kommando uucheck -v sollten die in der Datei Permissions gesetzten Optionen regelmäßig überprüft werden. Die Optionen sollten wie folgt gesetzt sein:

  REQUEST
  Diese Option sollte auf NO (Default-Wert) gesetzt sein, um entfernten Systemen das Le-

sen lokaler Dateien zu verbieten.

COMMANDS
Hier darf auf keinen Fall ALL eingetragen sein, es dürfen nur die Kommandos zugelassen werden, die nötig sind wie rnews oder rmail. Die Kommandos sollen mit vollem Pfadnamen angegeben werden.

WRITE/READ
Wenn diese Optionen nicht angegeben sind, ist der schreibende bzw. lesende Zugriff ausschließlich auf das Verzeichnis /usr/spool/uucppublic möglich.
Falls hiermit Verzeichnisse angegeben werden, auf die zugegriffen werden darf, ist zu dokumentieren, auf welche und warum. Auf keinen Fall darf hier das Root-Verzeichnis oder das Verzeichnis, in dem sich die UUCP-Konfigurationsdateien befinden, eingetragen sein.

NOWRITE/NOREAD
Hiermit werden Ausnahmen zu den mit WRITE/READ festgelegten Optionen festgelegt. Verzeichnisse mit sensitivem Inhalten sollten hier generell aufgeführt werden. Dann kann nicht dadurch, daß das Setzen von Restriktionen vergessen wird, von entfernten IT-Systemen auf solche Verzeichnisse zugegriffen werden, wenn darüberliegende Verzeichnisse über READ/WRITE freigegeben werden.

PUBDIR
Hiermit kann statt /usr/spool/uucppublic ein anderes öffentliches UUCP-Verzeichnis angegeben werden. Bei UUCP-Kommunikation mit mehreren IT-Systemen sollte hier für jedes IT-System ein eigenes UUCP-Verzeichnis angegeben werden.

CALLBACK
Wenn CALLBACK auf YES gesetzt ist, muß das lokale IT-System das anrufende IT-System zurückrufen, bevor ein Datenaustausch stattfinden kann. Dies macht natürlich nur für LOGNAME Einträge Sinn. Es sollte zwischen den Kommunikationspartnern abgesprochen sein, welche einen CALLBACK aktiviert.

MYNAME
Wenn MYNAME=name gesetzt ist, identifiziert sich das lokale System beim Aufbau einer UUCP-Verbindung beim entfernten System nicht mit dem Rechnernamen, sondern mit name. Diese Möglichkeit sollte benutzt werden, um sich mit einem Namen identifizieren zu können, der nur speziell für diese Verbindung benutzt wird und daher nicht so leicht herausgefunden werden kann.

VALIDATE
Wenn VALIDATE=namen gesetzt ist, können nur die unter namen aufgeführten IT-

Systeme über die unter LOGNAME angegebenen Systemnamen eine Verbindung aufbauen. Bei dieser Option muß unbedingt ein Eintrag vorhanden sein, da sonst ein entferntes IT-System eine Maskerade durchgeführt werden könnte, indem über MYNAME ein anderer Rechnername vorgespiegelt wird.

SENDFILES
Hier sollte die Voreinstellung (SENDFILE=CALL) beibehalten werden, da dann lokal in der Queue befindliche Aufträge nur nach extern übertragen werden, wenn das lokale IT-System die Verbindung aufgebaut hat.

- Die Datei /usr/lib/uucp/remote.unknown des HoneyDanBer UUCP wird ausgeführt, wenn ein unbekanntes, also ein nicht in der Datei Systems eingetragenes IT-System einen Verbindungsaufbau versucht. Es protokolliert den Versuch und weist ihn ab. Wenn remote.unknown nicht ausführbar ist, geht das lokale IT-System auf alle Verbindungsanforderungen entfernter IT-Systeme ein. Es muß daher darauf geachtet werden, daß remote.unknown stets ausführbar ist. remote.unknown ist je nach Unix-System als ausführbares Shellskript oder als C-Programm realisiert. Falls remote.unknown auf dem lokalen IT-System als Shellskript realisiert ist, sollte es aus Sicherheitsgründen durch ein Programm ersetzt werden. Sonst besteht die Gefahr, daß ein anrufendes IT-System ein Kommando wie cat < /etc/passwdäls Systemnamen einträgt, das dann zur Ausführung gelangen kann.

- Für UUCP gibt es einige Cleanup-Shellskripte, die automatisch über den crontab-Dämon ausgeführt werden. Dies darf nicht von root iniitiert werden, wie es auf vielen Systemen üblich ist, sondern muß durch den Benutzer uucp erfolgen. Bei der Benutzung von UUCP werden automatisch verschiedene Protokollierungsdateien angelegt. Beim HoneyDanBer UUCP finden sich diese in Unterverzeichnissen von /usr/spool. Hier werden erfolgreiche und abgelehnte Verbindungsversuche festgehalten, die gesendeten und empfangenen Datenmengen, Fehlermeldungen und Datentransferstatistiken. Diese Protokollierungsdateien müssen regelmäßig ausgewertet werden (siehe auch M 4.25 - Einsatz der Protokollierung im Unix-System).

M 5.36 Verschlüsselung unter Unix und Windows NT

Bei der Übertragung von Nachrichten über ein Netz sollten sich alle Kommunikationspartner darüber im klaren sein, daß unverschlüsselte Nachrichten während ihres gesamten Weges unbemerkt gelesen, geändert bzw. abgefangen werden können. Daher ist zu überlegen, ob die Nachrichten verschlüsselt und / oder digital signiert werden sollten.
In vielen Unix-Systemen stehen Verschlüsselungsprogramme wie crypt zur Verfügung, bei anderen sind die Verschlüsselungsprogramme beim Export aus den USA entfernt worden.
Unter Windows NT stehen verschiedene Verschlüsselungsprogramme von kommerziellen Software-Anbietern zur Verfügung. Darüber hinaus können auch viele Public-Domain-Programme für MS-DOS und MS-Windows, wie z.B. das weiter unten genannte Programm PGP unter Windows NT eingesetzt werden.

Zur Verschlüsselung von Nachrichten stehen u.a. mehrere Public-Domain-Verschlüsselungsprogramme betriebssystemübergreifend zur Verfügung:

DES ist ein einfaches Verschlüsselungsprogramm, das auf dem gleichnamigen Algorithmus basiert. Zum Entschlüsseln der Nachricht muß der Empfänger denselben Schlüssel verwenden, den der Sender zum Verschlüsseln benutzt hat.
PGP (Pretty Good Privacy) ist ein Public-Domain-Verschlüsselungsprogramm, das auf den Algorithmen RSA (für das Schlüsselmanagement) und IDEA (zur Datenverschlüsselung) basiert. Mit PGP können Nachrichten zum einen verschlüsselt und zum anderen zum Schutz vor Veränderungen mit einer digitalen Signatur (auch elektronische Unterschrift genannt) versehen werden.

Bei PGP werden öffentliche und private Schlüssel verwendet. Zu jedem privaten Schlüssel gibt es genau einen öffentlichen Schlüssel. Es ist praktisch ausgeschlossen, nur mit Kenntnis des öffentlichen Schlüssels den privaten Schlüssel zu errechnen. Eine Nachricht, die mit einem öffentlichen resp. privaten Schlüssel verschlüsselt wurde, kann nur mit dem zugehörigen privaten resp. öffentlichen Schlüssel wieder entschlüsselt werden. Der öffentliche Schlüssel kann jedem bekannt gemacht werden und dient dazu, Nachrichten an den Besitzer des privaten Schlüssels zu verschlüsseln. Zum Schutz vor Veränderungen einer Nachricht berechnet PGP unter Zuhilfenahme des privaten Schlüssels einen Prüfcode über die Nachricht, die digitale Signatur. Jeder Kommunikationspartner kann mit Hilfe des öffentlichen Schlüssels des Absenders der Nachricht feststellen, ob der am Ende der Nachricht stehende Prüfcode zu der erhaltenen Nachricht paßt oder ob die Nachricht nachträglich verändert wurde. Es können auch beide Verfahren kombiniert werden, indem der Sender einer Nachricht diese zuerst mit seinem privaten Schlüssel signiert und anschließend mit dem öffentlichen Schlüssel des Empfängers verschlüsselt.
Die Unix-Sourcen von PGP sind beispielsweise von dem FTP-Server ftp.Germany.EU.net (192.76.144.75) oder dem Mail-Server archive-server@Germany.EU.net beziehbar.
Die Unix-Standard-Editoren ed, ex und vi können in einem Verschlüsselungsmodus benutzt werden, so daß Texte direkt bei der Erstellung verschlüsselt werden. Dabei wird i. allg. das Verschlüsselungsprogramm crypt benutzt. Es ist darauf zu achten, daß der Schlüssel nie als Argument für den Kommandoaufruf benutzt wird, da er sonst, z.B. mit dem Kommando ps, ausgespäht werden kann.

Viele Mailprogramme enthalten ebenfalls Optionen zur Verschlüsselung der Nachrichten. Hier ist zu überprüfen, welche Verfahren zur Verschlüsselung eingesetzt werden. In vielen Fällen werden hier nur leicht zu brechende Verfahren eingesetzt. Die Benutzung solcher Verschlüsselungsverfahren erhöht auf jeden Fall den Schutz der Nachricht, es sollte aber überlegt werden, höherwertige Verfahren wie DES oder RSA einzusetzen.

Die Sicherheit der Verschlüsselung hängt von drei verschiedenen Punkten zentral ab:

- Der verwendete Verschlüsselungsalgorithmus muß so konstruiert sein, daß es ohne Kenntnis des verwendeten Schlüssels nicht möglich ist, den Klartext aus dem verschlüsselten Text zu rekonstruieren. Nicht möglich bedeutet dabei, daß der erforderliche Aufwand

zum Brechen des Algorithmus bzw. zum Entschlüsseln in keinem Verhältnis steht zum dadurch erzielbaren Informationsgewinn.

- Der Schlüssel ist geeignet zu wählen. Nach Möglichkeit sollte ein Schlüssel zufällig erzeugt werden. Wenn es möglich ist, einen Schlüssel wie ein Paßwort zu wählen, sollten die diesbezüglichen Regeln aus M 2.11 - Regelung des Paßwortgebrauchs beachtet werden.

- Das Verschlüsselungsprogramm, der verschlüsselte Text und die Schlüssel dürfen nicht zusammen auf einem Datenträger gespeichert werden. Es bietet sich an, den Schlüssel einzeln aufzubewahren. Dies kann dadurch geschehen, daß er schriftlich fixiert wird und anschließend wie eine Scheckkarte im Portemonnaie aufbewahrt wird. Werden die Schlüssel auf Disketten gespeichert, so sollten die Disketten getrennt vom IT-System aufbewahrt werden.

M 5.37 Einschränken der Peer-to-Peer-Funktionalitäten bei Nutzung von WfW, Windows 95 oder Windows NT in einem servergestützten Netz

Werden Windows für Workgroups, Windows 95 oder Windows NT als Benutzeroberfläche in einem servergestützten LAN eingesetzt, so kann damit neben dem servergestützten Netz ein Peer-to-Peer-Netz betrieben werden. Damit werden neben den im Client-Server-Netz (CS) angebotenen Kommunikationsmöglichkeiten neue geschaffen, die auf dem Server (CS) nicht protokolliert werden.
In einer solchen Konstellation ist der Parallelbetrieb der beiden Netzstrukturen nicht sinnvoll, da die gewünschte Funktionalität im allgemeinen vom servergestützten LAN übernommen werden kann. Daher sollte in einem servergestützten LAN auf eine Installation der Peer-to-Peer-Funktionalität ganz verzichtet werden. Der Administrator sollte im Einzelfall entscheiden, ob für bestimmte angeschlossene WfW-, Windows 95- und Windows NT-Rechner die Peer-to-Peer-Funktionalitäten "Dateifreigabeünd Netz-DDE-Freigabefreigeschaltetet wird. Die "Druckerfreigabe"kann hingegen in vielen Fällen eine sinnvolle Ergänzung sein.
Unter Windows NT können nur Administratoren Ressourcen zum Netzzugriff (unter Verwendung des Datei-Managers bzw. Explorers) freigeben. Vor einer derartigen Freigabe ist zu prüfen, ob sie mit den festgelegten Sicherheitsstrategien (siehe auch M 2.67 - Festlegung einer Sicherheitsstrategie für das Peer-to-Peer-Netz und M 2.91 - Festlegung einer Sicherheitsstrategie für das Windows NT Client-Server-Netz) zu vereinbaren ist.

M 5.38 Sichere Einbindung von DOS-PCs in ein Unix-Netz

DOS-PCs können auf verschiedene Arten in Unix-Netze eingebunden werden. PCs haben im allgemeinen schlechtere Sicherheitsmechanismen als Unix-Systeme. Jeder, der Zugang zu einem PC hat, kann diesen administrieren, also z.B. Einstellungen ändern oder Software einspielen.
Durch Einspielen entsprechender Software kann ein vernetzter PC zum Abhören des Netzes benutzt werden. Daher dürfen nur autorisierte Benutzer Zugang zu einem PC haben (siehe auch M 1.23 - Abgeschlossene Türen und M 2.6 - Vergabe von Zutrittsberechtigungen). Weiterhin muß sichergestellt werden, daß nicht unkontrolliert Software eingespielt werden kann und dies auch regelmäßig kontrolliert werden (siehe auch M 2.9 - Nutzungsverbot nicht freigegebener

Software und M 2.10 - Überprüfung des Software-Bestandes).
Außerdem ist es leicht möglich, durch eine Konfigurationsänderung des PCs jede beliebige Rechnerkennung vorzutäuschen und damit eine Maskerade durchzuführen. Daher dürfen bei der Benutzung von RPC auf dem Unix-Server keine Trusted Hosts definiert sein. Trusted Hosts sind Systeme, die als vertrauenswürdig angesehen werden und von denen aus ein Einloggen (mit rlogin) bzw. die Ausführung eines Befehles (mit rsh) ohne Angabe eines Paßwortes möglich ist. Dies wird über die Dateien $HOME/.rhosts und /etc/hosts.equiv auf dem Unix-Server festgelegt. Es muß sichergestellt werden, daß die Dateien $HOME/.rhosts und /etc/hosts.equiv nicht vorhanden oder daß sie leer sind und der Benutzer keine Zugriffsrechte auf sie hat (siehe auch M 5.20 - Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp).
Wenn PCs über NFS an ein Unix-Netz angebunden sind, sind die folgenden Punkte zu beachten:

- Auf einem NFS-Server muß in einer Datei (z.B. /etc/exports oder /etc/dfs/dfstab) jedes Dateisystem bzw. Verzeichnis eingetragen werden, das von anderen Rechnern gemountet werden können soll. Dort werden auch die Zugriffsrechte der NFS-Clients auf die freigegebenen Dateisysteme festgelegt. Bei der Benutzung von NFS muß auf dem Unix-Server darauf geachtet werden, daß nur die Verzeichnisse zum Mounten freigegeben sind, bei denen dies unbedingt erforderlich ist.

- Damit über NFS keine root-Rechte erlangt werden können, darf auf dem Unix-Server kein root-Zugang für exportierte Dateisysteme gewährt werden, wie dies über die Option -root= möglich wäre. Auf keinen Fall darf hiermit einem PC root-Zugang gewährt werden.

- Beim Kopieren von Dateien von einem PC auf ein Unix-System über NFS oder ftp kann es sein, daß die Attribute zu freizügig gesetzt sind. Es ist zu überprüfen, ob dies der Fall ist und gegebenenfalls die umask entsprechend abzuändern.

Computerviren treten hauptsächlich auf DOS-PCs auf. Bei der Vernetzung von PCs mit Unix-Systemen können sich Viren über die Weitergabe von infizierten Programmen von PC zu PC verbreiten. Daher sind hier die selben Maßnahmen zu treffen wie beim Austausch von Programmen über Datenträger oder per DFÜ (siehe auch M 4.3 - Regelmäßiger Einsatz eines Viren-Suchprogramms). Während File-Viren nur innerhalb einer DOS-Emulation eine Bedrohung darstellen, gefährden Viren, die den Boot-Sektor von Intel-basierenden Systemen wie PCs verändern, u.U. auch Unix-Systeme auf Intel-Plattformen. Daneben geht die größte Gefahr von Computerviren für Unix-Systeme von PCs aus, die über NFS Verzeichnisse von einem Unix-System gemountet haben. Viren, die auf einem PC Dateien oder Verzeichnisse löschen oder verändern, können auch auf gemountete Verzeichnisse zugreifen und diese zerstören. Daher sind bei der Freigabe von Verzeichnisse zum Mounten die Zugriffsrechte möglichst restriktiv zu vergeben, insbesondere sollte durch Einsatz der Option ro (read only) auf Verzeichnisse nur lesender Zugriff gewährt werden. Außerdem sollten die Benutzer unter Unix die Attribute ihrer Dateien und Verzeichnisse möglichst restriktiv setzen, z.B. so, daß andere Benutzer nicht darauf zugreifen können oder so daß kein der schreibende Zugriff auf Dateien, die nicht regelmäßig verändert werden, möglich ist. Dies sollte über umask entsprechend voreingestellt werden.

M 5.39 Sicherer Einsatz der Protokolle und Dienste

Die folgenden kurzen Beschreibungen der am häufigsten im Internet verwendeten Protokolle und Dienste sollen als Hinweis dienen, welche Informationen von diesen Protokollen übertragen werden und somit für eine Filterung durch eine Firewall zur Verfügung stehen. Desweiteren ist kurz beschrieben, welche Randbedingungen beim Einsatz der verschiedenen Protokolle und Dienste zu beachten sind.

Bei einer TCP/IP Kommunikation baut in der Regel ein Client-Prozeß von einem zufälligen Port mit einer Portnummer > 1023 eine Verbindung zu einem Server-Prozeß mit einer Portnummer < 1024 (well-known-port) auf. Die Ports mit einer Nummer < 1024 werden auch als privilegierte Ports bezeichnet, da sie nur von Prozessen mit Root-Berechtigung benutzt werden dürfen. Diese Einschränkung, daß Ports < 1024 nur von Prozessen mit Root-Berechtigung benutzt werden dürfen, ist aber nur eine Konvention, die auch umgangen werden kann. Daher darf in einem Sicherheitskonzept nicht vorausgesetzt werden, daß tatsächlich alle IT-Systeme ihre privilegierten Ports auf diese Weise schützen. Auch wenn z.B. mit FTP auf die Ports 20 oder 21 zugegriffen wird, darf dies also nicht als sichere Verbindung angesehen werden.

IP

Das Internet Protocol (IP) ist ein verbindungsloses Protokoll. Ein IP-Header enthält u.a. zwei 32-Bit Adressen (IP-Nummern) für Ziel und Quelle der kommunizierenden Rechner.

Da die IP-Nummern nicht durch kryptographische Verfahren geschützt werden, können sie nur in ganz bestimmten Topographien zur Authentisierung benutzt werden, also nur wenn sichergestellt ist, daß die Adressen nicht geändert werden können. Beispielsweise dürfen Pakete, die von außen kommen, aber als Quelladresse eine Adresse aus dem zu schützenden Netz haben, von der Firewall nicht durchgelassen werden.

ARP

Das Address Resolution Protocol (ARP) dient dazu, zu einer 32-Bit großen IP-Adresse die zugehörige 48-Bit große Hardware- oder Ethernet-Adresse zu finden. Falls in einer internen Tabelle des Rechners kein entsprechender Eintrag gefunden wird, wird ein ARP-Broadcast-Paket mit der unbekannten IP-Nummer ausgesandt. Der Rechner mit dieser IP-Nummer sendet dann ein ARP-Antwort-Paket mit seiner Hardware-Adresse zurück. Da die ARP-Antwort-Pakete nicht manipulationssicher sind, können sie nur in ganz bestimmten Topographien verwendet werden (s.o.).

ICMP

Das Internet Control Message Protocol (ICMP) hat als Protokoll der Transportschicht die Aufgabe, Fehler- und Diagnoseinformationen für IP zu transportieren. Es wird intern von IP, TCP oder UDP angestoßen und verarbeitet und kann auf der Benutzerebene durch den Befehl ping verwendet werden.

Die Meldung Destination Unreachable wird z.B. erzeugt, wenn ein Rechner oder ein Netz nicht erreichbar ist, und kann dazu mißbraucht werden, alle Verbindungen zwischen den beteiligten Rechnern zu unterbrechen.

Die Meldung Redirect wird ausgesandt, wenn ein Gateway erkennt, daß das Paket direkt an

ein anderes Gateway geschickt werden kann, also bisher ein Umweg benutzt wurde. Der kürzere Weg wird dann in die Routingtabelle des Absenders eingetragen. Dieses kann mißbraucht werden, um unerwünschte Routen zu konfigurieren.
Die Firewall muß sicherstellen, daß diese Meldungen nicht durch die Filter durchgelassen werden. Bei den anderen Meldungen ist abzuwägen, ob die nach außen gelieferte Information für einen Angriff mißbraucht werden kann.

Routing Protokolle
Routing Protokolle wie RIP (Routing Information Protocol) oder OSPF (Open Shortest Path First) dienen dazu, Veränderungen der Routen zwischen zwei vernetzten Systemen an die beteiligten Systeme weiterzuleiten und so eine dynamische Änderung der Routingtabellen zu ermöglichen. Es ist leicht möglich, falsche RIP-Pakete zu erzeugen und somit unerwünschte Routen zu konfigurieren. Dynamisches Routing sollte also nur in ganz bestimmten Topographien angewendet werden (s.o.).

TCP
Das Transmission Control Protocol (TCP) ist ein verbindungsorientiertes Protokoll der Transportschicht. Die Korrektheit der Übertragung wird durch Sequenznummern, Prüfsummenbildung mit Empfangsquittung, Quittung mit Zeitüberwachung und einer Segmentübertragungswiederholung nach Quittungszeitablauf sichergestellt. Der Header enthält u.a. zwei 16-Bit Portnummern, die zur Identifikation der Kommunikationsendpunkte dienen und die über eine standardisierte Zuordnung (well-known-ports) mit den Diensten der Anwendungsschicht verbunden sind. Da sie nicht durch kryptographische Verfahren geschützt werden, können sie nur in ganz bestimmten Topographien zur Authentisierung benutzt werden (s.o.).
Das erste bei einem Verbindungsaufbau übertragene Paket ist i.d.R. das einzige, welches ohne ein gesetztes Bestätigungsflag (ACK) übertragen wird. Auf diese Weise ist eine Unterscheidung zwischen Verbindungsaufbau- und Datenübertragungsphase möglich. Die Firewall muß zwischen ACK und ACK-losen Paketen unterscheiden können, also ob ein Verbindungsaufbau stattfindet oder eine bestehende Verbindung benutzt wird.

UDP
Das User Datagram Protocol (UDP) ist ein verbindungsloses Protokoll der Transportschicht. Es gibt keine Transportquittungen oder andere Sicherheitsmaßnahmen für die Korrektheit der Übertragung. Der Header enthält u.a. zwei 16-Bit Portnummern (siehe TCP), die unabhängig von denen beim TCP-Protokoll benutzten Portnummern sind. Da sie nicht durch kryptographische Verfahren geschützt werden, können sie nur in ganz bestimmten Topographien zur Authentisierung benutzt werden.
Da in der Protokolldefinition keine Unterscheidung zwischen einem Verbindungsaufbau und einer Datenübertragung vorgesehen ist, muß diese Unterscheidung von der Firewall übernommen werden. Es muß eine Kontrolle über den Zustand der Verbindung möglich sein, und es muß möglich sein, die Zugehörigkeit eines Paketes zu einer Verbindung eindeutig festzustellen.
Dies kann z.B. erreicht werden, indem bei einem UDP-Verbindungsaufbau der Zielport gespeichert und temporär freigegeben wird, Antwortpakete nur zu diesem Port durchgelassen werden

und nach der Beendigung der Verbindung der Port wieder gesperrt wird.

Telnet
Das Telnet-Protokoll erlaubt einem Benutzer, eine Terminalsitzung auf einem entfernten Rechner durchzuführen und definiert hierzu virtuelle Ein- und Ausgabe-Einheiten (Network Virtual Terminals), zwischen denen Verbindungsparameter ausgehandelt werden müssen.
Um mit dem Kommando Telnet auf einen anderen Rechner zugreifen zu können, muß auf diesem der Telnet-Daemon laufen. Standard-Port für eine Telnet-Sitzung ist der Port 23. Andere Portnummern lassen sich als Parameter angeben, wodurch auch eine Verbindung zu anderen Server-Prozessen hergestellt werden kann.
Da Telnet vollständigen Zugang zu einem Remote-Host für einen Benutzer ermöglicht, muß dieser Zugang durch eine starke Authentisierung geschützt werden.
Es wird häufig unterschieden zwischen einfacher und starker Authentisierung. Bei einfacher Authentisierung werden einfache Paßwortverfahren benutzt, bei denen das Paßwort im Klartext übertragen wird und somit nicht vor Mithören geschützt ist. Im Gegensatz dazu werden bei starker Authentisierung schwerer zu manipulierende Verfahren eingesetzt, die z.B. auf dem Einsatz von Einmalpaßwörter oder dem Besitz von Chipkarten basieren. Bei Telnet besteht die Gefahr, daß sich ein Angreifer auf dem Übertragungsweg in eine autorisierte Telnet-Verbindung eingeschaltet hat, z.B. um sicherheitsrelevante Informationen abzuhören oder um eigene Befehle in die Telnet-Verbindung einzugeben. Daher sollte eine verschlüsselte Übertragung möglich sein.

FTP
Das File Transfer Protocol (FTP) ermöglicht den Austausch von Dateien zwischen entfernten Rechnern.
Bei Benutzung von FTP werden zwei Verbindungen aufgebaut, wobei die Kommandos über Port 21 übertragen werden und die Daten über Port 20. Um den Austausch von Befehlen zwischen Rechnern verschiedener Betriebssysteme zu ermöglichen, definiert FTP eine Reihe von Standardbefehlen. Diese sind nicht identisch mit den Kommandos der Benutzeroberfläche. Der FTP-Client übersetzt die Kommandos der Benutzeroberfläche in die entsprechenden Standardbefehle. Für die Firewall sind die Standardbefehle relevant, da nur diese tatsächlich über TCP/IP übertragen werden.
Während der Client die Kommandoverbindung zum Port 21 des Servers aufbaut, ist der Server für den Aufbau des Datenkanals von seinem Port 20 zu einem Port (> 1023) des Clients verantwortlich. Dies stellt eine Sicherheitslücke dar, da sich Angreifer als Server ausgeben könnten. Daher sollte der Verbindungsaufbau umgekehrt stattfinden und seitens des Clients der Standardbefehl PASV statt PORT verwendet werden. Hierdurch wird erreicht, daß der Server eine zufällige Portnummer berechnet und auf diesem Port die Datenübertragung erwartet. Der Client kann dann eine Verbindung zu diesem Port aufbauen, der TCP-Verbindungsaufbau findet also vom zu schützenden ins externe Netz statt.
Alle Befehle, die Dateien oder Verzeichnisse manipulieren oder lesen (CWD, CDUP, RETR, STOR, DELE, LIST, NLIST), müssen an eine entsprechende Rechteverwaltung gekoppelt sein. Zugriffe nicht vertrauenswürdiger Benutzer werden damit auf bestimmte Dateien eingeschränkt oder ganz unterbunden. Dies setzt einen starken Authentisierungsmechanismus voraus.

Auch der Befehl SYST, mit dem ein Client nach der Betriebssystemversion des Servers fragt, sollte an eine Rechteverwaltung gekoppelt sein bzw. für nicht vertrauenswürdige Benutzer gesperrt werden.
Ferner muß es möglich sein, die Übertragung der Dateien, der Verzeichnisinformationen und der Paßworte zu verschlüsseln.

SMTP
Das Simple Mail Transfer Protocol (SMTP) ist ein einfaches Protokoll für die Übertragung der elektronischen Post im Internet, das aus wenigen Kommandos besteht.
Mit den Befehlen vrfy und expn können interne Informationen abgerufen werden, daher sollte die Verwendung dieser Befehle nur innerhalb des geschützten Netzes erlaubt werden. Für nicht vertrauenswürdige Benutzer sind vrfy und expn zu sperren. Die Firewall sollte in der Lage sein, SMTP-Verbindungen zwischen vertrauenswürdigen Benutzern zu verschlüsseln. Sinnvoll ist dies aber nur dann, wenn ein starker Authentisierungsmechanismus benutzt wird.

DNS
Der Domain Name Service (DNS) dient zur Umsetzung von Rechnernamen in IP-Nummern und umgekehrt und stellt ferner Informationen über im Netz vorhandene Rechnersysteme zur Verfügung. Die übertragenen Informationen werden nicht durch kryptographische Verfahren geschützt, so daß durch gefälschte Daten Spoofing-Angriffe möglich sind. Dies sollte insbesondere bei DNS-Antworten aus dem Internet berücksichtigt werden.
Um auf Rechner eines Netzes zuzugreifen, benötigt ein Eindringling zunächst deren Adressen, die er entweder durch blindes Probieren oder einfacher durch Auswertung der DNS-Informationen erhalten kann. Mittels der Adresse kann der Eindringling dann beispielsweise eine Adressfälschung (IP-Spoofing) vornehmen, indem er vortäuscht, daß sein Rechner zum zu schützenden Netz gehört, und Pakete an das Netz schickt.
Prinzipiell muß beachtet werden, daß alle von DNS zur Verfügung gestellten Informationen mißbraucht werden können. Wie eine Firewall konfiguriert sein muß, um vor den Gefährdungen beim Einsatz von DNS zu schützen, ist in Maßnahme M 2.77 - Sichere Anordnung weiterer Komponenten beschrieben.

NNTP
Das Network News Transfer Protocol (NNTP) wird für die Übertragung von Newsartikeln benutzt.
Die Firewall muß in der Lage sein, den Transport bestimmter Newsgruppen ganz zu verhindern oder nur für einige Rechner zuzulassen. Es muß sichergestellt werden, daß beim Versenden eigener News keine Informationen über das zu schützende Netz (z.B. die Rechnernamen) ins externe Netz gelangen.

HTTP
Das Hypertext Transfer Protokoll (HTTP) wird für die Übertragung von Daten zwischen WWW-Clients und WWW-Servern benutzt. Es werden vier Operationen unterstützt: Connection, Request, Response und Close.

Die Firewall muß in der Lage sein, die Befehle eines HTTP-Paketes zu analysieren und durch Filter einzuschränken. So muß es z.B. möglich sein, bei der Request-Operation die Ausführung des Befehls POST und die damit verbundene Änderung einer Datei zu verbieten. Die Filter müssen benutzerabhängig (mit Hilfe einer starken Authentisierung) und rechnerabhängig unterscheidbar sein.
Die übertragenen Daten müssen nach ihrer Art unterschieden werden können, und es muß möglich sein, spezielle Dateitypen auf bestimmte Informationen zu untersuchen. Sollten für die Verarbeitung der übertragenen Daten weitere Prozesse nötig sein (z. B. ein externer Viewer oder eine Shell), muß es möglich sein, die Ausführung dieser Prozesse vorher vom Benutzer bestätigen zu lassen.

Weitere Dienste: X11, BSD-r-Dienste", NFS, NIS, TFTP
Diese Dienste sollten nicht über eine Firewall hinweg eingesetzt werden (siehe dazu auch G 4.11 Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Client, G 4.12 Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Client bzw. die Maßnahmen

- M 5.17 - Einsatz der Sicherheitsmechanismen von NFS
- M 5.18 - Einsatz der Sicherheitsmechanismen von NIS
- M 5.19 - Einsatz der Sicherheitsmechanismen von sendmail
- M 5.20 - Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp
- M 5.21 - Sicherer Einsatz von telnet, ftp, tftp und rexec

M 5.40 Sichere Einbindung von DOS-PCs in ein Windows NT Netz
DOS-PCs können auf verschiedene Arten in Windows NT Netze eingebunden werden, beispielsweise über TCP/IP oder die Peer-to-Peer-Funktionalitäten von Windows für Workgroups. Im Vergleich zu Windows NT Systemen verfügen DOS-PCs jedoch über weniger Sicherheitsmechanismen. Jeder, der Zugang zu einem PC hat, kann diesen administrieren, also z.B. Einstellungen ändern oder Software einspielen.
Durch Einspielen entsprechender Software kann ein vernetzter PC zum Abhören des Netzes benutzt werden. Daher dürfen nur autorisierte Benutzer Zugang zu einem PC haben (siehe auch M 1.23 - Abgeschlossene Türen und M 2.6 - Vergabe von Zutrittsberechtigungen). Weiterhin muß sichergestellt werden, daß nicht unkontrolliert Software eingespielt werden kann, und dies muß auch regelmäßig kontrolliert werden (siehe auch M 2.9 - Nutzungsverbot nicht freigegebener Software und M 2.10 - Überprüfung des Software-Bestandes).
Außerdem ist es leicht möglich, durch eine Konfigurationsänderung des PCs jede beliebige Rechnerkennung vorzutäuschen und damit eine Maskerade durchzuführen.
Computer-Viren treten hauptsächlich auf DOS-PCs auf. Bei der Vernetzung von PCs mit Windows NT Systemen können sich Computer-Viren über die Weitergabe von infizierten Programmen von PC zu PC verbreiten. Daher sind hier dieselben Maßnahmen zu treffen wie

beim Austausch von Programmen über Datenträger oder per DFÜ (siehe auch M 4.3 - Regelmäßiger Einsatz eines Viren-Suchprogramms). Während File-Viren nur dann eine Bedrohung darstellen, wenn sie in der Lage sind, unter Windows NT ausführbare Dateien so zu verändern, daß diese ausführbar bleiben, gefährden Computer-Viren, die den Boot-Sektor von Intel-basierenden Systemen wie PCs verändern, u.U. auch Windows NT Systeme auf Intel-Plattformen, indem sie diese in einen nicht mehr startbaren Zustand versetzen. Dies kann durch eine Änderung der Bootreihenfolge vermieden werden (vgl. M 4.3 - Regelmäßiger Einsatz eines Viren-Suchprogramms).
Daneben geht die größte Gefahr von Computer-Viren für Windows NT Systeme von PCs aus, die Zugriff auf zum Netzzugriff freigegebene Verzeichnisse des Windows NT Systems haben. Computer-Viren, die auf einem PC Dateien oder Verzeichnisse löschen oder verändern, können auch auf freigegebene Verzeichnisse eines Windows NT Systems zugreifen und diese zerstören. Daher sind bei der Freigabe von Verzeichnissen zum Netzzugriff die Zugriffsrechte möglichst restriktiv zu vergeben; insbesondere sollte auf freigegebene Verzeichnisse nach Möglichkeit nur lesender Zugriff gewährt werden.
Generell sollten die Benutzer unter Windows NT die Attribute ihrer Dateien und Verzeichnisse möglichst restriktiv setzen, z.B. so daß andere Benutzer nicht darauf zugreifen können oder daß kein schreibender Zugriff auf Dateien, die nicht regelmäßig verändert werden, möglich ist. Dies sollte über die Funktionen der Zugriffskontrolle entsprechend voreingestellt werden (siehe auch M 4.53 - Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnissen unter Windows NT). Durch diese Maßnahme wird ein hinreichender Schutz aller auf dem Server abgelegten Dateien erreicht, der vom DOS-PC nicht unterlaufen werden kann.
Falls auf dem PC Windows für Workgroups oder Windows 95 installiert ist, sind außerdem noch die Gefährdungen zu betrachten, die durch die Benutzung der Peer-to-Peer-Funktionalitäten entstehen können (siehe Kapitel 6.3 - Peer-to-Peer-Netz). Als besonderes Problem ist hierbei die Paßwortspeicherung hervorzuheben. Paßwörter werden hier in Dateien der Form [anmeldename].pwl gespeichert. Dort werden sie zwar verschlüsselt abgelegt, können aber mit verschiedenen Programmen ausgelesen werden. Ist es unbedingt notwendig, daß sich ein Benutzer von WfW oder Windows 95 aus an einem Windows NT System anmeldet, sind die Hinweise aus M 4.46 - Nutzung des Anmeldepaßwortes unter WfW und Windows 95 zu beachten. Administratoren müssen auf jeden Fall darauf achten, daß keine Kennwortliste angelegt wird.

M 5.41 Sichere Konfiguration des Fernzugriffs unter Windows NT

Über RAS (Remote Access Service) können sich Benutzer von entfernten IT-Systemen mit lokalen Windows NT Systemen verbinden. Dafür muß auf dem entfernten IT-System der RAS-Client und auf dem lokalen IT-System, das die Fernverbindung annimmt, der RAS-Server installiert sein. Diese Benutzer können über RAS so arbeiten, als wären sie direkt mit dem Netz verbunden. Die entfernten Clients verwenden dabei Standardprogramme, um auf Ressourcen zuzugreifen. Mit Hilfe des Datei-Managers bzw. Explorers werden beispielsweise Netzlaufwerke und Drucker verbunden. Diese Verbindungen sind permanent, d.h. Benutzer müssen Verbindungen zu Netzressourcen während ihrer Sitzung nicht erneut aufbauen. Als Clients werden die Systeme Windows NT, Windows 95, WfW, MS-DOS und OS/2 unterstützt.
Der Benutzer baut eine Verbindung zum RAS-Server mit Hilfe eines lokalen Modems, X.25

oder einer ISDN-Karte auf. Der RAS-Server, der auf einem Windows NT Server ausgeführt wird, authentisiert den Benutzer und bedient die Sitzungen, bis diese durch den Benutzer oder den Netzadministrator beendet werden. Alle Dienste, die normalerweise einem mit einem LAN verbundenen Benutzer zur Verfügung stehen (Datei- und Druckfreigabe, Datenbankzugriff und Benachrichtigung), sind über die RAS-Verbindung möglich.
Der Zugriff auf RAS wird aus dem Pool sämtlicher Windows NT Benutzerkonten gewährt. Mit Hilfe des Benutzer-Managers können einem einzigen Benutzer, einer Benutzergruppe oder sämtlichen Benutzern die Einwählberechtigung ins lokale Netz erteilt werden. Weiterhin bietet die RAS-Verwaltung eine Option, die den Zugriff auf alle Ressourcen ermöglicht, auf die der RAS-Host im Netz zugreifen kann, bzw. nur auf die lokal auf dem Computer vorhandenen Ressourcen. Dann nutzen die Anwender ihre Domänenanmeldung zum Herstellen der Verbindung über RAS. Wurde die Zugriffsberechtigung des Benutzers vom RAS geprüft, kann er die lokalen Ressourcen oder, falls ihm die Berechtigung dazu erteilt wurde, die Ressourcen in der ganzen Domäne sowie in den vertrauten Domänen nutzen.

Über das Challenge Handshake Authentication Protocol (kurz CHAP) vermittelt der Remote Access Server die sicherste der angebotenen Formen verschlüsselter Zugriffsberechtigung, die sowohl vom Server als auch vom Client unterstützt wird. CHAP ermöglicht dem RAS-Server die abwärts gerichtete Aushandlung vom sichersten Verschlüsselungsmechanismus bis zum unsichersten Verfahren mit Klartextübertragung und schützt die in diesem Prozeß übertragenen Kennworte.

CHAP läßt den Einsatz diverser Verschlüsselungsalgorithmen zu. RAS arbeitet insbesondere mit dem kryptographischen Protokoll MD5. RAS greift für die Authentisierung auf DES-Verschlüsselung zurück, wenn sowohl der Client als auch der Server mit RAS arbeiten. Windows NT, Windows für Workgroups sowie Windows 95 handeln bei der Datenkommunikation untereinander immer die DES-verschlüsselte Echtheitsbestätigung aus. Bei Verbindung mit externer RAS-Server- oder Client-Software ist eine Echtheitsbestätigung mit SPAP oder unverschlüsseltem Text möglich, falls das externe Produkt keine verschlüsselte Echtheitsbestätigung unterstützt.

MD5, ein Verschlüsselungsschema, das von diversen PPP-Implementationen für verschlüsselte Echtheitsbestätigungen eingesetzt wird, kann vom Microsoft RAS-Client ausgehandelt werden, wenn eine Verbindung zu anderern RAS-Servern besteht.
PAP arbeitet mit einfachen, unverschlüsselten Kennworten und hat damit als für Echtheitsbestätigungen verantwortliches Protokoll am wenigsten zu bieten. Dieses Protokoll wird normalerweise ausgehandelt, wenn die externe Arbeitsstation und der Server sich nicht auf eine Verschlüsselungsform einigen können, die mehr Sicherheit bietet.

Das RAS-Verschlüsselungsprotokoll sollte [...] in Abhängigkeit vom zu erreichenden Schutzbedarf so gewählt werden, daß mindestens das dort angegebene Protokoll verwendet wird. Dies kann bedeuten, daß bei hohen Sicherheitsanforderungen die Verwendung von Clients, die das geforderte Protokoll nicht unterstützen, ausgeschlossen werden muß.

Datenverschlüsselung schützt Daten und gewährleistet eine sichere Anwählverbindung. Der RAS-Administrator kann den RAS-Server so einstellen, daß die Datenübertragung immer in verschlüsselter Form zu erfolgen hat. Die Benutzer, die an diesem Server angeschlossen sind, verschlüsseln automatisch alle gesendeten Daten.
Hinweis: Diese Option setzt voraus, daß alle angeschlossenen Clients verschlüsseln können. Falls dies gegeben ist, wie z.B. in einem homogenen Windows NT Netz, so ist diese Option auf jeden Fall zu aktivieren.
Die Startoptionen von RAS werden über die Systemsteuerungsoption "Diensteëingestellt, und die Konfigurierung erfolgt über die Systemsteuerungsoption Netzwerk", wobei hier auch die Wahl des Authentisierungsverfahrens geschieht. Durch Wahl der Option Nur Microsoft-verschlüsselte Echtheitsbestätigung"kann die Wahl von CHAP mit MD5 erzwungen werden; zusätzlich läßt sich dann auch die Verschlüsselung des Datenstroms einschalten. Dabei werden die übertragenen Daten in den deutschen Versionen von Windows NT nicht mit DES, sondern mit RC4 verschlüsselt.

RAS unterstützt Sicherheits-Hosts anderer Hersteller, wobei der Sicherheits-Host zwischen den Fernbenutzer und den RAS-Server geschaltet ist. Ein Sicherheits-Host ist ein zusätzlicher Rechner im Netz, der Sicherheitsdienste wie die Unterstützung von Chipkarten anbietet. Ein derartiger Sicherheits-Host bietet im allgemeinen eine zusätzliche Sicherheitsstufe, indem er eine Ausweiskarte zur Echtheitsbestätigung anfordert oder ähnliche starke Authentisierungsverfahren unterstützt, bevor der Zugriff auf den RAS-Server erteilt wird.

Als zusätzliche Sicherheitsmaßnahme bietet RAS die Zugriffsüberwachung per Rückruf (Callback). Mit dieser Funktion kann der Systemadministrator verlangen, daß ein bestimmter Fernbenutzer von einer vorher festgelegten Stelle aus (z.B. privater Telefonanschluß) anruft oder dieser von einer beliebigen Stelle aus zurückgerufen werden kann. Bei der Zugriffsüberwachung per Rückruf leitet der Anwender einen Anruf ein und stellt die Verbindung mit dem RAS-Server her. Der RAS-Server legt dann auf und ruft einen Augenblick später die vorher zugeteilte Rückrufnummer an. Bei Verwendung des analogen Telefonnetzes sind hierzu Rückrufmodems einzusetzen, während bei Übertragung über ISDN bzw. X.25 (z.B. Datex-P) die Leistungen dieser Netze in Anspruch genommen werden können. Dabei ist allerdings zu beachten, daß die Sicherheit der Partneridentifikation bei Wechsel des X.25-Carriers, also bei grenzüberschreitender Datenübertragung, nicht mehr gewährleistet ist.

Unter RAS wird der Fernzugriff auf das Netz vom Systemadministrator gesteuert. Zusätzlich zu den Dienstprogrammen, die zusammen mit Windows NT Server geliefert werden, bietet das Dienstprogramm RAS-Verwaltung dem Administrator die Möglichkeit, Zugriffsberechtigungen für einzelne Benutzer und/oder Gruppen zu erteilen bzw. wieder zu entziehen. Das bedeutet, daß der Zugriff auf das Netz – obwohl RAS auf einem Computer mit Windows NT Server läuft – jedem Benutzer, der auf das Netz über RAS zugreifen darf, ausdrücklich erteilt werden muß. Dabei gewährleistet dieses Verfahren nicht nur, daß Fernzugriff ausdrücklich erlaubt werden muß, sondern erlaubt zudem das Festlegen von Rückrufbeschränkungen.

RAS bietet ein zusätzliches Maß an Sicherheit. Die RAS-Verwaltung bietet eine Option, die den Zugriff auf alle Ressourcen ermöglicht, die der RAS-Host wahrnimmt, bzw. nur auf die lokal auf dem Computer vorhandenen Ressourcen. Somit kann der Administrator genau steuern, welche Daten einem Fernbenutzer zur Verfügung stehen. Nach Möglichkeit sollte die Erlaubnis zum Durchgriff auf weitere Rechner im Netz nur sehr restriktiv oder überhaupt nicht erteilt werden, um bei einem Durchbrechen der Sicherheitsbarrieren den möglichen Schaden zu begrenzen.
Hinweis: Wird RAS in einer Domäne verwendet, wirken sich Änderungen der RAS-Berechtigung nicht sofort auf alle Server aus. Es kann bis zu 15 Minuten dauern, bis eine Änderung auf alle Server der Domäne repliziert worden ist. Bei Bedarf können die Domänen explizit neu synchronisiert werden, um sicherzustellen, daß ein Benutzer mit entzogenen Berechtigungen bis zur automatischen Replikation der Änderung bereits keinen Zugriff auf das Netz mehr hat.

M 5.42 Sichere Konfiguration der TCP/IP-Netzverwaltung unter Windows NT
Bei der Einbindung von Windows NT Systemen in ein Rechnernetz kommt der korrekten Konfiguration der installierten Netzdienste eine besondere Bedeutung zu. In den folgenden Abschnitten werden einige Hinweise zu den meistgenutzten Diensten gegeben; diese ersetzen jedoch nicht eine detaillierte Prüfung der Sicherheitsanforderungen und die Notwendigkeit zur genauen Kenntnis der Systemdokumentation.

DHCP (Dynamic Host Configuration Protocol)
Um den Aufwand für die Verwaltung von IP-Adreßinformationen zu reduzieren, können über DHCP IP-Adressen und die zugehörigen Daten dynamisch konfiguriert werden.
Ein Windows NT Rechner wird ein DHCP-Client, wenn er bei der Installation von TCP/IP für automatische DHCP-Konfiguration konfiguriert wird. Nach dem Start eines DHCP-Clients stellt dieser eine Verbindung zu einem DHCP-Server her, um die erforderlichen TCP/IP-Konfigurationsdaten zu erhalten. Diese Konfigurationsdaten enthalten zumindest eine IP-Adresse, eine Subnetz-Maske sowie die für die Konfiguration geltende Gültigkeitsdauer der Adresse. Die Installation eines DHCP-Servers, die nur von einem Mitglied der Gruppe Ädministratoren"durchgeführt werden kann, gehört zur Installation von Microsoft TCP/IP.
Hinweis: Vor der Installation eines neuen DHCP-Servers muß geprüft werden, ob im Netz bereits andere DHCP-Server vorhanden sind, um einen eventuellen Konflikt zu vermeiden.
Eine automatische Konfiguration eines neuen DHCP-Servers kann nicht über DHCP vorgenommen werden, da ein Computer nicht gleichzeitig DHCP-Client und DHCP-Server sein kann.
Hinweis: Alle Einträge der Registrierung, die sich auf den DHCP Server beziehen, befinden sich unter dem Pfad
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPserver\Parameters.
Mittels des Dienstprogramms DHCP-Manager können folgende grundlegenden Aufgaben ausgeführt werden:

- Einen oder mehrere DHCP-Bereiche anlegen, damit die DHCP-Dienste zur Verfügung stehen.
- Definieren der Eigenschaften des Bereichs, einschließlich der Nutzungsdauer und der IP-

Adressen-Pools, die möglichen DHCP-Clients von Servern in diesem Bereich zugewiesen werden sollen.

- Festlegen von Standardwerten für Optionen wie Standard-Gateway, DNS-Server oder WINS-Server, die zusammen mit einer IP-Adresse zugewiesen werden sollen, und Hinzufügen von eigenen Optionen.

Ein DHCP-Bereich stellt eine Gruppe von Rechnern dar, die den DHCP-Client Dienst in einem Teilnetz ausführen. Der Bereich wird zum Definieren von Parametern für jedes Teilnetz verwendet. Jeder Bereich hat die folgenden Eigenschaften:

- Eine eindeutige Subnetz-Maske, die zum Ermitteln des Teilnetzes verwendet wird, das einer bestimmten IP-Adresse zugeordnet ist.
- Ein Bereichsname, der vom Administrator beim Erstellen des Bereichs zugewiesen wird.
- Werte für die Nutzungsdauer dynamischer Adressen, die den DHCP-Clients zugewiesen werden.

Jedes Teilnetz kann nur einen einzigen Bereich mit einem durchgehenden IP-Adressen-Pool haben; diese Adressen müssen für das Teilnetz gelten. Sollen in einem Teilnetz mehrere Adressenpools realisiert werden, wird ein durchgehender Bereich angelegt, der all diese Adressenpools umfaßt, und dann werden die Adressen zwischen den gewünschten Pools ausgeschlossen. Falls mehr Adressen benötigt werden, kann der Bereich später immer noch ausgeweitet werden.
Die Konfigurationsparameter, die ein DHCP-Server einem Client zuweist, werden unter Verwendung des DHCP-Managers als DHCP-Optionen definiert. Die meisten Optionen sind auf der Grundlage der Standardparameter, die in den Internet-Standards RFC 1541 bzw. RFC 1542 festgelegt wurden, vordefiniert. Wird ein DHCP-Bereich konfiguriert, so können ihm Optionstypen zugewiesen werden, die alle Konfigurationsparameter regulieren.
Zusätzlich zu den IP-Adreßinformationen müssen für jeden Bereich weitere DHCP-Optionen konfiguriert werden, die an DHCP-Clients zu übergeben sind. Diese Optionen können global für alle Bereiche, speziell für einzelne Bereiche oder für einzelne DHCP-Clients mit reservierten Adressen definiert werden. Aktive globale Optionen gelten, sofern sie nicht durch Bereichsoptionen oder DHCP-Client-Einstellungen außer Kraft gesetzt werden. Aktive Optionstypen für einen Bereich gelten für alle Computer in diesem Bereich, sofern sie nicht für einen einzelnen DHCP-Client außer Kraft gesetzt werden.
Hinweis: Eine Veränderung der voreingestellten Werte darf nur bei genauer Kenntnis der Auswirkungen dieser Änderungen erfolgen. Die zu verwendenden Werte sind im Rahmen einer spezifischen Sicherheitsanalyse festzulegen.
Für einen Client kann eine bestimmte IP-Adresse reserviert werden. Das ist in der Regel in den folgenden Fällen notwendig:

- für Domänencontroller, wenn das Netz auch mit LMHOSTS-Dateien arbeitet, die IP-Adressen für Domänencontroller definieren,
- für Clients, die mit IP-Adressen arbeiten, die zur TCP/IP-Konfiguration über ein anderes Verfahren zugewiesen wurden,

- zur Zuweisung durch RAS-Server an Clients, die nicht mit DHCP arbeiten,
- für DNS-Server.

Falls mehrere DHCP-Server Adressen im selben Bereich verteilen, müssen die Client-Reservierungen auf jedem DHCP-Server identisch sein, ansonsten erhält der reservierte Client – in Abhängigkeit vom antwortenden Server – unterschiedliche IP-Adressen. Hinweis: Die IP-Adresse und der statische Name, die in WINS angegeben werden, haben Vorrang vor der IP-Adresse, die vom DHCP-Server zugewiesen wird. In diesen Fällen wird für den Client eine Client-Reservierung mit der IP-Adresse generiert, die in der WINS-Datenbank festgelegt ist.
Die folgenden Dateien sind im Verzeichnis %SystemRoot% \SYSTEM32\DHCP gespeichert, das beim Einrichten eines DHCP-Servers angelegt wird:

- DHCP.MDB ist die DHCP-Datenbankdatei.
- DHCP.TMP ist eine temporäre Datei, die DHCP für temporäre Datenbankdaten anlegt.
- Die Dateien JET.LOG und JET*.LOG enthalten Protokolle mit sämtlichen Transaktionen, die mit der Datenbank ausgeführt wurden. Mit Hilfe dieser Dateien stellt DHCP eventuell verlorengegangene Daten bei Bedarf wieder her.
- SYSTEM.MDB wird von DHCP zum Ablegen der Daten über die Struktur seiner Datenbank genutzt.

Hinweis: Die Dateien DHCP.TMP, DHCP.MDB, JET.LOG und SYSTEM.MDB sollten weder gelöscht noch in irgendeiner Weise verändert werden, da dies zu Fehlfunktionen von DHCP führen kann. Zugriff auf diese Dateien darf nur den Administratoren gegeben werden, da sonst unkontrollierte Veränderungen der DHCP-Konfiguration möglich sind.

WINS (Windows Internet Name Service)
Über WINS können NetBIOS-Computer-Namen zu IP-Adressen zugeordnet werden. Die Installation eines WINS-Servers läuft als Teil der Installation von TCP/IP unter Windows NT Server ab. Damit die einzelnen Server besser verfügbar sind und die Arbeitslast gleichmäßig auf diese Server verteilt ist, sollten mehrere WINS-Server eingerichtet sein. Jeder WINS-Server muß dann so konfiguriert sein, daß er gleichzeitig als Reproduktionspartner für mindestens einen anderen WINS-Server fungiert.
Zur Konfiguration eines WINS-Servers gehört die Angabe von Informationen darüber, wann die Datenbankeinträge für die Partner reproduziert werden. Unter einem Pull-Partner ist ein WINS-Server zu verstehen, der sich Kopien der Datenbankeinträge von seinem Partner beschafft, indem er zuerst eine Anforderung ausgibt und die gewünschten Kopien dann annimmt. Ein Push-Partner ist ein WINS-Server, der seine Partner mit einer Aktualisierungsmeldung benachrichtigt, wenn sich in der WINS-Datenbank etwas geändert hat. Wenn sein Partner auf diese Mitteilung mit einer Reproduktionsanforderung reagiert, sendet der Push-Partner eine Kopie der aktuellen WINS-Datenbank an diesen Reproduktionspartner. Damit die Datenbanken auf dem primären WINS-Server und auf dem Backup-Server immer übereinstimmen,

müssen beide jeweils die Rolle des Push- bzw. des Pull-Partners übernehmen. Es ist ohnehin stets zweckmäßig für Reproduktionspartner, beide Rollen zu übernehmen, d.h. sowohl Push- als auch Pull-Partner zu sein. Für jeden WINS-Server muß ein bestimmter Zeitpunkt, eine Zeitdauer oder eine bestimmte Anzahl von Datensätzen als Schwellwert festgelegt werden. Wird dieser Wert erreicht, so erfolgt die Datenbankreproduktion. Wird für die Reproduktion ein bestimmter Zeitpunkt festgelegt, so wird diese einmal durchgeführt. Ist dagegen eine Zeitdauer festgelegt, so wiederholt sich die Reproduktion in den jeweiligen Abständen. Diese können z.B. in einer geographischen Region im Bereich von $\frac{1}{4}$ bis $\frac{1}{2}$ Stunde liegen, während über größere Entfernungen auch Abstände von einigen Stunden gewählt werden können.
Hinweis: Alle Einträge der Registratur, die sich auf die Konfiguration des WINS-Servers beziehen, befinden sich unter dem Pfad
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WINS\Parameters.
WINS-Server verständigen sich untereinander, um eine vollständige Reproduktion ihrer Datenbanken zu erreichen und zu gewährleisten, daß ein in einem WINS-Server registrierter Name letztlich in allen anderen WINS-Servern des Netzverbundes reproduziert wird. Alle Zuordnungsänderungen werden innerhalb der sogenannten Reproduktionsperiode (maximaler Zeitraum für die Weitergabe der Änderungen an alle WINS-Server) für das gesamte WINS-System gesammelt. Alle freigegebenen Namen werden, sobald sie entsprechend dem im WINS-Manager festgelegten Intervall veraltet sind, an alle WINS-Server weitergeleitet. Die Reproduktion erfolgt unter den Reproduktionspartnern, und nicht zwischen einem Server und den jeweils anderen Servern. Letztendlich werden sämtliche Kopien von den anderen WINS-Servern in einem Netzverbund angefordert, aber die WINS-Server senden Startsignale aus, um darauf hinzuweisen, wann eine Reproduktion eingeleitet werden soll. Damit eine Reproduktion stattfinden kann, muß jeder WINS-Server der Push- oder Pull-Partner von mindestens einem weiteren WINS-Server sein.
Hinweis: Alle Einträge der Registratur, die sich auf die WINS-Reproduktion beziehen, befinden sich unter dem Pfad
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WINS\Partners.
Statische Zuordnungen sind feststehende Listen, in denen Rechnernamen IP-Adressen zugeordnet sind. Diese Zuordnungen lassen sich nicht anzweifeln oder löschen, es sei denn, der Administrator entfernt eine bestimmte Zuordnung. Über den Befehl SStatische Zuordnungenïm WINS-Manager können statische Zuordnungen für diejenigen Clients im Netz hinzugefügt, editiert, importiert oder gelöscht werden, auf denen der WINS-Dienst nicht aktiviert ist.
Hinweis: Ist auf dem Netz auch DHCP im Einsatz, setzt eine reservierte (oder statische) IP-Adresse alle Einstellungen des WINS-Servers außer Kraft. Statische Zuordnungen sollten einem Computer nicht zugewiesen werden, wenn auf diesem Computer WINS aktiv ist
Die folgenden Dateien werden im Verzeichnis %SystemRoot%\SYSTEM32\WINS gespeichert. Dieses Verzeichnis wird automatisch bei der Konfiguration eines WINS-Servers erstellt.

- JET.LOG ist die Protokolldatei für alle Transaktionen, die in der Datenbank durchgeführt werden. WINS verwendet die Datei bei Bedarf zur Wiederherstellung der Daten.

- Mit Hilfe von SYSTEM.MDB hält WINS Informationen über die Struktur der Datenbank fest.

- WINS.MDB ist die WINS-Datenbankdatei.
- WINSTMP.MDB ist eine durch WINS erstellte temporäre Datei. Sie kann nach einem Systemausfall im Verzeichnis \WINS übrig bleiben.

Hinweis: Die Dateien JET.LOG, SYSTEM.MDB, WINS.MDB und WINSTMP.MDB sollten weder gelöscht noch in irgendeiner Form verändert werden, da dies zu Fehlfunktionen von DHCP führen kann. Zugriff auf diese Dateien darf nur den Administratoren gegeben werden, da sonst unkontrollierte Veränderungen der WINS-Konfiguration möglich sind.

SNMP (Simple Network Management Protocol)
SNMP dient zur Überwachung und Administration von TCP/IP-basierten Netzen. Der SNMP-Dienst wird installiert, wenn die entsprechende Option bei der Installation von Windows NT TCP/IP gewählt wird. Nach der Installation muß der SNMP-Dienst mit den gültigen Informationen konfiguriert werden, damit SNMP betriebsbereit ist.
Nur Mitglieder der Gruppe der Administratoren des lokalen Computers können SNMP konfigurieren. Bei der Konfiguration von SNMP werden Communities und Trap-Ziele bestimmt:

- Unter einer Community ist eine Gruppe von Hosts zu verstehen, zu der ein Server gehört, der den SNMP-Dienst ausführt. Es können eine oder mehrere Communities angegeben werden, an die das Windows NT System, auf dem SNMP installiert wird, Traps sendet. Der Name der Community wird beim Senden des Traps in das SNMP-Paket aufgenommen. Empfängt der SNMP-Dienst eine Anforderung, die nicht den richtigen Community-Namen enthält und nicht zu einem der akzeptierten Hosts für den Dienst paßt, kann der SNMP-Dienst ein Trap an das (die) Trap-Ziel(e) senden, das darauf hinweist, daß die Echtheitsbestätigung der Anforderung fehlschlug.
- Trap-Ziele sind die Namen oder IP-Adressen von Hosts, an die der SNMP-Dienst Traps, d.h. Meldungen vordefinierter Ereignisse, mit dem ausgewählten Community-Namen senden soll. Hinweis: SNMP sollte grundsätzlich so konfiguriert werden, daß es nur Anforderungen definierter Communities (und möglichst nicht der vordefinierten Community public) annimmt.

Die SNMP Sicherheit gestattet es, die Communities und Hosts festzulegen, von denen ein Computer Anforderungen entgegennimmt. Ferner kann festgelegt werden, ob ein Echtheitsbestätigungs-Trap gesendet wird, wenn eine Community oder ein Host unberechtigterweise Informationen anfordern. Diese Festlegungen sind sorgfältig zu planen, und die Möglichkeit des Versendens von Traps ist zu nutzen. Die dabei entstehenden Protokolle sind regelmäßig auszuwerten.

M 5.43 Sichere Konfiguration der TCP/IP-Netzdienste unter Windows NT

TCP/IP
Bei der Installation des Protokolls TCP/IP werden dessen Eigenschaften mit der Systemsteuerungsoption Netzwerkfestgelegt. Dabei ist zu beachten, daß, sofern der betreffende Rechner über mehr als eine Netzkarte verfügt und/oder Fernzugriff über RAS (Remote Access Server, siehe M 5.41 - Sichere Konfiguration des Fernzugriffs unter Windows NT) installiert ist, das

Routing zwischen diesen Karten bzw. zwischen dem Fernzugriffsinterface und der Netzkarte über die Registerkarte Routing", Option ÏP-Forwarding aktivierenëingeschaltet werden kann. Diese Option sollte bei Rechnern, die eine Verbindung zu einem externen Netz, etwa dem Internet, haben, in der Regel nicht aktiviert werden, da sie dann externen Rechnern transparent Zugriff auf das lokale Netz gewähren.
In der Version 4.0 läßt sich in begrenztem Maße auch eine Filterung des Datenverkehrs über TCP/IP erreichen. Dazu ist auf der Registerkarte ÏP-Adressen"die Option Ërweitertßu wählen und in dem dann dargestellten Fenster die Option SSicherheit aktivierenßu wählen. Mit der Option "Konfigurierenlassen sich dann die für die einzelnen Netzkarten zuzulassenden bzw. zu sperrenden TCP- und UDP-Anschlüsse (Ports) und IP-Protokolle wählen. Die hier einzutragenden Werte sollten unter Berücksichtigung der notwendigen Funktionalität und der gegebenen Sicherheitsanforderungen gewählt werden. Für einen Rechner mit externen Verbindungen sollte dabei ein Sicherheitskonzept für die Nutzung der Internet-Dienste vorhanden sein. Hierzu sollten ähnliche Überlegungen wie bei der Installation eines Firewalls angestellt werden (siehe Grundschutz-Baustein 7.3 - Firewall, insbesondere M 2.76 - Auswahl und Implementation geeigneter Filterregeln).

FTP (File Transfer Protocol)
Ein FTP-Server wird unter Version 3.51 während der Installation von TCP/IP eingerichtet; in der Version 4.0 kann der FTP-Server als Teil der Installation der Peer-Web-Dienste installiert werden. Wird der FTP-Serverdienst auf einem Windows NT System ausgeführt, können andere IT-Systeme über das Dienstprogramm FTP als Clients den Anschluß zu diesem Windows NT System herstellen und Dateien übertragen. Benutzer, die eine Verbindung zum FTP-Serverdienst herstellen, werden über ihr Benutzerkonto unter Windows NT authentisiert und erhalten je nach ihrem Benutzerprofil Zugriff. Aus diesem Grund ist es erforderlich, den FTP-Serverdienst auf einer NTFS-Partition zu installieren, damit die Dateien und Verzeichnisse, die über FTP zugänglich gemacht werden, geschützt werden können.
Nach Installation des FTP-Serverdienstes muß dieser Dienst konfiguriert werden, bevor damit gearbeitet werden kann. Bei der Konfiguration führen die Einstellungen zu einer der folgenden Situationen:

- Es ist keine anonyme FTP-Verbindung zulässig. In diesem Fall muß jeder Benutzer einen unter Windows NT gültigen Benutzernamen und ein Kennwort eingeben.
- Sowohl anonyme Benutzer als auch Benutzer unter Windows NT können eine Verbindung herstellen. In diesem Fall kann ein Benutzer zwischen einem anonymen Anschluß oder einer Verbindung über einen Benutzernamen und ein Kennwort unter Windows NT wählen.
- Es sind nur anonyme FTP-Verbindungen zulässig. In diesem Fall kann ein Anwender durch Eingabe eines Benutzernamens und eines Kennwortes unter Windows NT keine Verbindung herstellen.

Hinweis: FTP überträgt standardmäßig die Benutzerkennwörter unverschlüsselt über das Netz. Ein Benutzer mit einem Netzanalyseprogramm kann daher die Benutzerkennwörter für Fern-

konten während der FTP-Authentisierung herausfinden.
Ob anonyme FTP-Verbindungen zugelassen werden sollten, hängt von verschiedenen Faktoren ab:

- In einem reinen NT-Netz gibt es sicherere Arten der Datenübertragung, FTP sollte daher überhaupt nicht zugelassen werden.
- In einem heterogen LAN mit NT-Rechnern kann FTP zur Datenübertragung zwischen verschiedenen Systemen erforderlich sein. Um zu verhindern, daß die NT-Benutzerkennungen inklusive Paßwörtern abgehört werden, beispielsweise mit Sniffern, sollte auf den NT-Rechnern nur anonymes FTP zugelassen werden.
- Beim Einsatz von FTP in WANs muß das lokale Netz zusätzlich durch eine Firewall geschützt werden. Anonyme Verbindungen sollten nur auf speziell hierfür eingerichteten Systemen erlaubt werden; auf diesen Systemen darf keine andere Information als nur die über FTP anzubietende gespeichert werden.

Für anonyme Verbindungen muß der Benutzername Änonymouseingegeben werden, ein Paßwort wird nicht benötigt, aber der Benutzer wird aufgefordert, seine E-Mail-Adresse einzugeben. Unter Windows NT muß für anonyme Verbindungen ein lokales Benutzerkonto eingerichtet werden, standardmäßig ist dies "Gast". Sobald über eine anonyme FTP-Verbindung eine Datenübertragung erfolgt, überprüft Windows NT den in diesem Dialogfenster zugewiesenen Benutzernamen und stellt anhand dieses Namens fest, welche Dateizugriffe zulässig sind.
Die für anonyme Verbindungen verwendete Benutzerkennung sollte Mitglied der Gruppe "Gästeünd auf keinen Fall Mitglied der Gruppe "Benutzerßein, da im zweiten Fall leicht zu umfangreiche Zugriffsmöglichkeiten bestehen können.
Bei der Erstinstallation des FTP-Serverdienstes müssen zusätzlich die Zugriffsrechte dieses Dienstes konfiguriert werden. Dabei sind die Laufwerke bzw. Partitionen auszuwählen, deren Zugriffsrechte konfiguriert werden sollen. Je nach gewünschter Sicherheit für die ausgewählte Partition wird der Lesezugriff oder Schreibzugriff oder beide aktiviert. Die so vergebenen Berechtigungen gelten auf FAT-Partitionen und HPFS-Partitionen für alle Dateien der gesamten Partition. Auf NTFS-Partitionen kann mit Hilfe dieser Einstellung der Lese- oder Schreibzugriff (oder beides) für die gesamte Partition gesperrt werden.
Alle so festgelegten Einschränkungen gelten zusätzlich zu den Sicherheitsmaßnahmen, die unter Umständen einen Teil des Dateisystems bilden. Das heißt, daß ein Administrator über dieses Dialogfeld die Berechtigungen für bestimmte Datenträger entfernen, aber über die im Dateisystem festgehaltenen Berechtigungen hinaus keine weiteren erteilen kann. Wenn z.B. für eine Partition nur Lesezugriff erteilt wurde, kann über FTP niemand auf diese Partition schreiben, unabhängig davon, welche Berechtigungen für FTP festgelegt wurden.
Es besteht die Möglichkeit, eingehende FTP-Verbindungen im System-Ereignisprotokoll festzuhalten, indem für Version 3.51 von Windows NT die Werte für LogAnonymous und LogNonAnonymous im Registrierungsschlüssel
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ftpsvc\Parameters auf 1 gesetzt werden. Diese Werte sind standardmäßig nicht in der Registrierung vorgesehen. Damit eingehende Verbindungen protokolliert werden, müssen die Werte neu eingetragen werden. Es

kann angegeben werden, ob sowohl für anonyme als auch für nicht-anonyme Benutzer, die eine Verbindung zum FTP-Server herstellen, Einträge in das Ereignisprotokoll vorgenommen werden sollen.
In Version 4.0 von Windows NT können die entsprechenden Einstellungen für die Sicherheit des FTP-Serverdienstes mit Hilfe des Internet Service Managers vorgenommen werden; direkte Änderungen der Registrierung sind hier nicht mehr erforderlich.

Telnet
Windows NT stellt selbst keinen Telnet-Server zur Verfügung; dieses System kann nur als Telnet-Client arbeiten. Der Telnet-Client wird zusammen mit TCP/IP installiert. Falls ein Telnet-Server benötigt wird, kann der als Bestandteil des Windows NT Resource Kits Version 4.0 verfügbare Telnet-Dämon bzw. ein Produkt eines Fremdherstellers oder Shareware eingesetzt werden.
Hinweis: Da Telnet beim Logon die Benutzerpaßwörter im Klartext überträgt, sollte die Installation und Nutzung von Telnet nur dann erlaubt werden, wenn das Rechnernetz zuverlässig gegen Abhören geschützt ist. Nach Möglichkeit sollte deshalb auf die Verwendung von Telnet grundsätzlich verzichtet werden.

NFS (Network File System)
Windows NT stellt selbst weder einen NFS-Client noch einen NFS-Server zur Verfügung. Sofern NFS genutzt werden soll, müssen Produkte von Drittherstellern eingesetzt werden.
Zur Konfiguration dieser Produkte können keine allgemeinen Angaben gemacht werden, doch sollten, soweit dies unterstützt wird, die entsprechenden Vorgaben für die Konfiguration von NFS unter dem Betriebssystem Unix umgesetzt werden.

M 5.44 Einseitiger Verbindungsaufbau
In den meisten Fällen gibt es für ein Modem genau einen Telefonanschluß. Über diesen Telefonanschluß iniiert das Modem einerseits ausgehende Anrufe und nimmt andererseits auch die eingehenden Anrufe entgegen. Damit kein Angreifer unbemerkt Zugriff auf das angeschlossene IT-System nehmen kann, sollte hier zumindest ein Callback-Mechanismus eingesetzt werden (siehe auch M 5.30 Aktivierung einer vorhandenen Callback-Option).
Trotz eines aktivierten Callback kann das Problem bestehen, daß eine kommende Verbindung nicht ausgelöst wird, solange der Anrufer nicht auflegt. Die öffentliche Vermittlungsstelle löst eine solche Verbindung erst nach einem gewissen Zeitraum aus. Dies Problem tritt in erster Linie dann auf, wenn keine TK-Anlage die Verbindung zusätzlich auslöst.
Damit kann ein Angreifer einen Callback iniitieren, aber gleichzeitig die Leitung belegt halten, so daß das Modem zwar korrekt die gespeicherte Rufnummer für den Callback anwählt, aber nach wie vor mit dem Angreifer verbunden bleibt.
Um dies zu verhindern, sollte zunächst überprüft werden, ob eine kommende Verbindung auch dann getrennt wird, wenn der Anrufer nicht auflegt. Ist dies nicht der Fall und kann es außerdem nicht gewährleistet werden, daß alle Modemverbindungen durch einen Betreuer überwacht werden, sollte überlegt werden, mit getrennten Telefonanschlüssen mit einseitigem Verbindungsaufbau zu arbeiten, d. h. mit einem Anschluß für gehende und einem für kommende Verbindun-

gen. Dies erfordert für jeden Anschluß ein eigenes Modem und die Durchführung des Callback über die Applikation. Dabei ist darauf zu achten, daß das Modem für gehende Verbindungen keine Anrufe automatisch entgegennimmt (S0=0, d.h. kein Auto-Answer). Damit vom Modem für kommende Verbindungen keine Verbindungen nach außen aufgebaut werden können, sollte der Modemanschluß entweder an der internen TK-Anlage für gehende Verbindungen gesperrt werden oder eine entsprechende Sperre bei der Telekom beantragt werden.

M 5.45 Sicherheit von WWW-Browsern

Beim Zugriff auf das World Wide Web (WWW) können verschiedene Sicherheitsprobleme auf den angeschlossenen Arbeitsplatzrechnern auftreten. Diese können durch falsche Handhabung durch die Benutzer bzw. durch eine unzureichende Konfiguration der benutzten Browser (also der Programme für den Zugriff auf das WWW), aber auch durch Sicherheitslücken in den Browsern verursacht werden.

Eine Gefährdung der lokalen Daten geht beispielsweise von Programmen aus, die aus dem Internet geladen werden und ohne Nachfrage auf dem lokalen Rechner ausgeführt werden (z.B. ActiveX-Programme, Java-Applets o.ä.). Auch innerhalb von Dokumenten oder Bildern können Befehle enthalten sein, die automatisch beim Betrachten ausgeführt werden und zu Schäden führen können (z.B. Makro-Viren in Winword- oder Excel-Dokumenten). Um solche Probleme zu vermeiden, sollten die im folgenden beschriebenen Maßnahmen umgesetzt werden.

Laden von Dateien und/oder Programmen

Beim Laden von Dateien und/oder Programmen können eine Vielzahl von Sicherheitsproblemen auftreten, die bekanntesten sind sicherlich Viren, Makro-Viren und trojanische Pferde. Die Benutzer dürfen sich nie darauf verlassen, daß die geladenen Dateien oder Programme aus vertrauenswürdigen Quellen stammen. Alle Benutzer müssen darauf hingewiesen werden, daß sie selber dafür verantwortlich sind, beim Dateiladen alle entsprechenden Vorsichtsmaßnahmen zu ergreifen. Selbst wenn über die Firewall automatisch die geladenen Informationen auf Viren überprüft werden, bleiben die Benutzer verantwortlich für die Schadensfreiheit von geladenen Dateien oder Programmen. Grundsätzlich müssen bei der Installation von Programmen natürlich die organisationsinternen Sicherheitsregeln beachtet werden. Insbesondere dürfen nur getestete und zugelassene Programme installiert werden. Vor der Installation sollten auf Standalone-Rechnern Tests auf die Schadensfreiheit der Programme durchgeführt werden.

In Zweifelsfällen ist die IT-Administration hinzuzuziehen.

Cookies

In sogenannten Cookie-Dateien werden auf dem Rechner des Benutzers Informationen über abgerufene WWW-Seiten, Paßwörter und Benutzerverhalten gespeichert. Damit können WWW-Anbieter beim nächsten Besuch des jeweiligen Benutzers spezielle Informationen für diesen anbieten oder diesem paßwortgesichert nur bestimmte Dienste zugänglich machen. Allerdings kann ein WWW-Anbieter hiermit auch Benutzerprofile erstellen, z.B. für zielgruppenorientierte Werbung.

Um dies zu verhindern, sollte das Anlegen von Cookie-Dateien verhindert werden oder, wo das nicht möglich ist, diese regelmäßig gelöscht werden. Cookies finden sich meist im Konfigurationsverzeichnis des benutzten WWW-Browsers in Dateien wie cookie.txt oder Verzeichnissen

wie cookies. Beispielsweise heißt diese Datei beim Netscape Navigator 2.02 unter Unix $HOME/.netscape/cookies. Es sollten vorzugsweise Browser eingesetzt werden, mit denen sich das Anlegen von Cookies verhindern läßt. Wo dies nicht möglich ist, sollten zumindest solche Browser eingesetzt werden, die Benutzer vor der Annahme von Cookies warnen. Diese Option muß immer aktiviert werden. Die Benutzer können dann in jedem Einzelfall die Annahme von Cookies akzeptieren oder ablehnen. Lehnen sie die Annahme ab, kann dies dazu führen, daß einige WWW-Seiten nicht oder nicht vollständig übertragen werden, dies ist aber nur selten der Fall. Lassen sich die Benutzer vor der Annahme von Cookies warnen, bekommen sie mit der Warnung auch den angedachten Inhalt des Cookies angezeigt, so daß damit auch transparent wird, welche Anbieter welche Informationen über die Benutzer sammeln.
Um das Anlegen von Cookie-Dateien zu verhindern, kann auch eine leere Cookie-Datei angelegt werden und mit einem Schreibschutz versehen werden. Inwieweit dies effektiv ist, hängt vom eingesetzten Betriebssystem und der Browser-Variante ab. Hier ist insbesondere zu überprüfen, ob der Browser weder den Schreibschutz zurücksetzen kann noch dadurch einen Absturz verursacht.
Ansonsten kann es hilfreich sein, das regelmäßige Löschen der Cookies über eine Batch-Datei zu steuern, die beispielsweise bei jedem Systemstart oder jeder Benutzeranmeldung die alten Cookie-Dateien löscht.

Datensammlungen
Nicht nur extern werden Daten über die Internetnutzung der verschiedenen Benutzer gesammelt, sondern auch lokal. Auch hier muß sichergestellt werden, daß nur Befugte darauf Zugriff haben können. Dies gilt insbesondere auch für die von Browsern angelegten Dateien über History, Hotlists und Cache. Die Benutzer müssen informiert werden, wo auf ihren lokalen Rechner solche Daten gespeichert werden und wie sie diese löschen können. Diese Dateien sind auf Proxy-Servern besonders sensibel, da auf einem Proxy-Server alle externen WWW-Zugriffe aller Mitarbeiter protokolliert werden, inklusive der IP-Nummer des Clients, der die Anfrage gestartet hat, und der nachgefragten URL. Ein schlecht administrierter Proxy-Server kann daher massive Datenschutz-Verletzungen nach sich ziehen.
Von den meisten Browsern werden viele Informationen über den Benutzer und sein Nutzerverhalten gesammelt, von denen dieser einerseits vielleicht nicht will, daß sie weitergegeben werden, und die anderseits in ihrer Masse den verfügbaren Speicherplatz mit überflüssigen Informationen blockieren. Zu diesen Informationen gehören:

- Favoriten,
- abgerufene WWW-Seiten,
- Newsserver Visiten (s.u.),
- History Datenbank (s.u.),
- URL Liste (Liste der letzten aufgerufenen URLs),
- Cookie Liste,

- Informationen über Benutzer, die im Browser gespeichert und evtl. auch weitergegeben werden (s.u.),
- Informationen im Cache (s.u.).

Informationen über Newsserver Visiten
Aus den meisten Browsern heraus kann direkt auf Newsserver zugegriffen werden.
Netscape merkt sich dabei die laufende Nummern der gelesenen News. Damit kann für ein Benutzerprofil festgestellt werden, welche Newsgruppen und welche News ein Benutzer gelesen hat.
Der Microsoft Internet Explorer geht noch einen Schritt weiter und speichert den vollständigen Inhalt aller gelesenen News.

History Datenbank
Die History Datenbank des Internet Explorer enthält eine vollständige Sammlung über alle Aktivitäten, die mit diesem Browser durchgeführt worden sind, d.h. Angaben über betrachtete Bilder, Adressen, evtl. betrachtete vertrauliche interne Dokumente etc.
Dadurch verbraucht die History Datenbank auch schnell sehr viel Speicherplatz und sollte regelmäßig aufgeräumt werden. Die Dateien der History Datenbank sollten nicht einfach gelöscht werden, sondern durch vorbereitete Kopien einer leeren History Datenbank ersetzt werden, da bestimmte Einträge erhalten bleiben müssen.

Informationen über Benutzer
In einem Browser werden auch diverse Informationen über Benutzer gespeichert und evtl. auch weitergegeben, z.B. Realname, E-Mail-Adresse, Organisation. Um nicht mit Werbe-E-Mail überflutet zu werden, empfiehlt es sich, für die Browser-Benutzung einen Alias zu verwenden.

Informationen im Cache
Der Internet Explorer ebenso wie Netscape und andere Browser erzeugen in einem Cache-Verzeichnis große Mengen an Dateien, die den Text und die Bilder aller besichtigten Web-Seiten enthalten, seit der Cache das letzte Mal gelöscht wurde.
Der Cache dient dazu, um das mehrfache Laden von Informationen einer Seite während einer Seite zu verhindern. Der Internet Explorer löscht diese Daten, die in jeder weiteren Sitzung absolut nutzlos sind, allerdings nicht eigenständig, so daß sich in einem nicht regelmäßig gelöschten Cache schnell Dutzende Megabyte Datenmüll ansammeln. Aus diesen Daten lassen sich darüber hinaus auch Benutzerprofile erstellen.
Daher sollte der Cache ebenso wie der Verlaufsordner regelmäßig gelöscht werden.
Leider ist es für die Benutzer nicht immer leicht zu erkennen, wie sie den Cache leeren können. Beispielsweise kann beim Internet Explorer unter Windows 95 der Cache geleert werden, indem dort unter Ansicht/Optionen/Erweitert/Temporäre Internet-Dateien/Einstellungen die Option Ordner leeren gewählt wird.

Zugriff auf Client-Festplatte
Bei einigen Browsern (wie z.B. Netscape oder Microsoft Internet Explorer) wird WWW-Servern

die Möglichkeit gegeben, aktiv auf die Festplatte des Client zuzugreifen (ActiveX, Java).
Java- bzw. ActiveX-Programme werden über den Browser statt auf dem Server auf der Client-Seite ausgeführt. Dies führt aber zu einer Verlagerung des Sicherheitsrisikos vom Server auf den Client. Daher sind in Java und ActiveX verschiedene Sicherheitsmechanismen eingebaut, um einen möglichen Mißbrauch zu verhindern, allerdings sind bereits mehrfach Sicherheitslücken gefunden worden.
Die Benutzung von Browsern, die Zugriffe auf Dateien des Client gestatten, birgt im Zusammenhang mit ActiveX und Java gewisse Sicherheitsrisiken. ActiveX erlaubt unter bestimmten Bedingungen die Nutzung lokaler Ressourcen. Bei Java ist ein solcher Zugriff ebenfalls möglich, jedoch nur wenn der Anwender dies explizit gestattet. Das Sicherheitskonzept von ActiveX basiert darauf, daß der Anwender dem Anbieter und einer authentifizierten dritten Stelle im World Wide Web vertraut. Dieses Vertrauen ist problematisch, wenn Web-Seiten eines unbekannten oder eines neuen Anbieters aufgerufen werden.
Aufgrund der bestehenden Probleme mit ActiveX, Java und JavaScript sollten diese generell abgeschaltet werden.
Falls die Benutzung von ActiveX, Java und JavaScript unbedingt notwendig ist, sollten diese nur auf Rechnern zugelassen sein, die gegenüber anderen internen Rechnern so abgeschottet sind, daß die Vertraulichkeit und Integrität sicherheitsrelevanter Daten nicht beeinträchtigt werden können.

Sicherheitslücken in den WWW-Browsern
In den meisten Browsern sind bereits gravierende Sicherheitslücken gefunden worden. So wurden beispielsweise im Februar und März 1997 gleich mehrere Sicherheitslücken in verschiedenen Versionen des Microsoft Internet Explorers entdeckt.
Diese Fehler entsprangen alle aus dem Versuch von Microsoft, WWW und lokale Windows-Komponenten miteinander zu verbinden. Dabei wurde bestimmten WWW-Seiten soviel Vertrauen wie lokalen Daten eingeräumt. Hierdurch konnten durch entsprechende Schadprogramme alleine durch das Aufrufen unseriöser WWW-Seiten auf den lokalen Rechnern der WWW-Benutzer gefährliche Programme ausgeführt werden, ohne daß die Benutzer dies bemerkten.

Verschlüsselung
Da im Internet alle Daten im Klartext übertragen werden, sollten sensible Daten nur verschlüsselt übertragen werden. Hierbei wäre es sinnvoll, wenn entsprechende Mechanismen schon in den unteren Schichten des Protokolls vorgesehen würden. Es ist zu überlegen, inwieweit zur sicheren Übertragung von Daten über das Internet neuere Protokolle wie IPv6, S-HTTP oder SSL eingesetzt werden können. Neuere Browser unterstützen die Benutzung diverser Sicherheitsprotokolle, zumindest SSL sollte unterstützt werden.

Nutzung vorhandener Sicherheitsfunktionalitäten
Die vorhandenen Sicherheitsfunktionalitäten der Browser (Rückfrage vor dem Ausführen von Programmen, Zugriff nur auf eingeschränkte Dateisysteme, keine Möglichkeit zum Verändern lokaler Daten) sollten auf jeden Fall genutzt werden.
Beim Surfen im Internet sollte die automatische Ausführung von Programmen verhindert wer-

den (z. B. über die Option Disable Java) und nur bei vertrauenswürdigen Servern wieder eingeschaltet werden.
Beim Hinzufügen von Plug-Ins, also Programmerweiterungen, für den WWW-Browser sind dieselben Vorsichtsmaßnahmen wie beim Laden von Dateien und/oder Programmen zu beachten. Es dürfen keine Programme installiert werden, denen man nicht unbedingt vertrauen kann.
News-Reader und Mail-Clients bieten häufig die Möglichkeit, beliebige Daten im MIME-Format zu lesen. Auch in diesen Daten können Befehle enthalten sein, die zu einem automatischen Starten von Programmen auf dem lokalen Rechner führen. Die entsprechenden Möglichkeiten sollten daher in den Konfigurationsdateien entfernt werden bzw. nur nach Rückfrage gestartet werden können.

Informationsbeschaffung über Sicherheitslücken
Da immer wieder neue Sicherheitslücken in WWW-Browsern bekannt werden, ist eine regelmäßige Informationsbeschaffung über solche Sicherheitslücken und deren Beseitigung erforderlich. Hierbei sollte nicht die Beschaffung der aktuellsten Version des Produktes im Vordergrund stehen, da auch hier durch neue Programmteile ggf. neue Sicherheitsprobleme auftreten. Zumindest sollte durch das Einspielen von Patches sichergestellt werden, daß bekannte Sicherheitslücken beseitigt werden.

Regelungen
Ein Großteil der oben beschriebenen Maßnahmen liegt im Verantwortungsbereich der Benutzer, da deren Umsetzung wie beispielsweise die Aktivierung bestimmter Optionen nicht ständig durch die Systemadministration überprüft werden kann. Daher sollte jeder Benutzer vor der Nutzung von Internet-Diensten durch entsprechende Anweisungen verpflichtet werden, die aufgeführten Sicherheitsrichtlinien zu beachten. Es empfiehlt sich vor der Zulassung von Benutzern zu Internet-Diensten diese auf eine Benutzerordnung zu verpflichten. Die Inhalte der Internet-Sicherheitsrichtlinie und der Benutzerordnung sind in einer Schulung den Benutzern darzulegen. In dieser Benutzerordnung sollten die zur Verfügung stehenden Kommunikationsdienste kurz erläutert und alle relevanten Regelungen aufgeführt werden. Jeder Benutzer sollte durch Unterschrift bestätigen, daß die dargestellten Regelungen zur Kenntnis genommen wurden und bei Benutzung der Kommunikationsdienste beachtet werden.

Es sollte jeder Benutzer darauf hingewiesen werden, daß die Nutzung von Internetdiensten mit nicht unerheblichen Kosten verbunden ist. Dementsprechend sollte darauf geachtet werden, im Internet gesammelte Informationen den anderen Mitarbeitern zur Verfügung zu stellen, um wiederholte Zugriffe auf dieselben externen WWW-Seiten zu vermeiden. Dafür sollte im internen Netz ein spezieller Bereich vorgesehen werden, in dem solche Informationen strukturiert abgelegt werden können.
Weiterhin müssen die Benutzer darauf hingewiesen werden, daß

- die Konfiguration der WWW-Programme nicht eigenmächtig geändert werden darf,
- welche Daten protokolliert werden,

- wer Ansprechpartner bei Sicherheitsproblemen sind.

M 5.46 Einsatz von Stand-alone-Systemen zur Nutzung des Internets
Um die Gefährdungen, die durch Angriffe aus dem Internet auf lokale Daten oder Rechner im LAN entstehen, zu verringern, ist es sinnvoll Rechner einzusetzen, die nur mit dem Internet vernetzt sind und keine weitere Netzverbindung zu einem LAN haben.
Hierfür bieten die verschiedenen Betriebssysteme unterschiedliche Möglichkeiten mit jeweils spezifischen Gefährdungen für die Vertraulichkeit und Integrität der Daten auf diesem Rechner.
Wichtig ist es zu beachten, daß bei der Installation der Internet-Zugangssoftware keine unnötigen Programme installiert werden. So gibt es bei einigen Produkten und Betriebssystemen die Möglichkeiten, durch die Installation von Server-Programmen den Rechner zu einem vollständigen Internet-Server zu machen. Die Installation der TCP/IP-Software bietet eine vollständige bidirektionale Verbindung zum Internet, über die Daten sowohl ins Internet geschickt als auch von dort abgeholt werden können.
Beispielsweise muß unter Unix darauf geachtet werden, daß keine Daemon-Prozesse gestartet werden. Dies geschieht normalerweise beim Booten oder mit Hilfe des inetd. Die entsprechenden Einträge müssen aus den Konfigurationsdateien (rc.* und inetd.conf) entfernt werden. Die Software (PPP, SLIP) muß so installiert werden, daß kein Verbindungsaufbau vom Internet aus möglich ist.

M 5.47 Einrichten einer Closed User Group
Das Integrated Services Digital Network (ISDN) ermöglicht die Einrichtung einer geschlossenen Benutzergruppe (GBG), auch als Closed User Group (CUG) bezeichnet. Merkmal einer solchen Gruppe ist, daß alle Teilnehmer einer CUG untereinander über das öffentliche ISDN kommunizieren können, Verbindungswünsche von außerhalb der CUG an CUG-Teilnehmer jedoch genauso abgewiesen werden wie Verbindungswünsche von CUG-Teilnehmer an Teilnehmer des öffentlichen ISDN.

Funktionsweise:
Alle Kommunikationspartner sind Mitglied in einer Closed User Group des Netzbetreibers (z. B. Deutsche Telekom AG). Die Berechtigungsprüfung zur Kommunikation erfolgt über den einer CUG eindeutig zugeordneten Interlock Code durch die jeweilige digitale Vermittlungsstelle (DIV) der Kommunikationspartner. Zu Beginn übermittelt der rufende Kommunikationspartner eine Verbindungsanforderung an die ihm zugeordnete DIV. Die DIV fügt der Verbindungsanforderung nicht nur die ISDN-Rufnummer des rufenden Kommunikationspartners, sondern auch den eindeutigen Interlock Code der entsprechenden Closed User Group hinzu. Die DIV des gerufenen Kommunikationspartners erkennt anhand des Interlock Codes, ob der Verbindungsanforderung stattgegeben werden kann. Ist die Identifikation erfolgreich, wird der Verbindungswunsch an den gerufenen Kommunikationspartner weiter vermittelt.
Vorteilhaft an der beschriebenen Funktionalität ist, daß unerlaubte Zugriffsversuche bereits von der DIV des Netzbetreibers abgewiesen werden und nicht bis zu Netzkoppelelementen eines Kommunikationspartners gelangen.

Nachteilig ist, daß Änderungen der Mitgliedschaft in einer CUG immer dem Netzbetreiber mitgeteilt werden müssen, da nur dieser die notwendigen Berechtigungsänderungen durchführen kann. Weiterhin bedeutet dies auch, daß der Netzbetreiber die vollständige Kontrolle über die Mitgliedschaft in einer CUG besitzt und von ihm vorgenommene Änderungen durch den Nutzer einer CUG nicht kontrolliert werden können. Hingewiesen werden soll ebenfalls darauf, daß sowohl für das Einrichten als auch für den Betrieb einer CUG durch einen Netzbetreiber einmalige und fortlaufende Kosten entstehen.
Das Einrichten einer Closed User Group durch den Betreiber eines öffentlichen Netzes empfiehlt sich immer dann, wenn

- Hard- und Software für andere Verfahren (z.B. M 5.48 - Authentisieren mittels CLIP/COLP) erst beschafft werden müßte,
- die Mitglieder einer CUG nur selten wechseln und
- der Netzbetreiber ausreichend vertrauenswürdig ist.

M 5.48 Authentisieren mittels CLIP/COLP
Das Integrated Services Digital Network (ISDN) liefert die Möglichkeit, Rufnummern von Teilnehmern nicht nur für die öffentlichen Vermittlungskomponenten, sondern auch direkt für die beteiligten Kommunikationspartner zu signalisieren. Diese ISDN-Leistungsmerkmale bezeichnet man als

- CLIP = Calling Line Identification Presentation und
- COLP = Connected Line Identification Presentation oder allgemeiner als
- Rufnummernanzeige.

Die Auswertung der Rufnummernangabe kann von den jeweiligen Kommunikationspartnern zur Authentisierung genutzt werden.

Funktionsweise:
In einem ersten Schritt wird seitens des rufenden Kommunikationspartners eine Verbindungsanforderung an die ihm zugeordnete digitale Vermittlungsstelle (DIV) abgesetzt. Die DIV vermittelt die Verbindungsanforderung an den zu rufenden Kommunikationspartner innerhalb des ISDN incl. der Rufnummer des rufenden Kommunikationspartners. Die gegenüberliegende DIV vermittelt anschließend den Verbindungswunsch an die ISDN-Kommunikationseinrichtung des gewünschten Kommunikationspartners. Anhand der übermittelten Rufnummer kann diese Kommunikationseinrichtung (z.B. ein ISDN-Router oder eine TK-Anlage) den rufenden Kommunikationspartner identifizieren (CLIP). Bei erfolgreicher Identifikation wird der Verbindungswunsch angenommen und der Datenaustausch kann beginnen.
Vorteilhaft an der beschriebenen Funtionalität ist, daß die Identifikation durch Komponenten der jeweiligen Kommunikationspartner (ISDN-Router, TK-Anlage) durchgeführt wird und somit vollständig in deren Kontrollbereich liegt.

Nachteilig ist, daß die über den ISDN-D-Kanal übertragenen Rufnummern grundsätzlich manipulierbar sind (siehe G 5.63 - Manipulationen über den ISDN-D-Kanal). Eine einfache Authentisierung durch die übermittelte Rufnummer ist somit entweder nur in Zusammenhang mit dem Einsatz einer Callback-Funktion (siehe M 5.49 - Callback basierend auf CLIP/COLP) oder in Kombination mit dem Einsatz eines D-Kanal-Filters (siehe M 4.62 - Einsatz eines D-Kanal-Filters), das Protokollmanipulationen aufdeckt, möglich.

M 5.49 Callback basierend auf CLIP/COLP

Viele Kommunikationskarten bieten die Option automatischer Rückruf (Callback). Ist diese Option aktiviert, trennt die Kommunikationskarte, wenn sie einen Anruf erhält, sofort nach dem erfolgreichen Verbindungsaufbau die Verbindung und ruft eine voreingestellte Nummer zurück. Dadurch wird verhindert, daß ein nicht autorisierter Anrufer diesen Fernzugang mißbrauchen kann, solange er nicht unter der voreingestellten Nummer erreichbar ist. Callback ist immer dann einzusetzen, wenn ein fester Kommunikationspartner sich automatisch einwählen können soll. Zu beachten ist, daß mit dem automatischen Rückruf auch die Kosten der Datenübertragung übernommen werden.

Mit Hilfe des ISDN ist eine Variante des Callback zu einer festen Rufnummer möglich: Die angesprochene ISDN-Karte prüft mit Hilfe des ISDN-Leistungsmerkmals Calling Line Identification Presentation (CLIP), von welcher Stelle aus die Verbindungsanforderung erfolgte, und vergleicht die übermittelte Rufnummer mit einer Rufnummerntabelle. Wurde über CLIP eine gültige Rufnummer übermittelt, wird die in der Rufnummerntabelle hinterlegte Rufnummer zurückgerufen.

Vorteilhaft ist gegenüber der ausschließlichen Authentisierung über CLIP/COLP (s. M 5.48 - Authentisieren mittels CLIP/COLP), daß selbst beim Vorspiegeln einer autorisierten Rufnummer von einem nicht autorisierten Teilnehmer aus keine Verbindung zustande kommt, da der nicht autorisierte Teilnehmer tatsächlich ja nicht unter der vorgegebenen Rückrufnummer erreichbar ist.

M 5.50 Authentisierung mittels PAP/CHAP

Viele ISDN-Karten unterstützen die Kommunikation über das Point-to-Point Protocol (RFC 1661), nachdem eine ISDN-Wählverbindung aufgebaut wurde. Innerhalb dieses Internet-Standards werden auch Authentisierungsprotokolle, wie das Password Authentication Protocol (PAP) und das Challenge Handshake Authentication Protocol (CHAP) angeboten (RFC 1994). Bietet die verwendete ISDN-Karte diese Funktionalitäten, sollte zur Authentisierung anstelle des Password Authentication Protocols das Challenge-Handshake Authentication Protocol genutzt werden, da bei PAP das zur Authentisierung verwendete Paßwort unverschlüsselt übertragen wird.

Die bei PAP bzw. CHAP verwendeten Paßwörter werden i. allg. nicht bei jeder Authentisierung vom Benutzer erneut eingegeben, sondern in den IT-Systemen gespeichert. Damit sich diese Verfahren auch nach einer erneuten Installation wieder aufsetzen lassen, sollten die benötigten Paßwörter notiert und sicher verwahrt werden (siehe M 2.22 - Hinterlegen des Paßwortes).

Funktionsweise:
Bei CHAP werden grundsätzlich zwei Kommunikationspartner unterschieden: Authenticator und Peer. Dabei handelt es sich beim Authenticator um den Kommunikationspartner, der die Authentisierung abfordert, und beim Peer um den Kommunikationspartner, der die Authentisierung erbringen soll. Im allgemeinen wird also der Authenticator der Server sein, an dem sich der Benutzer von seinem IT-System aus als Peer anmelden will.
Bei CHAP wird auf beiden Seiten die Kenntnis eines gemeinsamen Geheimnisses (Paßwort) überprüft. Dabei wird das Geheimnis nicht im Klartext über die Leitung gesandt und durch die Einbindung von Zufallszahlen vor Wiedereinspielen geschützt.

Das eingesetzte Challenge-Response-Protokoll läuft wie folgt ab:
In einem ersten Schritt errechnet der Authenticator eine Zufallszahl. Mittels eines Hash-Algorithmus wird der Hash-Wert der eben berechneten Zufallszahl gebildet. Eine Hash-Funktion ist eine Rechenvorschrift, durch die eine Eingabe beliebiger Länge in einen Ausgabewert fester (i.a. kürzerer) Länge umgewandelt wird. Eine Einweg-Hashfunktion funktioniert nur in eine Richtung, d.h. aus der Eingabe läßt sich problemlos der Hashwert berechnen, aber es sollte sehr schwer bis unmöglich sein, zu einem Hashwert passende Eingabedaten zu berechnen.
Im nächsten Schritt überträgt der Authenticator das sogenannte Challenge, also die eben errechnete Zufallszahl, an den Peer. Da Authenticator und Peer über den gleichen Hash-Algorithmus verfügen, kann in einem vierten Schritt ebenfalls der Peer den Hash-Wert der eben übermittelten Zufallszahl bilden. Der Peer berechnet den Hashwert über die drei Werte Identifier (Benutzerkennung), Secret (Paßwort) und der gesendeten Zufallszahl. Den Hashwert überträgt er dann als Antwort an den Authenticator. Der Authenticator überprüft die Korrektheit des Paßworts, indem er ebenfalls den entsprechenden Hashwert berechnet und mit dem übermittelten Hash-Wert vergleicht. Fällt der Vergleich positiv aus, hat sich der Peer gegenüber dem Authenticator authentisiert und die Kommunikationsverbindung kann aufgebaut werden.
Die Authentisierung nach dem eben beschriebenen Verfahren sollte auch während einer bestehenden Kommunikationsverbindung mehrfach wiederholt werden, um auch Attacken auf bereits bestehende Verbindungen zu verhindern. Dies wird, ohne das der Benutzer eingreifen muß, in zufälligen Zeitabständen durch den Authenticator angestoßen.

M 5.53 Schutz vor Mailbomben
Mailbomben sind E-Mails, die absichtlich eingebaute Schadfunktionen enthalten. Als Mailbombe kann sich beispielsweise eine als Anlage mitversandte komprimierte Datei erweisen, die nach dem Auspacken Unmengen von Unterverzeichnissen anlegt oder sehr viel Festplattenplatz beansprucht. Archive, also mit Packprogrammen komprimierte Dateien, sollten niemals ohne vorhergehende Prüfung ausgepackt werden. Um sich vor trojanischen Pferden oder anderen Schadfunktionen in komprimierten Dateien zu schützen, sollte man sich vor dem Auspacken solcher Dateien das Inhaltsverzeichnis über die archivierten Dateien und deren Größe anzeigen lassen. Weiterhin sollten Archivdateien bereits vor dem Auspacken auf Computer-Viren überprüft werden.
Auf Arbeitsplatzrechnern sollten selbstextrahierende Archive, also solche mit Endungen wie *.EXE, niemals aufgerufen werden, da vor dem Auspacken der Inhalt nicht geprüft kann.

Neue Programme sollten immer zunächst auf von den Produktionssystemen getrennten IT-Systemen getestet werden (siehe M 4.65 - Test neuer Hard- und Software). Bei Unix-Systemen und anderen Server-Betriebssystemen sind außerdem folgende Punkte zu beachten:

- Unbekannte Archive dürfen nie unter Superuser-Berechtigung ausgepackt werden, sondern nur unter einer Benutzerkennung mit möglichst wenig Schreibrechten.
- Es sollte ein Filesystem mit Disk-Quota verwendet werden, um den Festplattenplatz zu begrenzen, den ein solches Programm im schlimmsten Fall belegen kann.

M 5.54 Schutz vor Mailüberlastung und Spam
Durch die Überhäufung mit Werbemails oder durch absichtliche Überlastung durch eingehende E-Mails kann nicht nur das Mailsystem blockiert werden, sondern kann auch für den Empfänger solcher E-Mail teuer werden. Um sich vor SSpam", d.h. inhaltsleeren Mailings, zu schützen, sollte jeder Benutzer überlegen, wann und an wen er seine E-Mail-Adresse weitergibt.
Mögliche Maßnahmen gegen Werbemails bzw. SSpamßind die folgenden:

- Es können Anonyme-Remailer-Dienste benutzt werden, also ein Server, der E-Mail entpersonalisiert. Ein Remailer ermöglicht es, in eine Newsgruppe zu posten oder eine E-Mail zu versenden, ohne daß der Empfänger die E-Mail-Adresse des Absenders erkennen kann. Dies hat allerdings den Nachteil, daß häufig andere Personen den E-Mail-Kontakt verweigern, weil sie den Absender nicht identifizieren können.
- Auf dem Mailserver bzw. der Firewall sollten E-Mail-Filterprogramme eingesetzt werden, die nur E-Mails von und/oder zu definierten Kommunikationspartnern zulassen oder über andere Header-Einträge versuchen, Spam auszugrenzen. Hierbei muß mit Bedacht vorgegangen werden, damit der Filterung keine erwünschten E-Mails zum Opfer fallen.
- Jede Organisation sollte festlegen, ob ihre Mitarbeiter Artikel in Newsgruppen posten dürfen und wenn ja, in welcher Form und zu welchen Themen. Dabei sind die Benutzer darauf hinzuweisen, daß die Netiquette zu beachten ist, insbesondere ist die Verbreitung von für die Allgemeinheit irrelevanten Informationen zu unterlassen.
- Es kann u.U. sinnvoll sein, keine leicht erratbaren E-Mail-Adressen zu verwenden (siehe auch M 2.122 - Einheitliche E-Mail-Adressen).
- Auf keinen Fall sollte versucht werden, Spam-Verursacher durch Mailbomben oder ähnliches zu bestrafen. Spam sollte nicht einmal durch ein Reply beantwortet werden. Häufig sind die Absenderangaben in Spam-Mail gefälscht. Antworten erreichen dann nur Unschuldige oder kommen als unzustellbar zurück. Auf jeden Fall verursachen auch Antworten wiederum ein erhöhtes Netzaufkommen und im schlimmsten Fall bestätigen sie Werbemailern sogar noch die Korrektheit angeschriebener E-Mail-Adressen.
- Eine wirkungsvolle Maßnahme gegen akute Belästigung durch Spam ist die Benachrichtigung des eigenen Mail-Providers sowie des Mail-Providers des Verursachers, damit diese gegen den Verursacher vorgehen können.

Dabei ist zu beachten, daß nicht alle dieser Maßnahmen in allen Umgebungen sinnvoll sind, weil sie diverse Einschränkungen mit sich bringen. So kann es einerseits sinnvoll sein, nicht aus den Benutzernamen abgeleitete E-Mail-Adressen zu verwenden, um sich vor unerwünschten Werbemails zu schützen. Andererseits können abstrakte E-Mail-Adressen die Kommunikation mit Externen erschweren, da sie schwerer zu merken sind. Die Form der E-Mail-Adressen muß auf jeden Fall den organisationsinternen Regelungen genügen.
Durch die Eintragung auf Mailinglisten kann ebenfalls eine hohe Mailbelastung entstehen. Generell sollte regelmäßig überprüft werden, ob die in einer Mailingliste diskutierten Inhalte das Lesen lohnen, sonst ist sie abzubestellen. Die Benutzer müssen darüber informiert sein, daß nach der Eintragung auf Mailinglisten die dadurch entstehende Mailbelastung regelmäßig, d.h. möglichst täglich, zu kontrollieren ist. In größeren Organisationen sollten für die Arbeit interessante Mailinglisten nur über einen Mitarbeiter (z.B. den Mail-Administrator) abonniert werden und dann zentral allen zur Verfügung gestellt werden.

M 5.55 Kontrolle von Alias-Dateien und Verteilerlisten
Um die Adressierung von E-Mails zu vereinfachen, werden häufig Alias-Dateien oder Verteilerlisten geführt. Werden sowohl auf den Mailservern als auch auf den Mailclients Alias-Dateien geführt, ist zunächst zu klären, welche Einträge Priorität haben, d.h. ob bei gleicher Wahl eines Alias der vom Mailserver oder der vom Mailclient akzeptiert wird. Beim Empfang von E-Mails sollte die Alias-Umsetzung des Mailservers ausschlaggebend sein, beim Versand die des Mailclients. Die Benutzer müssen darüber informiert sein, welche Aliase auf dem Mailserver aufgelöst werden, damit sie dies bei der Weitergabe von E-Mail-Adressen berücksichtigen können.
Damit die Benutzer die Alias-Dateien auf dem Mailserver verwenden können, müssen sie lesend darauf zugreifen können. Schreibrecht darauf sollte aber nur der Mail-Administrator haben.
Um zu verhindern, daß E-Mails aufgrund fehlerhafter, nicht aktueller oder manipulierter Verteilerlisten an falsche Empfänger übertragen werden, müssen die Verteilerlisten regelmäßig auf Korrektheit und Aktualität überprüft werden.

M 5.56 Sicherer Betrieb eines Mailservers
Der sichere Betrieb eines Mailservers setzt voraus, daß sowohl die lokale Kommunikation als auch die Kommunikation auf Seiten des öffentlichen Netzes abgesichert wird. Der Mailserver nimmt von anderen Mailservern E-Mails entgegen und leitet sie an die angeschlossenen Benutzer oder Mailserver weiter. Weiterhin reicht der Mailserver die gesendete E-Mails lokaler Benutzer an externe Mailserver weiter. Der Mailserver muß hierbei sicherstellen, daß lokale E-Mails der angeschlossenen Benutzer nur intern weitergeleitet werden und nicht in das öffentliche Netz gelangen können. Ein Mailserver speichert die E-Mail bis zur Weitergabe zwischen. Viele Internetprovider und Administratoren archivieren zusätzlich die ein- und ausgehenden E-Mails. Damit Unbefugte nicht über den Mailserver auf Nachrichteninhalte zugreifen können, muß der Mailserver gegen unbefugten Zugriff gesichert sein. Dafür sollte er gesichert (in einem Serverraum oder Serverschrank) aufgestellt sein. Für den ordnungsgemäßen Betrieb sind ein Administrator und Stellvertreter zu benennen und zum Betrieb des Mailservers und dem zugrundeliegenden Betriebssystems zu schulen. Es muß ein Postmaster-Account eingerichtet werden, an den alle unzustellbaren E-Mails und alle Fehlermeldungen weitergeleitet werden

(siehe auch M 2.120 - Einrichtung einer Poststelle).
Auf die Mailboxen der der lokal angeschlossenen Benutzer dürfen nur diese Zugriff haben. Auf die Bereiche, in denen E-Mails nur temporär für die Weiterleitung zwischengespeichert werden (z.B. Spooldateien), ist der Zugriff auch für die lokalen Benutzer zu unterbinden. Es muß regelmäßig kontrolliert werden, ob die Verbindung mit den benachbarten Mailservern, insbesondere dem Mailserver des Mail-Providers, noch stabil ist. Es muß regelmäßig überprüft werden, ob der für die Zwischenspeicherung der Mail zur Verfügung stehende Plattenplatz noch ausreicht, da ansonsten kein weiterer Nachrichtenaustausch möglich ist.
Umfang und Inhalt der Protokollierung der Aktivitäten des Mail-Servers sind festzulegen.
Der Mailserver sollte nie ein Produktionssystem sein, insbesondere sollten von der Verfügbarkeit des Mailservers keine weiteren Dienste abhängig sein. Es sollte jederzeit kurzfristig möglich sein, ihn abzuschalten, z.B. bei Denial-of-Service-Angriffen oder bei Verdacht auf Manipulationen. Die Benutzernamen auf dem Mailserver sollten nicht aus den E-Mail-Adressen unmittelbar ableitbar sein, um mögliche Angriffe auf Benutzer-Accounts zu erschweren.
Eingehende E-Mails sollten am Firewall oder am Mailserver auf Computer-Viren und andere schädliche Inhalte wie aktive Inhalte (z.B. Java-Applets) überprüft werden.
Über Filterregeln können für bestimmte E-Mail-Adressen der Empfang oder die Weiterleitung von E-Mails gesperrt werden. Dies kann z.B. sinnvoll sein, um sich vor Spam-Mail zu schützen. Auch über die Filterung anderer Header-Einträge kann versucht werden, Spam auszugrenzen. Hierbei muß mit Bedacht vorgegangen werden, damit der Filterung keine erwünschten E-Mails zum Opfer fallen. Daher sollten entsprechende Filterregeln sehr genau definiert werden, indem beispielsweise aus jeder Spammail eine neue dedizierte Filterregel abgeleitet wird. Entsprechende Filterlisten sind im Internet verfügbar bzw. können von verschiedenen Herstellern der Kommunikationssoftware bezogen werden.
Es ist festzulegen, welche Protokolle und Dienste am Mailserver erlaubt sind, beispielsweise ist es sinnvoll, SMTP (TCP-Port 25) nach außen und innen, aber POP3 nur innerhalb zuzulassen.
Ein Mailserver sollte davor geschützt werden, als Spam-Relay verwendet zu werden. Dafür sollte ein Mailserver so konfiguriert werden, daß er E-Mails nur für die Organisation selber entgegennimmt und nur E-Mails verschickt, die von Mitarbeitern der Organisation stammen. Der Mailserver sollte eingehende E-Mails nur dann annehmen, wenn entweder die IP-Adresse des absendenden Mailservers in einem vom Administrator explizit zugelassenen IP-Netz liegt oder für den Empfänger ein MX-Eintrag auf den Mailserver zeigt. Alle anderen E-Mails werden mit einer Fehlermeldung abgewiesen. BerechtigteBenutzer können trotz dieser Maßnahmen weiterhin E-Mails an beliebige Empfänger versenden, ebenso können sie E-Mails von beliebigen Absendern empfangen. Durch die oben beschriebene Filterung eingehender E-Mails wird jedoch verhindert, daß der Mailserver von externen Nutzern als Spam-Relay mißbraucht werden kann.
Sollten versehentlich IP-Netze, aus denen E-Mails angenommen werden sollen, nicht in obiger Liste stehen, muß der Administrator des Mailservers davon in Kenntnis gesetzt werden, damit er diese nachtragen kann.
Wenn eine Organisation keinen eigenen Mailserver betreibt, sondern über einen oder mehrere Mailclients direkt auf den Mailserver eines Providers zugreift, sollte mit dem Provider abgeklärt werden, welche Regelungen dort gelten und welche Sicherheitsmaßnahmen ergriffen worden sind

(siehe M 2.123 - Auswahl eines Mailproviders).

M 5.57 Sichere Konfiguration der Mailclients
Die E-Mail-Progamme der Benutzer müssen durch den Administrator so vorkonfiguriert sein, daß ohne weiteres Zutun der Benutzer maximale Sicherheit erreicht werden kann. Die Benutzer sind darauf hinzuweisen, daß sie die Konfiguration nicht selbsttätig ändern dürfen.
Insbesondere die folgenden Punkte sollten bei der Konfiguration der E-Mail-Clients berücksichtigt werden:

- Das E-Mail-Paßwort darf keinesfalls dauerhaft vom E-Mail-Programm gespeichert werden. Dabei wird das Paßwort auf der Client-Festplatte abgelegt, u.U. sogar im Klartext oder nur schwach verschlüsselt. Jeder, der Zugriff auf den Mailclient hat, hat so die Möglichkeit, unter fremden Namen E-Mails zu verschicken bzw. das E-Mail-Paßwort auszulesen.

- Als Reply-Adresse ist die E-Mail-Adresse des Benutzers einzustellen, um sicherzustellen, daß keine internen E-Mail-Adressen weitergegeben werden.

- Um die Netzbelastung niedrig zu halten, sollte der Mailclient nicht zu häufig den Mailserver auf neu eingetroffene Nachrichten überprüfen. Ein automatischer Abholversuch alle 30 Minuten (= 1800 Sekunden) wird als Standardwert empfohlen und ist im allgemeinen ausreichend. Sollten Benutzer eine dringende Nachricht erwarten, sollten sie das E-Mail-Programm manuell dazu veranlassen, in ihrer Mailbox nachzusehen.

- Nachrichten, die vom Mailserver abgeholt wurden, sollten dort auch gelöscht werden. So kann ein mehrmaliges Abholen derselben Nachrichten verhindert und Speicherprobleme am Mailserver vermieden werden.

M 5.58 Installation von ODBC-Treibern
ODBC (Open Database Connectivity) legt zwischen Datenbankanwendungen und dem jeweiligen Datenbankprotokoll eine zusätzliche Schicht (und ist somit kein eigenes Datenbankprotokoll). Durch die Installation des zur Datenbank passenden ODBC-Treibers wird zwischen Anwendung und Datenbank eine einheitliche Schnittstelle geschaffen, über die die Kommunikation (Absetzen von Datenbankanfragen, Lesen von Daten) zur Datenbank abgewickelt wird. Die zugehörige ANSI-SQL-konforme SQL-Schnittstelle ermöglicht das Erstellen von Anwendungen, ohne auf die jeweiligen Datenbankspezifika unterschiedlicher Produkte Rücksicht nehmen zu müssen. Bei einem Wechsel der Datenbank-Software muß deshalb die Anwendung nicht angepaßt werden, sondern es reicht aus, den ODBC-Treiber auszutauschen. Ursprünglich für Microsoft-Produkte entwickelt, hat sich ODBC inzwischen als Standard etabliert. ODBC-Treiber sind für alle gängigen Datenbanken unterschiedlichster Hersteller erhältlich.
Bei der Installation von ODBC-Treibern ist darauf zu achten, daß keine Sicherheitslücken hinsichtlich der Zugangskontrolle zum Datenbanksystem entstehen.

Beispiel:
Für MS Access Datenbanken ist die Verwendung von Benutzerkennungen optional. Wird allerdings die Zugangskontrolle aktiviert, so werden die Benutzerkennungen über eine separate

MS Access Datenbank, die sogenannte Systemdb verwaltet, die auch als eigene Datei abgespeichert wird.
Bei der Installation eines ODBC-Treibers für eine MS Access Datenbank wird die Systemdb nicht automatisch integriert. Die Default-Einstellungen während der Installation sind nämlich dergestalt, daß eine eventuell existierende Systemdb unberücksichtigt bleibt. Wurde also während der Installation des ODBC-Treibers die Systemdb nicht explizit angegeben, so führt dies dazu, daß für Datenbankabfragen mittels ODBC keine Identifizierung seitens der Systemdb gefordert wird. Somit wird die Zugangskontrolle unterlaufen.
Um dies zu verhindern, kann regelmäßig geprüft werden, ob die Systemdb integriert ist. Da dieser Mechanismus jedoch jederzeit wieder rückgängig gemacht bzw. manipuliert werden kann, ist eine Verschlüsselung einer MS Access Datenbank die sicherere Lösung. In diesem Fall schlägt ein Zugriff ohne die Systemdb immer fehl. Dafür muß die in MS Access integrierte Verschlüsselung aktiviert werden (unter Extras/Zugriffsrechte/Datenbank ver-/entschlüsseln). In diesem Fall schlägt ein Zugriff über die ODBC-Schnittstelle fehl, da die Systemdb auch für den Verschlüsselungsmechanismus benötigt wird.

M 5.59 Schutz vor DNS-Spoofing
Gefahr durch DNS-Spoofing besteht dann, wenn eine Authentisierung anhand eines Rechnernamens durchgeführt wird. Eine hostbasierte Authentisierung, d.h. Rechte werden anhand eines Rechnernamens oder IP-Adresse gewährt, sollte durch eine der drei folgenden Konfigurationen (auch in Kombination) abgesichert werden:

1. Es sollten IP-Adressen, keine Hostnamen verwendet werden.

2. Wenn Hostnamen verwendet werden, sollten alle Namen lokal aufgelöst werden (Einträge in der /etc/hosts).

3. Wenn Hostnamen verwendet werden, sollten alle Namen direkt von einem Nameserver aufgelöst werden, der für diese Namen der sogenannte Primary- oder Secondary-Nameserver ist, d. h. er hat sie nicht in einem temporären Cache, sondern dauerhaft abgespeichert.

Das Ziel obiger Konfigurationen ist es, die Zuordnung zwischen IP-Adressen und Rechnernamen in einem sicheren Umfeld vorzunehmen. Auf keinen Fall sollte ein hostbasierter Zugang über einen Hostnamen gewährt werden, wenn die Namensauflösung nicht direkt ausgeführt werden kann, also ein Cache zwischengeschaltet ist.

H.6 Maßnahmenkatalog Notfallvorsorge

M 6.1 Erstellung einer Übersicht über Verfügbarkeitsanforderungen
Für die in einem IT-System betriebenen IT-Anwendungen und deren Daten sind die Verfügbarkeitsanforderungen festzustellen. Da eine IT-Anwendung nicht zwingend jeden Bestandteil des IT-Systems benötigt, sind die Verfügbarkeitsanforderungen der IT-Anwendungen auf die

wesentlichen Komponenten des IT-Systems abzubilden. Das Ergebnis dieser Arbeit kann in Form einer Übersicht mit folgenden Inhalten dargestellt werden:

Tabelle H.1: Übersicht über Vefügbarkeitsanforderungen

IT-System	IT-Komponente	IT-Anwendung	tolerierbare Ausfallzeit
Zentralsystem	Host	Reisekosten	5 Arbeitstage
		Buchhaltung	3 Stunden
	DFÜ	E-Mail	3 Arbeitstage
		Buchhaltung	1 Arbeitstag
	Drucker	Reisekosten	10 Arbeitstage
		Buchhaltung	2 Arbeitstage
		Einsatzplanung	1 Arbeitstag
LAN	Server	Datenerfassung	1 Arbeitstag
		Leitstelle	4 Stunden
	PC	Datenerfassung	10 Arbeitstage
	PC	Leitstelle	4 Stunden

(Lesart: Die IT-Komponente Host im IT-System „Zentralsystem“ hat aufgrund der IT-Anwendung „Buchhaltung“ eine maximal tolerierbare Ausfallzeit von 3 Stunden.)

Eine praktikable Vorgehensweise ist es, zu den einzelnen IT-Anwendungen den Verfahrensverantwortlichen nach den tolerierbaren Ausfallzeiten der benutzten IT-Komponenten zu befragen, um danach die Ergebnisse nach IT-System und Komponenten geordnet in der Tabelle aufzuführen.
Die Übersicht erleichtert es, die besonders zeitkritischen Komponenten des IT-Systems zu extrahieren, für die die Notfallvorsorge unumgänglich ist. Bei Ausfall einer Komponente gibt diese Übersicht darüber hinaus Auskunft über die betroffenen IT-Anwendungen und deren Verfügbarkeitsanforderungen. Die Anforderungen an die Verfügbarkeit sind von den Anwendern bzw. Fachabteilungen zu begründen, sofern dies nicht schon an anderer Stelle geschehen ist. Die Verfügbarkeitsanforderungen sind von der Behörden- bzw. Unternehmensleitung zu bestätigen.
Bei Ausfall einer Komponente des IT-Systems ermöglicht diese Übersicht eine schnelle Aussage, ab wann ein Notfall vorliegt. Daß ein Notfall auch bei Ausfall einer besonders zeitkritischen Komponente nicht zwingend eintreten muß, läßt sich anhand des Ersatzbeschaffungsplans (siehe M 6.14 - Ersatzbeschaffungsplan) und der Untersuchung über interne und externe Ausweichmöglichkeiten (siehe M 6.6 - Untersuchung interner und externer Ausweichmöglichkeiten) ermitteln.

M 6.2 Notfall-Definition, Notfall-Verantwortlicher

Nicht jeder Teil- oder Gesamtausfall des Systems stellt jedoch einen Notfall dar. Oftmals lassen sich Ausfälle des IT-Systems durch geplante Maßnahmen, z.B. Ersatzbeschaffung, auch in kurzer Zeit beheben. Der Notfall tritt erst dann ein, wenn ein Zustand erreicht wird, bei dem innerhalb der geforderten Zeit eine Wiederherstellung der Verfügbarkeit (siehe M 6.1 - Erstellung einer Übersicht über Verfügbarkeitsanforderungen) nicht möglich ist und sich daraus ein sehr hoher Schaden ergibt. Schon bei Eintritt eines Ereignisses, in dessen Folge der Notfall

entstehen könnte, sind die erforderlichen Maßnahmen zu ergreifen, die zu einer Schadensreduzierung führen.
Für die autorisierte und rechtzeitige Einleitung von Notfallmaßnahmen bedarf es der Benennung eines Notfall-Verantwortlichen. Die Behörden- bzw. Unternehmensleitung muß den Notfall-Verantwortlichen sowohl für die Entscheidung autorisieren, ob ein Notfall eingetreten ist, als auch für die Einleitung erforderlicher Notfallmaßnahmen.

M 6.3 Erstellung eines Notfall-Handbuches
In einem Notfall-Handbuch sind alle Maßnahmen, die nach Eintritt eines notfallauslösenden Ereignisses zu ergreifen sind, und alle dazu erforderlichen Informationen zu dokumentieren. Das Notfall-Handbuch ist so zu gestalten, daß ein sachverständiger Dritter in der Lage ist, die im Handbuch spezifizierten Notfallmaßnahmen durchzuführen.

Nachfolgend wird beispielhaft ein umfassendes Inhaltsverzeichnis eines Notfall-Handbuches zur Orientierung aufgeführt. Welche Teile dieses Vorschlags übernommen werden können, ist abhängig von der vorhandenen System- und Anwendungsdokumentation und kann daher nur individuell entschieden werden.

Inhaltsverzeichnis Notfall-Handbuch

Teil A: Sofortmaßnahmen

1 Alarmierung im Notfall
1.1 Alarmierungsplan und Meldewege
1.2 Adresslisten betroffener Mitarbeiter
1.3 Festlegung konkreter Aufgaben für einzelne Personen/Funktionen im Notfall
1.4 Notrufnummern
(z.B. Feuerwehr, Polizei, Notarzt, Wasser- und Stromversorger, Ausweichrechenzentrum, externes Datenträgerarchiv, externe Telekommunikationsanbieter)
2 Handlungsanweisung für spezielle Ereignisse
2.1 Brand
2.2 Wassereinbruch
2.3 Stromausfall
2.4 Ausfall der Klimaanlage
2.5 Explosion
2.6 Sabotage
2.7 Ausfall der Datenfernübertragungseinrichtung
2.8 Einbruch
2.9 Vandalismus
2.10 Bombendrohung
2.11 Streik / Demonstrationen

2.12 .....
Teil B: Regelungen für den Notfall
3 Allgemeine Regelungen
3.1 Notfall-Verantwortliche
3.2 Benennung der an der Durchführung der Notfallpläne beteiligten Organisationseinheiten, Kompetenzverteilung
3.3 Organisationsrichtlinien, Verhaltensregeln
4 Tabelle der Verfügbarkeitsanforderungen
Teil C: Wiederanlaufpläne für kritische Komponenten
5 Wiederanlauf-Planung
5.1 Wiederanlauf-Plan für Komponente 1 (z.B. Host)
5.1.1 Wiederbeschaffungsmöglichkeiten
5.1.2 Interne / externe Ausweichmöglichkeiten
5.1.3 DFÜ-Versorgung
5.1.4 Eingeschränkter IT-Betrieb
5.1.5 Wiederanlaufreihenfolge
5.2 Wiederanlauf-Plan für Komponente 2 (z.B. Drucker)
...
Teil D: Dokumentation
6 Beschreibung der IT-Systeme
6.1 Beschreibung des IT-Systems A (im Überblick)
6.1.1 Beschreibung der Hardware-Komponenten
6.1.2 Beschreibung der Software-Komponenten
6.1.2.1 Bestandsverzeichnis der Systemsoftware
6.1.2.2 Bestandsverzeichnis der zu dem IT-System gehörenden Systemdaten
6.1.3 Beschreibung der Netzanbindungen des IT-Systems
6.1.4 Beschreibung der IT-Anwendungen
6.1.4.1 Bestandsverzeichnis der Anwendungssoftware
6.1.4.2 Bestandsverzeichnis der zu einer IT-Anwendung gehörenden Daten
6.1.4.3 Kapazitätsanforderungen einzelner IT-Anwendungen im Normalfall
6.1.4.4 Minimale Kapazitätsanforderungen der IT-Anwendungen für den Notfall
6.1.4.5 Wiederanlaufverfahren der IT-Anwendungen
6.1.5 Datensicherungsplan
6.1.6 Beschreibung der notwendigen Infrastruktureinrichtungen
6.1.7 Sonstige Unterlagen (Handbücher etc.)
6.2 Beschreibung des IT-Systems B
...
7 Wichtige Informationen
7.1 Ersatzbeschaffungsplan
7.2 Hersteller- und Lieferantenverzeichnis
7.3 Verzeichnis der Dienstleistungsunternehmen des Fachgebiets „Sanierung“

Letztes Änderungsdatum:

Das Notfall-Handbuch ist durch die Behörden- bzw. Unternehmensleitung in Kraft zu setzen und muß nach Bedarf aktualisiert werden. Die Verfügbarkeit des Notfall-Handbuches ist von zentraler Bedeutung. Deshalb ist ein aktuelles Exemplar extern auszulagern. Zusätzlich ist das Notfall-Handbuch allen im Handbuch genannten Personen oder Organisationseinheiten zur Kenntnis zu geben.
(Die Ausgestaltung wichtiger Inhalte ist den nachfolgenden Maßnahmenbeschreibungen zu entnehmen.)

M 6.4 Dokumentation der Kapazitätsanforderungen der IT-Anwendungen
Im Hinblick auf interne und externe Ausweichmöglichkeiten für den Betrieb der IT-Anwendungen sind für diese Kapazitätsanforderungen zu dokumentieren. Hierunter fallen u.a.:

- CPU-Leistung,
- Plattenkapazitäten,
- DFÜ-Leistung und
- Leistungen weiterer Hardwarekomponenten (Drucker, Belegleser etc.).

Die Kapazitätsanforderungen einer IT-Anwendung sind dahingehend zu untersuchen, ob sie für den Zeitraum eines Notfalls reduziert werden können, um auf diese Weise einen eingeschränkten IT-Betrieb zu ermöglichen (z.B. Reduzierung der Anzahl der angeschlossenen Terminals). Diese eingeschränkten Kapazitätsanforderungen für den Notfall sind ebenfalls zu dokumentieren und zu aktualisieren.

M 6.5 Definition des eingeschränkten IT-Betriebs
Für den Fall, daß Teile des IT-Systems ausfallen, ist zu untersuchen, ob ein eingeschränkter IT-Betrieb notwendig und möglich ist. Um bei einem eingeschränkten IT-Betrieb möglichst viele IT-Anwendungen betreiben zu können, ist die für jede einzelne IT-Anwendung die zur Verfügung gestellte Kapazität auf das notwendige Maß zu reduzieren (siehe M 6.4 - Dokumentation der Kapazitätsanforderungen der IT-Anwendungen).
Für den eingeschränkten IT-Betrieb muß festgelegt werden, welche IT-Anwendungen mit welcher Priorität betrieben werden. Dies ist schriftlich zu fixieren. Auch manuelle Ersatzverfahren können geeignet sein, um die Verfügbarkeitsanforderungen einer IT-Anwendung zu senken. Die für den Einsatz eines manuellen Ersatzverfahrens erforderlichen Hilfsmittel (Formulare, Papierlisten, Mikrofiche) müssen dazu allerdings bereitgehalten werden.

M 6.6 Untersuchung interner und externer Ausweichmöglichkeiten
Um Kapazitätsengpässe im eingeschränkten IT-Betrieb zu vermeiden, sind interne und externe Ausweichmöglichkeiten zu untersuchen. Bei der Untersuchung von Ausweichmöglichkeiten

ist insbesondere auf die technischen Anforderungen an das Ausweich-IT-System zu achten. Kompatibilität und ausreichende Kapazitätsreserven (siehe M 6.4 - Dokumentation der Kapazitätsanforderungen der IT-Anwendungen) des Ausweich-IT-Systems sind Grundvoraussetzung für dessen Benutzung.
Zunächst steht die interne Verlagerung von IT-Anwendungen von einem IT-System auf ein anderes IT-System im Vordergrund (z.B. Ausweichen auf den Entwicklungsrechner, wenn der Produktionsrechner ausfällt). Externe Ausweichmöglichkeiten sind dann heranzuziehen, wenn mit internen Ausweichmöglichkeiten die Verfügbarkeitsanforderungen nicht mehr oder nicht wirtschaftlich erfüllt werden können.
Ausweichmöglichkeiten für nicht IT-spezifische Komponenten sind auch zu berücksichtigen. Beispielsweise im Bereich der Infrastruktur sind Ausweichmöglichkeiten für IT-Räume in Betracht zu ziehen.

M 6.7 Regelung der Verantwortung im Notfall
Für den Zeitraum nach Eintritt des schädigenden Ereignisses bis hin zur vollständigen Wiederherstellung der Verfügbarkeit kann eine zeitlich befristete Notfall-Organisation erforderlich sein.
Es müssen Verantwortliche bestimmt sein, die befugt sind zu entscheiden, ob ein Notfall eingetreten ist, und die die entsprechenden Maßnahmen des Notfall-Handbuchs einleiten (siehe M 6.2 - Notfall-Definition, Notfall-Verantwortlicher). Die an der Durchführung der Maßnahmen im Bereich der Notfallvorsorge beteiligten Organisationseinheiten müssen befugt sein, die ihnen übertragenen Aufgaben eigenverantwortlich durchzuführen. Die hierzu erforderlichen Regelungen sind schriftlich festzuhalten. Dieses Notfall-Organigrammmuß von der Behörden- bzw. Unternehmensleitung autorisiert werden.

M 6.8 Alarmierungsplan
Ein Alarmierungsplan enthält eine Beschreibung des Meldewegs, über den bei Eintritt eines Notfalls die zuständigen Personen oder Organisationseinheiten zu informieren sind. Die Alarmierung kann z.B. über Telefon, Fax, Funkrufdienste oder Kurier erfolgen. Beschrieben werden muß, wer wen benachrichtigt, wer ersatzweise zu benachrichtigen ist bzw. wie bei Nichterreichen zu verfahren ist. Zu diesem Zweck sind evtl. Adress- und Telefonlisten zu führen.
Der Alarmierungsplan muß sämtlichen Notfall-Verantwortlichen zur Verfügung stehen, darüber hinaus an zentraler Stelle redundant vorgehalten werden (z.B. Pforte, Bewachungspersonal). Die im Alarmierungsplan genannten Personen müssen den sie betreffenden Teil kennen. Allen Mitarbeitern müssen die Ansprechpartner bekannt sein, denen das Eintreten eines evtl. Notfall-auslösenden Ereignisses gemeldet werden kann. Es kann verschiedene Alarmierungspläne für unterschiedliche Schadensfälle geben (Feuer, Wasser, DFÜ-Ausfall). Dann muß darauf geachtet werden, daß alle Schadensfälle abgedeckt sind.
Mit der Erstellung eines Alamierungsplans sollte auch die Festlegung eines Ruf- oder Bereitschaftsdienstes erwogen werden.

M 6.9 Notfall-Pläne für ausgewählte Schadensereignisse
Notfall-Pläne beinhalten Handlungsanweisungen und Verhaltensregeln für bestimmte Schaden-

sereignisse. Hierbei handelt es sich um Ereignisse, die diejenigen Teile des IT-Systems gefährden, die von existentieller Bedeutung sind. Ein Notfall-Plan ist auf die möglichst schnelle Wiederherstellung der Verfügbarkeit gerichtet.
Ein Notfall-Plan muß auch das Zusammenwirken eines schädigenden Ereignisses und der getroffenen Notfall-Maßnahme berücksichtigen. Beispielsweise kann durch den Einsatz einer Sprinkleranlage ein Brand bekämpft werden. Jedoch können durch den Wassereinsatz wiederum auch neue Gefährdungen entstehen, z.B. für die Stromversorgung oder für Datenträgerarchive.
Notfall-Pläne sind je nach Umfeldgegebenheiten für folgende Ereignisse aufzustellen:

- Brand,
- Wassereinbruch,
- Stromausfall,
- Ausfall der Klimaanlage,
- Explosion,
- Ausfall der Datenfernübertragungseinrichtung (siehe M 6.10 - Notfall-Plan für DFÜ-Ausfall),
- Sabotage.

Die Wirksamkeit von Notfall-Plänen ist durch Notfallübungen (siehe M 6.12 - Durchführung von Notfallübungen) zu überprüfen.

M 6.10 Notfall-Plan für DFÜ-Ausfall
Der Notfall-Plan für den DFÜ-Ausfall beinhaltet die Handlungsanweisungen, die bei Ausfall von DFÜ-Einrichtungen durchzuführen sind. Insbesondere müssen die bestehenden internen und externen Ausweichmöglichkeiten bekannt sein, bevor die Entscheidung fixiert wird, wie ein Ausfall kompensiert werden soll.
Alternative Ausweichmöglichkeiten sind zum Beispiel:

- Ersatz der Datenübertragung durch Austausch von Datenträgern oder Druckerzeugnissen per Kurier ,
- Datenübertragung über andere DFÜ-Einrichtungen oder
- Einsatz mobiler Kommunikationseinrichtungen (z. B. Bündelfunk, Mobiltelefonie, Satellitenkommunikation).

M 6.11 Erstellung eines Wiederanlaufplans
Für einen geregelten Wiederanlauf nach Ausfall einer IT-Komponente sind folgende Informationen zu dokumentieren (siehe Beispiel in M 6.5 - Definition des eingeschränkten IT-Betriebs, Teil C):

- Wiederbeschaffungsmöglichkeiten, zum Beispiel die Nutzung eines Testrechners für den Dialogbetrieb oder die Ersatzbeschaffung (siehe M 6.14 - Ersatzbeschaffungsplan),
- interne/externe Ausweichmöglichkeiten für IT-Anwendungen (siehe M 6.6 - Untersuchung interner und externer Ausweichmöglichkeiten) sind aufzuzählen,
- DFÜ-Versorgung (siehe M 6.10 - Notfallplan für DFÜ-Ausfall) für den Notbetrieb, um die minimal notwendigen Datenübertragungen zu gewährleisten,
- die im eingeschränkten IT-Betrieb (siehe M 6.5 - Definition des eingeschränkten IT-Betriebs) laufenden IT-Anwendungen,
- Systemstart der IT-Komponente und Einbindung in das IT-System und
- um den Anforderungen an die Verfügbarkeit (siehe M 6.1 - Erstellung einer Übersicht über Verfügbarkeitsanforderungen) der einzelnen IT-Anwendungen gerecht zu werden, ist eine Reihenfolge für den Wiederanlauf der IT-Anwendungen festzulegen.

Die für den Wiederanlauf einer IT-Anwendungen erforderlichen Schritte sind im Notfall-Handbuch aufzuzeigen (siehe Beispiel in M 6.5 - Definition des eingeschränkten IT-Betriebs, Teil D). Beispiele für solche Schritte sind:

- Aufbau und Installation der notwendigen Hardware-Komponenten,
- Einspielen der Systemsoftware,
- Einspielen der Anwendungssoftware,
- Bereitstellen der notwendigen Daten einschließlich Konfigurationsdateien,
- Wiederanlauf.

Eine revisionsfähige Protokollierung des Wiederanlaufs ist zu gewährleisten.
Der Wiederanlaufplan ist durch Notfallübungen (sowohl bei internen als auch bei externen Ausweichmöglichkeiten) auf seine Durchführbarkeit zu testen. Insbesondere ist bei der Durchführung solcher Übungen der ausschließliche Einsatz der Software und Daten zu testen, die in internen oder externen Sicherungsarchiven aufbewahrt werden.
Der Wiederanlauf kann, je nach Umfang der betriebenen IT-Anwendungen, mit erheblichen Zeitaufwand verbunden sein. Der Zeitaufwand für die mit dem Wiederanlauf verbundenen Maßnahmen kann durch solche Übungen ermittelt werden und ist bei der Überarbeitung des Wiederanlaufplans zu berücksichtigen.

M 6.12 Durchführung von Notfallübungen
Notfallübungen dienen der Prüfung der Wirksamkeit von Maßnahmen im Bereich der Notfallvorsorge. Einerseits wird durch eine Notfallübung der effektive und reibungslose Ablauf eines Notfall-Plans erprobt und andererseits werden bisher unerkannte Mängel aufgedeckt. Typische Übungen sind:

- die Durchführung einer Alarmierung,
- Durchführung von Brandschutzübungen (vgl. M 6.17 - Alarmierungsplan und Brandschutzübungen),
- Funktionstests von Stromaggregaten,
- Wiederanlauf nach Ausfall einer ausgewählten IT-Komponente und
- Wiedereinspielen von Datensicherungen.

Die Ergebnisse einer Notfallübung sind zu dokumentieren.
Notfallübungen sind regelmäßig zu wiederholen. Da diese Übungen den normalen Betriebsablauf stören können, sollte die Häufigkeit an der Gefährdungslage orientiert sein, jedoch sollten die entsprechenden Notfallübungen zumindest einmal jährlich stattfinden. Soweit erforderlich sind Schulungsmaßnahmen der Mitarbeiter durchzuführen (Erste Hilfe, Brandbekämpfung etc.)
Vor Durchführung einer Notfallübung ist das Einverständnis der Behörden- bzw. Unternehmensleitung einzuholen.

M 6.13 Erstellung eines Datensicherungsplans
Mit Hilfe des Datensicherungsplans muß ein sachverständiger Dritter in der Lage sein, sämtliche für den Wiederanlauf einer IT-Anwendung erforderliche Software (Betriebssystemsoftware, Anwendungssoftware) und deren Daten in angemessener Zeit beschaffen und installieren zu können.
Ein Datensicherungsplan muß Auskunft geben können über:

- Speicherungsort der Daten im Normalbetrieb (Plattenspeicher-Belegungsplan),
- den Bestand der gesicherten Daten (Bestandsverzeichnis),
- die Zeitpunkte der Datensicherungen,
- Art und Umfang der Datensicherung (logische/physikalische, Teil-/Vollsicherung),
- das Verfahren zur Datensicherung und zur Rekonstruktion der gesicherten Daten und
- den Ort der Aufbewahrung (Hinweis auf ggf. erforderliche Zutrittsmittel).

Die systematische Erarbeitung eines Datensicherungskonzeptes, aus dem sich ein Datensicherungsplan ableitet, wird in [BSI1998] Kapitel 3.4 - Datensicherungskonzept beschrieben.

M 6.14 Ersatzbeschaffungsplan
Bei Ausfall einzelner Teile des IT-Systems ist neben der Reparatur die Ersatzbeschaffung zunächst die Maßnahme, die am zielgerichtetsten die Wiederherstellung der Verfügbarkeit verfolgt.
Um den Vorgang der Ersatzbeschaffung zu beschleunigen, ist die Erstellung eines Ersatzbeschaffungsplans sinnvoll. Dieser muß für jede wichtige IT-Komponente Angaben machen über:

- Bezeichnung der IT-Komponente (Name, Geräte-Nr., Beschaffungsdatum),
- Hersteller,
- Lieferant,
- Lieferzeit und
- Dauer der Reinstallation.

Lassen sich für eine IT-Komponente mehrere Hersteller oder Lieferanten benennen, so sind sie alternativ aufzuführen. Gegebenenfalls lassen sich auch anderweitige Produkte benennen. Bei einer Ersatzbeschaffungsmaßnahme sind solche Angaben für eine sparsame Mittelbewirtschaftung erforderlich.
Ersatzbeschaffungsmaßnahmen müssen neben der Wiederherstellung der Verfügbarkeit des IT-Systems auch der Fortentwicklung der Informationstechnik Rechnung tragen. Entsprechen eingesetzte Teile des IT-Systems nicht mehr dem Stand der Technik, so darf eine Ersatzbeschaffung nicht ausschließlich darauf gerichtet sein, den alten Zustand wiederherzustellen. Dies erfordert eine regelmäßige Überarbeitung des Ersatzbeschaffungsplans. Der Bezug zur Betriebsmittelverwaltung ist zu beachten (vgl. M 2.2 - Betriebsmittelverwaltung).

M 6.15 Lieferantenvereinbarungen
Bei Kauf von Informationstechnik ergibt sich für den IT-Betreiber die Notwendigkeit, Ersatzbeschaffungsmaßnahmen zu planen. Von besonderer Bedeutung beim Kauf ist eine vom Hersteller oder Lieferanten zugesicherte Nachkaufgarantie, Ersatzteillieferung, garantierte Lieferzeiten, die Garantiezeit bei auftretenden Mängeln sowie der angebotene Support.
Miet- bzw. Leasingverträge müssen Regelungen über schadensvorbeugende Wartungsarbeiten und die Anforderungen an die Beseitigung von Störungen oder Schäden beinhalten.
Im Gegensatz zum Kauf von Informationstechnik ist bei deren Miete oder Leasing eine Vielzahl von Risiken über den Vermieter bereits abgesichert. In der Regel schließt ein Vermieter eine Feuerversicherung für die vermietete Informationstechnik ab, die vom Mieter durch den Mietvertrag mitbezahlt wird. Somit ist bei Miete oder Leasing von Informationstechnik auf die nicht vom Vertrag abgedeckten Versicherungslücken zu achten.

M 6.16 Abschließen von Versicherungen
Für Bundesbehörden ist der Abschluß von Versicherungen unüblich.
Die auch bei hinreichender Notfallplanung nicht auszuschließenden Restrisiken lassen sich teilweise durch Versicherungen abdecken. Die Versicherungsarten lassen sich gliedern in:

- Sachversicherungen
  - Feuerversicherung
  - Leitungswasserversicherung
  - Einbruchdiebstahlversicherung
  - Montage-/Demontage-Versicherung
  - Transportversicherung

- Datenträgerversicherung
- Elektronik-Versicherung

- Folgekostenversicherungen
  - Feuer-Betriebsunterbrechungs-Versicherung
  - Maschinen-Betriebsunterbrechungs-Versicherung
  - Mehrkostenversicherung
  - Elektronik-Betriebsunterbrechungs-Versicherung

- Personenbezogene Versicherungen
  - Vertrauensschadenversicherung
  - Computer-Mißbrauch-Versicherung
  - Datenschutzversicherung

M 6.17 Alarmierungsplan und Brandschutzübungen

Es ist erforderlich, Pläne für die im Brandfall zu ergreifenden Maßnahmen zu erstellen. In einem solchen Plan ist z.B. niederzulegen,

- welche Maßnahmen bei welchen Ereignissen zu treffen sind,
- ob und wie Gebäudeteile evtl. zu räumen sind (Personen und Geräte),
- wer zu informieren ist und
- welche hilfeleistenden Kräfte zu informieren sind.

Ergänzt werden kann der Alarmierungsplan um Verhaltensregeln für den Brandfall, die allen Mitarbeitern bekanntzugeben sind. Dazu siehe auch Kapitel 3.3 - Notfallvorsorge.
Der beste Alarmierungsplan nützt allerdings wenig, wenn nicht sichergestellt ist, daß die darin aufgelisteten Maßnahmen richtig und praktikabel sind. Es ist also erforderlich, den Alarmplan regelmäßig zu prüfen und zu aktualisieren. Eine dieser Prüfungsmaßnahmen ist die Durchführung von Brandschutzübungen.
Beispiel: Eine im Herbst 1993 in einem 21-geschossigen Bonner Bürogebäude durchgeführte Brandschutzübung hat gezeigt, daß viele Mitarbeiter nicht wußten, wo ein Feuerlöscher oder wo das Treppenhaus ist. Im Ernstfall kann diese Unkenntnis zu einer Katastrophe führen. Teilweise wurde die Übung ignoriert, man verließ aus Bequemlichkeit den Raum nicht.
Gerade in Brandschutzübungen soll das richtige Verhalten im Brandfall geschult und geübt werden, um Menschenleben zu schützen und Schäden u.a. für die IT zu vermeiden. Die Durchführung solcher Übungen ist vorher mit der Behörden- bzw. Unternehmensleitung abzustimmen.

M 6.18 Redundante Leitungsführung

Bei der redundanten Leitungsführung werden zwischen geeigneten Punkten im Netz neben den im normalen Betrieb genutzten Leitungen zusätzliche Verbindungen eingerichtet. Diese sollten über eine andere Trasse geführt werden. Dadurch besteht die Möglichkeit, bei Störungen auf die

redundante Verbindung umzuschalten. Diese Umschaltung kann automatisch oder von Hand erfolgen. Die automatische Umschaltung ist an einer Stelle anzuzeigen, die die Störungsbeseitigung auf der normalen Leitung veranlaßt.

Die Funktionsfähigkeit von redundanten Leitungen ist in sinnvollen Zeitabständen durch tatsächliche Nutzung auf ihre Funktionsfähigkeit hin zu überprüfen. Die Dimensionierung, die Prüfintervalle und die grundsätzliche Notwendigkeit von redundanten Leitungen ist direkt von der Verfügbarkeitsanforderung an das Netz abhängig. Ebenso muß man das Verhältnis der Bereitstellungszeit der redundanten Leitung zur Wiederherstellungszeit der normalen Leitung berücksichtigen. Es ist allerdings von entscheidender Bedeutung, ob es sich um Leitungen im öffentlichen Bereich (z.B. Telekom) oder im privaten Bereich handelt.

- Bei Leitungen im öffentlichen Bereich hat der Benutzer keinen Einfluß auf deren Schutz. Das öffentliche Netz stellt grundsätzlich eine ausreichende Zahl von redundanten Leitungen zur Verfügung. Meistens reicht es aus, bei Ausfall einer Verbindung (gleichgültig ob Festverbindung oder Wählleitung) durch Aufbau einer Wählleitung die Verbindung wiederherzustellen. Die Schaltung von redundanten Festverbindungen ist in der Regel zu teuer und meistens verzichtbar.
- In einem privaten Netz kann der Betreiber die Sicherheit von Leitungen wesentlich beeinflussen. Kostenüberlegungen führen meist dazu, daß es keine redundanten Leitungen gibt. In privaten Netzen verursachen redundante Leitungen jedoch außer den Herstellungskosten keine laufenden Ausgaben.

M 6.20 Geeignete Aufbewahrung der Backup-Datenträger
Backup-Datenträger unterliegen besonderen Anforderungen hinsichtlich ihrer Aufbewahrung:

- Der Zugriff auf diese Datenträger darf nur befugten Personen möglich sein, so daß eine Entwendung ausgeschlossen werden kann.
- Ein ausreichend schneller Zugriff muß im Bedarfsfall gewährleistet sein.
- Für den Katastrophenfall müssen die Backup-Datenträger räumlich getrennt vom Rechner aufbewahrt werden, wenn möglich in einem anderen Brandabschnitt.

Zu beachten sind auch die Anforderungen aus M 2.3 - Datenträgerverwaltung.

M 6.21 Sicherungskopie der eingesetzten Software
Von den Originaldatenträgern erworbener Software bzw. von der Originalsoftware bei Eigenentwicklungen ist eine Sicherungskopie zu erstellen, von der bei Bedarf die Software wieder eingespielt werden kann. Die Originaldatenträger und die Sicherungskopien sind getrennt voneinander aufzubewahren. Es ist darauf zu achten, daß der physikalische Schreibschutz des Datenträgers ein versehentliches Löschen oder Überschreiben der Daten verhindert. Wird die Software auf CD-ROM zur Verfügung gestellt, sollte alternativ nach der Installation von der CD-ROM eine Sicherungskopie der installierten Software erstellt werden, da der Datenumfang

auf der CD-ROM i.allg. zu umfangreich ist.
Ein unerlaubter Zugriff, z.B. zur Erstellung einer Raubkopie, muß ausgeschlossen sein.

M 6.22 Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
Für die Rekonstruktion eines Datenbestandes muß geprüft werden, ob mit den vorhandenen Sicherungskopien der Daten ein solches Vorhaben durchgeführt werden kann. Durch technische Defekte, falsche Parametrisierung, einer unzureichenden Datenträgerverwaltung oder der Nichteinhaltung von Regeln, die in einem Datensicherungskonzept gefordert werden, ist es möglich, daß eine Rekonstruktion eines Datenbestandes nicht möglich ist. Daher ist es notwendig, daß sporadisch überprüft wird, ob die erzeugten Datensicherungen zur Wiederherstellung verlorener Daten genutzt werden können.

M 6.23 Verhaltensregeln bei Auftreten eines Computer-Virus
Gibt es Anzeichen, daß ein Rechner von einem Computer-Virus befallen ist (z.B. Programmdateien werden länger, unerklärliches Systemverhalten, nicht auffindbare Dateien, veränderte Dateiinhalte, ständige Verringerung des freien Speicherplatzes, ohne daß etwas abgespeichert wurde), so sind zur Feststellung eines Computer-Virus und zur anschließenden Beseitigung folgende Schritte durchzuführen:

1. Ruhe bewahren!
2. Falls möglich, holen Sie einen fachkundigen PC-Betreuer zur Hilfe.
3. Beenden Sie die laufenden Programme und schalten Sie den Rechner aus.
4. Legen Sie eine einwandfreie, schreibgeschützte System-Diskette (die Notfall-Diskette aus M 6.24 - Erstellen einer PC-Notfalldiskette) in Laufwerk A: ein.
5. Booten Sie den Rechner von dieser Diskette (evtl. vorher Boot-Reihenfolge im CMOS-Setup ändern, siehe M 4.3 - Regelmäßiger Einsatz eines Viren-Suchprogramms).
6. Überprüfen Sie den Rechner mit einem aktuellen Viren-Suchprogramm um festzustellen, ob und um welchen Computer-Virus es sich handelt.
7. Entfernen Sie den Virus abhängig vom jeweiligen Virustyp (falls sich Probleme ergeben, können Sie sich an die Viren-Hotline des BSI wenden unter (0228) 9582-444).
8. Überprüfen Sie mit dem Viren-Suchprogramm die Festplatte erneut.
9. Untersuchen Sie alle anderen Datenträger (Disketten, Wechselplatten) auf Virenbefall und entfernen Sie die Computer-Viren.
10. Versuchen Sie die Quelle der Vireninfektion festzustellen:
    wenn erfolgreich, anschließend
    - bei Programm-Disketten: Hersteller informieren,
    - bei Daten-Disketten: Ersteller der Diskette informieren.

11. Warnen Sie andere IT-Benutzer, wenn ein Disketten-Austausch vom infizierten Rechner erfolgte.

12. Schicken Sie den Virus-Meldebogen ans BSI (Vordruck befindet sich im Anhang).

Sollte der Computer-Virus Daten gelöscht oder verändert haben, versuchen Sie, die Daten aus den Datensicherungen (vgl. M 6.19 - Datensicherung am PC) und die Programme aus den Sicherungskopien der Programme (vgl. M 6.21 - Sicherungskopie der eingesetzten Software) zu rekonstruieren. Anschließend sollte nochmals Schritt 8 wiederholt werden.

M 6.24 Erstellen einer PC-Notfalldiskette

Bei der erstmaligen Einrichtung eines PC sollte eine Notfalldiskette erstellt werden, die bei Ausfall einer Festplatte zum Starten des Systems oder bei Auftreten eines Computer-Virus zum Erzeugen eines kontrollierten Systemzustands genutzt werden kann.
Diese Diskette sollte als Systemdiskette formatiert werden (DOS-Befehl FORMAT A: /S). Anschließend sollten, soweit der Speicherplatz reicht, die folgenden Programme darauf gespeichert werden: der deutsche Keyboard-Treiber KEYB.COM sowie KEYBOARD.SYS, COUNTRY.SYS, HIMEM.SYS und die Programme FORMAT.EXE, SYS.COM, FDISK.EXE, CHKDSK.EXE, MEM.EXE und DEBUG.EXE.
Darüber hinaus sollte eine AUTOEXEC.BAT sowie eine CONFIG.SYS-Datei generiert und auf der Notfall-Diskette gespeichert werden, die die gewünschte Tastaturbelegung und den gewohnten DOS-Prompt erzeugt. Dabei muß darauf geachtet werden, daß alle Pfadnamen stimmen (es darf kein C: mehr enthalten sein!).
Die Notfall-Diskette sollte ebenfalls einen Editor enthalten. Die Verfügbarkeit des Programms, mit dem die Backups erstellt wurden, muß ebenfalls sichergestellt sein. Es kann sich bei Speicherplatzproblemen aber auch auf einer zweiten Diskette befinden. Falls Treiber zur Festplattenkomprimierung eingesetzt wurden, müssen diese auch auf die Notfall-Diskette gespeichert werden, sonst kann im Notfall nicht auf die Festplatte zugegriffen werden. Nach dem Erstellen der Notfall-Diskette sollte diese auf Computer-Viren überprüft und danach schreibgeschützt werden.
Ist diese Notfalldiskette für den fachkundigen PC-Betreuer greifbar, erleichtert sie seine Arbeit gerade bei der Beseitigung von Computer-Viren.

M 6.25 Regelmäßige Datensicherung der Server-Festplatte

An die Verfügbarkeit der auf der Festplatte des Servers gespeicherten Daten müssen hohe Anforderungen gestellt werden, da in der Regel viele Benutzer auf diese Daten zugreifen. Mit einer regelmäßigen Datensicherung muß erreicht werden, daß alle Daten der Server-Festplatte, die z.B. nicht älter als ein Tag sind, rekonstruiert werden können (vgl. auch M 6.32 - gelmäßige Datensicherung).
Ein mögliches Datensicherungskonzept wäre, täglich inkrementell (d.h. alle veränderten Dateien) zu sichern und einmal wöchentlich oder monatlich eine Komplettsicherung vorzunehmen. Dabei sollte mindestens das Drei-Generationen-Prinzip (es werden drei aufeinanderfolgende Datensicherungen erzeugt, bevor die erste überschrieben wird) eingehalten werden.
Eine erfolgte Datensicherung ist unbedingt zu dokumentieren. Mindestens muß die (möglichst

sprechende) Bezeichnung des Datenträgers, das Datum der Datensicherung und die Art der Sicherung (inkrementell/komplett) festgehalten werden.

M 6.26 Regelmäßige Datensicherung der TK-Anlagen-Konfigurationsdaten
Die in der TK-Anlage gespeicherten Daten sind in regelmäßigen Abständen zu sichern. Dies kann mit Hilfe eines anlageninternen oder -externen Bandlaufwerkes geschehen. Der Sicherungszyklus hängt dabei stark von der Anzahl der durchgeführten Administrationsvorgänge ab. Als ein Beispiel für einen sinnvollen Wert kann eine Datensicherung nach ca. 50 Administrationsvorgängen angenommen werden. Legt man den durchaus üblichen Wert von einer Veränderung pro Teilnehmer und Jahr zugrunde, so ergibt sich hieraus bei 600 Teilnehmern ein Datensicherungszyklus von einem Monat. Neben diesen regelmäßigen Datensicherungen sollte nach grundlegenden Änderungen ebenfalls eine Datensicherung erfolgen.

M 6.27 Sichern des CMOS-RAM
Benutzer von AT-Bus-Platten müssen normalerweise die Anzahl der Köpfe, Sektoren und Zylinder ihrer Festplatte von Hand ins Setup eintragen. In den Handbüchern finden sich diese Angaben nur selten, daher sollten sie unbedingt nach jeder Änderung schriftlich niedergelegt (z.B. im PC-Checkheft, M 2.24 Einführung eines PC-Checkheftes) oder mit einem entsprechenden Programm auf Diskette gespeichert werden.

M 6.28 Vereinbarungen über Lieferzeiten lebensnotwendigerTK-Baugruppen
Lebensnotwendige Baugruppen, wie zentrale Steuereinheiten, digitale Koppelfelder etc. sollten auch bei redundanter Auslegung in hinreichend kurzer Zeit lieferbar sein oder bevorratet werden. Redundante Baugruppen sollten ab und zu mit den aktiven ausgetauscht werden.

M 6.29 TK-Basisanschluß für Notrufe
Bei einem Total- oder Teilausfall der TK-Anlage kann es geschehen, daß über die an diese Anlage angeschlossenen Amtsleitungen keine Verbindungen mehr möglich sind. Um dennoch Hilfe heranholen zu können, ist es sinnvoll, einen völlig separaten Basisanschluß bzw. analogen Fernsprechanschluß einzurichten.

M 6.30 Katastrophenschaltung
Um in Ausnahmesituationen zur Einleitung von Maßnahmen Telefonleitungen verfügbar zu haben, bieten einige TK-Anlagen die Möglichkeit, in einer sog. Katastrophenschaltung die vorhandenen kommenden und gehenden Leitungen vorher festgelegten Anschlüssen zuzuweisen. Dies gewährleistet, daß in einem Katastrophenfall wichtige Einrichtungen handlungsfähig bleiben. Steht diese Möglichkeit zur Verfügung, sollte sie genutzt werden.

M 6.31 Verhaltensregeln nach Verlust der Systemintegrität
Falls sich das Unix-System in nicht vorgesehener Weise verhält (zum Beispiel undefiniertes Systemverhalten, nicht auffindbare Daten, veränderte Dateiinhalte, ständige Verringerung des freien Speicherplatzes, ohne daß etwas abgespeichert wurde), kann ein Verlust der Systemintegrität vorliegen, der durch mißbräuchliche Nutzung des Systems verursacht wurde (zum Beispiel

unautorisierte Administration, Veränderungen der Systemeinstellungen, Einspielen eines Trojanisches Pferdes oder eines Computer-Virus).
Dann sollten die Benutzer folgende Punkte beachten:

- Ruhe bewahren!
- Benachrichtigen Sie den Administrator.
- Beenden Sie laufende Programme. Der Administrator sollte folgende Schritte durchführen: Herunterfahren des Systems,
- Hochfahren des Systems, so daß nur Zugriff von der Konsole aus möglich ist (z.B. Single-User-Modus),
- Überprüfung der ausführbaren Dateien auf sichtbare Veränderungen, z.B. Erstellungsdatum und Dateigröße (Da diese von einem Angreifer auch wieder auf ihre Ursprungswerte zurückgesetzt werden können, sollte die Integrität der Dateien mit Prüfsummenverfahren wie TRIPWIRE überprüft werden.),
- Löschen der ausführbaren Dateien und Wiedereinspielen der Original-Dateien von schreibgeschützten Datenträgern (vgl. M 6.21 - cherungskopie der eingesetzten Software) (keine Programme aus der Datensicherung wiedereinspielen),
- Überprüfung der Attribute aller Benutzerverzeichnisse und -dateien z. B. mit Prüfsummenverfahren wie TRIPWIRE und ggf. Zurücksetzen auf Minimal-Einstellungen (nur Rechte für den Eigentümer, keine root-Dateien in Benutzerbereichen),
- Überprüfung und ggf. Zurücksetzen der Attribute aller Systemverzeichnisse und -dateien,
- Benachrichtigung der Benutzer mit der Bitte, ihre Bereiche auf Unregelmäßigkeiten zu prüfen.

Falls sich Probleme ergeben, können Sie sich an die Hotline des BSI wenden unter Tel. 0228 / 9582-444 oder E-Mail cert@bsi.de.
Falls Daten gelöscht oder unerwünscht geändert wurden, können diese aus den Datensicherungen wiedereingespielt werden.

M 6.32 Regelmäßige Datensicherung
Zur Vermeidung von Datenverlusten müssen regelmäßige Datensicherungen durchgeführt werden. In den meisten Rechnersystemen können diese weitgehend automatisiert erfolgen. Es sind Regelungen zu treffen, welche Daten von wem wann gesichert werden. Empfehlenswert ist die Erstellung eines Datensicherungskonzepts.
Abhängig von der Menge und Wichtigkeit der laufend neu gespeicherten Daten und vom möglichen Schaden bei Verlust dieser Daten ist folgendes festzulegen:

- Zeitintervall
  Beispiele: täglich, wöchentlich, monatlich,

- Zeitpunkt
  Beispiele: nachts, freitags abends,
- Anzahl der aufzubewahrenden Generationen,
  Beispiel: Bei täglicher Komplettsicherung werden die letzten sieben Sicherungen aufbewahrt, außerdem die Freitagabend-Sicherungen der letzten zwei Monate.
- Umfang der zu sichernden Daten
  Am einfachsten ist es, Partitionen bzw. Verzeichnisse festzulegen, die bei der regelmäßigen Datensicherung berücksichtigt werden. Eine geeignete Differenzierung kann die Übersichtlichkeit vergrößern sowie Aufwand und Kosten sparen helfen.
  Beispiel: selbsterstellte Dateien und individuelle Konfigurationsdateien.
- Speichermedien (abhängig von der Datenmenge)
  Beispiele: Bänder, Kassetten, Disketten, Spiegelung auf 2. Platte,
- Vorherige Löschung der Datenträger vor Wiederverwendung (Bänder, Kassetten)
- Zuständigkeit für die Durchführung (Administrator, Benutzer)
- Zuständigkeit für die Überwachung der Sicherung, insbesondere bei automatischer Durchführung (Fehlermeldungen, verbleibender Platz auf den Speichermedien)
- Dokumentation der erstellten Sicherungen (Datum, Art der Durchführung der Sicherung / gewählte Parameter, Beschriftung der Datenträger)

Wegen des großen Aufwands können Komplettsicherungen in der Regel höchstens einmal täglich durchgeführt werden. Die seit der letzten Sicherung erstellten Daten können nicht wiedereingespielt werden. Daher und zur Senkung der Kosten sollen zwischen den Komplettsicherungen regelmäßig inkrementelle Sicherungen durchgeführt werden, das heißt, nur die seit der letzten Komplettsicherung neu erstellten Daten werden gesichert. (Werden zwischen zwei Komplettsicherungen mehrere inkrementelle Sicherungen durchgeführt, können auch jeweils nur die seit der letzten inkrementellen Sicherung neu erstellten Daten gesichert werden.)
Eine inkrementelle Sicherung kann häufiger erfolgen, zum Beispiel sofort nach Erstellung wichtiger Dateien oder mehrmals täglich. Die Vereinbarkeit mit dem laufenden Betrieb ist sicherzustellen.
Für eingesetzte Software ist in der Regel die Aufbewahrung der Originaldatenträger und deren Sicherungskopien ausreichend. Sie braucht dann von der regelmäßigen Datensicherung nicht erfaßt zu werden.
Alle Benutzer sollten über die Regelungen zur Datensicherung informiert sein, um ggf. auf Unzulänglichkeiten (zum Beispiel zu geringes Zeitintervall für ihren Bedarf) hinweisen oder individuelle Ergänzungen vornehmen zu können (zum Beispiel zwischenzeitliche Spiegelung wichtiger Daten auf der eigenen Platte). Auch die Information der Benutzer darüber, wie lange die Daten wiedereinspielbar sind, ist wichtig. Werden zum Beispiel bei wöchentlicher Komplettsicherung nur zwei Generationen aufbewahrt, bleiben in Abhängigkeit vom Zeitpunkt des Verlustes nur zwei bis drei Wochen Zeit, um die Wiedereinspielung vorzunehmen.

Falls bei vernetzten Rechnern nur die Server-Platten gesichert werden, ist sicherzustellen, daß die zu sichernden Daten regelmäßig von den Benutzern oder automatisch dorthin überspielt werden.
Der Ausdruck von Daten auf Papier ist keine angemessene Art der Datensicherung.

M 6.33 Entwicklung eines Datensicherungskonzepts
Die Verfahrensweise der Datensicherung wird von einer großen Zahl von Einflußfaktoren bestimmt. Das IT-System, das Datenvolumen, die Änderungsfrequenz der Daten und die Verfügbarkeitsanforderungen sind einige dieser Faktoren. Im Datensicherungskonzept gilt es, eine Lösung zu finden, die diese Faktoren berücksichtigt und gleichzeitig unter Kostengesichtspunkten wirtschaftlich vertretbar ist.

Die technischen Möglichkeiten, Datensicherungen durchzuführen, sind vielfältig. Jedoch wird die Auswahl immer von den genannten Faktoren bestimmt. Daher gilt es zunächst, die Einflußgrößen der IT-Systeme und der damit realisierten IT-Anwendungen zu bestimmen und nachvollziehbar zu dokumentieren. Anschließend muß die geeignete Verfahrensweise entwickelt und dokumentiert werden. Zum Abschluß muß durch die Behörden-/Unternehmensleitung die Durchführung angeordnet werden.

Das Datensicherungskonzept muß für die Gewährleistung einer funktionierenden Datensicherung die Datenrestaurierbarkeit mittels praktischer Übungen als Verpflichtung vorsehen (siehe M 6.41 - Übungen zur Datenrekonstruktion) Die Ergebnisse sollten aktualisierbar und erweiterbar in einem Datensicherungskonzept niedergelegt werden. Ein möglicher Aufbau eines Datensicherungskonzept ist im nachfolgenden Inhaltsverzeichnis beispielhaft aufgezeigt:

Inhaltsverzeichnis Inhaltsverzeichnis Datensicherungskonzept

1. Definitionen
   - Anwendungsdaten, Systemdaten, Software, Protokolldaten
   - Vollsicherung, inkrementelle Datensicherung
2. Gefährdungslage zur Motivation
   - Abhängigkeit der Institution vom Datenbestand
   - Typische Gefährdungen wie ungeschulte Benutzer, gemeinsam genutzte Datenbestände, Computer-Viren, Hacker, Stromausfall, Festplattenfehler
   - Institutionsrelevante Schadensursachen
   - Schadensfälle im eigenen Haus
3. Einflußfaktoren je IT-System

- Spezifikation der zu sichernden Daten
- Verfügbarkeitsanforderungen der IT-Anwendungen an die Daten
- Rekonstruktionsaufwand der Daten ohne Datensicherung
- Datenvolumen
- Änderungsvolumen
- Änderungszeitpunkte der Daten
- Fristen
- Vertraulichkeitsbedarf der Daten
- Integritätsbedarf der Daten
- Kenntnisse und datenverarbeitungsspezifische Fähigkeiten der IT-Benutzer

4. Datensicherungsplan je IT-System
   (a) Festlegungen je Datenart
      - Art der Datensicherung
      - Häufigkeit und Zeitpunkt der Datensicherung
      - Anzahl der Generationen
      - Datensicherungsmedium
      - Verantwortlichkeit für die Datensicherung
      - Aufbewahrungsort der Backup-Datenträger
      - Anforderungen an das Datensicherungsarchiv
      - Transportmodalitäten
      - Rekonstruktionszeiten bei vorhandener Datensicherung
   (b) Festlegung der Vorgehensweise bei der Datenrestaurierung
   (c) Randbedingungen für das Datensicherungsarchiv
      - Vertragsgestaltung (bei externen Archiven)
      - Refresh-Zyklen der Datensicherung
      - Bestandsverzeichnis
      - Löschen von Datensicherungen
      - Vernichtung von unbrauchbaren Datenträgern
   (d) Vorhalten von arbeitsfähigen Lesegeräten
5. Minimaldatensicherungskonzept
6. Verpflichtung der Mitarbeiter zur Datensicherung
7. Sporadische Restaurierungsübungen

Einzelne Punkte dieses Datensicherungskonzepts werden in den Maßnahmen M 6.34 - Erhebung der Einflußfaktoren der Datensicherung, M 6.35 - Festlegung der Verfahrensweise für die Datensicherung, M 6.37 - Dokumentation der Datensicherung, M 6.41 - Übungen zur Datenrekonstruktion und M 2.41 - Verpflichtung der Mitarbeiter zur Datensicherung näher ausgeführt, so daß nach Bearbeitung dieser Maßnahmen für jedes relevante IT-System die wesentlichen Teile eines anwenderspezifischen Datensicherungskonzepts erstellt sind.

M 6.34 Erhebung der Einflußfaktoren der Datensicherung
Für jedes IT-System, eventuell sogar für einzelne IT-Anwendungen mit besonderer Bedeutung, müssen die nachfolgenden Einflußfaktoren ermittelt werden. Dazu können die Systemadministratoren und die Verantwortlichen der einzelnen IT-Anwendungen befragt werden. Die Ergebnisse sind nachvollziehbar zu dokumentieren.

Im einzelnen muß ermittelt werden:

Spezifikation der zu sichernden Daten
Ermittelt werden sollte der Datenbestand des IT-Systems (der IT-Anwendung), der für die Erledigung der Fachaufgaben erforderlich ist. Dazu gehören die Anwendungs- und Betriebssoftware, die Systemdaten (z. B. Initialisierungsdateien, Makrodefinitionen, Konfigurationsdaten, Textbausteine, Paßwortdateien, Zugriffsrechtedateien), die Anwendungsdaten selbst und Protokolldaten (Login-Protokollierung, Protokolle über Sicherheitsverletzungen, Datenübertragungsprotokolle, ...).

Verfügbarkeitsanforderungen der IT-Anwendungen an die Daten
Für die im ersten Schritt spezifizierten Daten müssen nun die Verfügbarkeitsanforderungen festgelegt werden. Ein erprobtes Maß dazu ist die Angabe der maximal tolerierbaren Ausfallzeit (mtA). Sie gibt an, über welchen Zeitraum die Fachaufgabe ohne diese Daten weitergeführt werden kann, ohne daß auf Datensicherungsbestände zurückgegriffen werden muß. Betrachtet werden sollte dabei auch, ob aufgrund der Papierlage ohne IT-Unterstützung kurzfristig weitergearbeitet werden kann.

Rekonstruktionsaufwand der Daten ohne Datensicherung
Um ein unter wirtschaftlichen Gesichtspunkten angemessenes Datensicherungskonzept zu entwickeln, ist es notwendig zu wissen, ob und mit welchem Aufwand zerstörte Datenbestände rekonstruiert werden können, wenn eine Datensicherung nicht zur Verfügung steht. Untersucht werden sollte, aus welchen Quellen die Daten rekonstruiert werden können. Beispiele hierfür sind die Aktenlage, Ausdrucke, Mikrofiche, Befragungen und Erhebungen.
Gemessen werden sollte der pekuniäre Aufwand oder der Arbeitsaufwand von Datenerfassungskräften in Arbeitstagen (AT).

Datenvolumen

Für die Auswahl des Speichermediums ist ein entscheidender Faktor das gespeicherte und zu sichernde Datenvolumen. Die erforderliche Angabe richtet sich ausschließlich auf die zu sichernden Daten und sollte als Maßeinheit Megabyte (MB) benutzen.

Änderungsvolumen
Um die Häufigkeit der Datensicherung und das adäquate Sicherungsverfahren bestimmen zu können, muß bekannt sein, wieviele Daten/Dateien sich in einem bestimmten Zeitabschnitt ändern. Als Arbeitsgröße wäre hier eine Einheit MB/Woche denkbar. Notwendig sind Angaben, ob bestehende Dateien inhaltlich geändert oder ob neue Dateien erzeugt werden.

Änderungszeitpunkte der Daten
Es gibt IT-Anwendungen, bei denen sich Datenänderungen nur zu bestimmten Terminen ergeben, wie zum Beispiel der Abrechnungslauf zur Lohnbuchhaltung zum Monatsende. In solchen Fällen ist eine Datensicherung unverzüglich nach einem solchen Termin sinnvoll. Daher sollte für die zu sichernden Daten angegeben werden, ob sie sich täglich, wöchentlich oder zu bestimmten Terminen ändern.

Fristen
Für die Daten ist zu klären, ob bestimmte Fristen einzuhalten sind. Hierbei kann es sich um Aufbewahrungsfristen oder auch um Löschfristen im Zusammenhang mit personenbezogenen Daten handeln. Diese Fristen sind bei der Festlegung der Datensicherung zu berücksichtigen.

Vertraulichkeitsbedarf der Daten
Der Vertraulichkeitsbedarf einer Datei überträgt sich bei einer Datensicherung auf die Sicherungskopie. Bei der Zusammenführung von Sicherungskopien mit gleichem Vertraulichkeitsbedarf auf einem Datenträger, kann sich durch die Kumulation ein höherer Vertraulichkeitsbedarf der gespeicherten Daten ergeben. Anzugeben ist also, wie hoch der Vertraulichkeitsbedarf der einzelnen zu sichernden Daten ist und zusätzlich, welche Kombinationen von Daten einen höheren Vertraulichkeitsbedarf haben als die Daten selbst.

Integritätsbedarf der Daten
Für Datensicherungen muß sichergestellt sein, daß die Daten integer gespeichert wurden und während der Aufbewahrungszeit nicht verändert werden. Dies ist um so wichtiger, je höher der Integritätsbedarf der Nutzdaten ist. Daher ist für die Datensicherungen anzugeben, wie hoch der Integritätsbedarf ist.

Kenntnisse und datenverarbeitungsspezifische Fähigkeiten der IT-Benutzer
Um entscheiden zu können, wer die Datensicherung durchführt, der IT-Benutzer selbst oder speziell beauftragte Mitarbeiter bzw. die Systemadministratoren, ist ausschlaggebend, über welche Kenntnisse und datenverarbeitungsspezifischen Fähigkeiten der IT-Benutzer verfügt und welche Werkzeuge ihm zur Verfügung gestellt werden können. Falls die zeitliche Belastung bei der Durchführung einer Datensicherung für IT-Benutzer zu hoch ist, sollte dies angegeben werden.

M 6.35 Festlegung der Verfahrensweise für die Datensicherung
Die Verfahrensweise, wie die Datensicherung durchzuführen ist, wird von den in M 6.34 - Erhebung der Einflußfaktoren der Datensicherung erhobenen Einflußfaktoren bestimmt. Für jedes IT-System und für jede Datenart muß die Verfahrensweise der Datensicherung festgelegt werden. Bei Bedarf ist sogar noch eine Unterscheidung für einzelne IT-Anwendungen des IT-Systems vorzunehmen, wenn sich hier differente Datensicherungsstrategien ergeben, was insbesondere im Großrechnerbereich sinnvoll sein kann.

Folgende Modalitäten einer Datensicherung sind für die Festlegung einer Verfahrensweise für die Datensicherung zu betrachten:

- Art der Datensicherung,
- Häufigkeit und Zeitpunkt der Datensicherung,
- Anzahl der Generationen,
- Vorgehensweise und Speichermedium,
- Verantwortlichkeit für die Datensicherung,
- Aufbewahrungsort,
- Anforderungen an das Datensicherungsarchiv,
- Transportmodalitäten,
- Aufbewahrungsmodalität.

In der nachfolgenden Tabelle werden die Abhängigkeiten zwischen den Modalitäten einer Datensicherung und den Einflußfaktoren dargestellt und anschließend erläutert:

Tabelle H.2: Datensicherung: Abhängigkeiten zwischen den Modalitäten einer Datensicherung und den Einflußfaktoren. X bedeutet direkter Einfluß, (X) bedeutet indirekter Einfluß

	Art der Datensicherung	Häufigkeit und Zeitpunkte der Datens.	Anzahl der Generationen	Vorgehensweise und Speichermedium	Verantwortlichkeit für Datens.	Aufbewahrungsort	Anforderungen an DS-Archiv	Transportmodalitäten	Aufbewahrungsmodalität
Verfügbarkeitsanforderungen	X	(X)	X	X	X	X	X	X	

Tabelle H.2: Datensicherung: Abhängigkeiten zwischen den Modalitäten einer Datensicherung und den Einflußfaktoren. X bedeutet direkter Einfluß, (X) bedeutet indirekter Einfluß

Rekonstruktionsaufwand ohne Datens.		(X)	X						
Datenvolumen	X		X	X		X	X	X	
Änderungsvolumen	X	X	X	X					
Änderungszeitpunkte der Daten	(X)	X						(X)	
Fristen				X			X		X
Vertraulichkeitsbedarf der Daten				(X)	X		X	X	X
Integritätsbedarf der Daten			(X)	(X)	X		X	X	X
Kenntnisse der IT-Benutzer	X			X	X				

Erläuterungen:

Art der Datensicherung
Folgende Datensicherungsarten lassen sich aufzeigen:

- Datenspiegelung:
  bei der Datenspiegelung werden die Daten redundant und zeitgleich auf verschiedenen Datenträgern gespeichert. Da es sich meist um schnelle Datenträger handelt, entstehen durch die doppelte Auslegung der Datenträger und durch die notwendige Steuerungssoftware entsprechend hohe Kosten. Der wesentliche Vorteil der Datenspiegelung ist, daß der Ausfall eines dieser Speicher ohne Zeitverlust überbrückt werden kann.

- Volldatensicherung:
  bei der Volldatensicherung werden sämtliche zu sichernden Dateien zu einem bestimmten Zeitpunkt auf einen zusätzlichen Datenträger gespeichert. Es wird dabei nicht berücksichtigt, ob die Dateien sich seit der letzten Datensicherung geändert haben oder nicht. Daher benötigt eine Volldatensicherung einen hohen Speicherbedarf. Der Vorteil ist, daß die Daten vollständig für den Sicherungszeitpunkt vorliegen und die Restaurierung von Dateien einfach und schnell möglich ist, da nur die betroffenen Dateien aus der letzten Volldatensicherung extrahiert werden müssen. Werden Volldatensicherungen selten durchgeführt, so kann sich durch umfangreiche nachträgliche Änderungen innerhalb einer Datei ein hoher Nacherfassungsaufwand ergeben.

- Inkrementelle Datensicherung:
  bei der inkrementellen Datensicherung werden im Gegensatz zur Volldatensicherung nur die Dateien gesichert, die sich gegenüber der letzten Datensicherung (Volldatensicherung oder inkrementelle Sicherung) geändert haben. Dies spart Speicherplatz und verkürzt die erforderliche Zeit für die Datensicherung. Für die Restaurierung der Daten ergibt sich i. allg. ein höherer Zeitbedarf, da die Dateien aus Datensicherungen verschiedener Zeitpunkte extrahiert werden müssen. Die inkrementelle Datensicherung basiert immer auf einer Volldatensicherung. In periodischen Zeitabständen werden Volldatensicherungen erzeugt, in der Zeit dazwischen werden eine oder mehrere inkrementelle Datensicherungen vollzogen. Bei der Restaurierung wird die letzte Volldatensicherung als Grundlage genommen, die um die in der Zwischenzeit geänderten Dateien aus den inkrementellen Sicherungen ergänzt wird.

- Differentielle Datensicherung:
  bei der differentiellen Datensicherung werden nur die Dateien gesichert, die sich gegenüber der letzten Volldatensicherung geändert haben. Eine differentielle Datensicherung benötigt mehr Speicherplatz als eine inkrementelle, Dateien lassen sich aber einfacher und schneller restaurieren. Für die Restaurierung der Daten reicht die letzte Volldatensicherung sowie die aktuellste differentielle, nicht wie bei der inkrementellen, wo u. U. mehrere Datensicherungen nacheinander eingelesen werden müssen.

Eine spezielle Form dieser genannten Datensicherungsstrategien ist die Image-Datensicherung. Bei der Image-Datensicherung werden nicht die einzelnen Dateien eines Festplattenstapels gesichert, sondern die physikalischen Sektoren der Festplatte. Es handelt sich dabei um eine Vollsicherung, die sehr schnell auf eine gleichartige Festplatte restauriert werden kann.

Eine weitere Form ist das Hierarchische Speicher-Management (HSM). Hierbei geht es in erster Linie um die wirtschaftliche Ausnutzung teurer Speicher. Dateien werden abhängig von der Häufigkeit, mit der auf sie zugegriffen wird, auf schnellen Online-Speichern (Festplatten) gehalten, auf Nearline-Speicher (automatische Datenträger-Wechselsysteme) ausgelagert oder auf Offline-Speichern (Magnetbänder) archiviert. Gleichzeitig bieten diese HSM-Systeme i.allg. auch automatische Datensicherungsroutinen kombiniert aus inkrementeller Datensicherung und Volldatensicherung.
Eine redundante Datenspeicherung bieten RAID-Systeme an (Redundant Array of Inexpensive Disks). Das RAID-Konzept beschreibt die Verbindung von mehreren Festplatten unter dem Kommando eines sogenannten Array-Controllers. Man unterscheidet verschiedene RAID-Level, wovon RAID-Level 1 die Datenspiegelung beschreibt.

RAID-Systeme ersetzen keine Datensicherung! RAID-Systeme helfen nicht bei Diebstahl oder Brand, daher müssen auch die auf RAID-Systemen gespeicherten Daten auf zusätzliche Medien gesichert werden und diese Medien auch in anderen Brandabschnitten untergebracht werden.

Für die Entscheidung, welche Datensicherungsstrategie angewendet werden soll, sind die folgenden Einflußfaktoren zu berücksichtigen, um eine für die Anforderungen geeignete und gleich-

zeitig wirtschaftliche Form zu finden:

Verfügbarkeitsanforderungen:
Sind die Verfügbarkeitsanforderungen sehr hoch, so ist eine Datenspiegelung in Erwägung zu ziehen, sind die Verfügbarkeitsanforderungen hoch, so sollte einer Volldatensicherung gegenüber der inkrementellen Datensicherung der Vorzug gegeben werden.
Datenvolumen und Änderungsvolumen:
Entspricht das Änderungsvolumen annähernd dem Datenvolumen (z.B. bei der Nutzung einer Datenbank), so verringert sich die Speicherplatzersparnis der inkrementellen Datensicherung so stark, daß eine Vollsicherung in Erwägung gezogen werden kann. Ist jedoch das Änderungsvolumen erheblich kleiner als das Datenvolumen, so spart die inkrementelle Datensicherung Speicherplatz und damit Kosten im großen Umfang.
Änderungszeitpunkte der Daten:
Einen geringen Einfluß auf die Datensicherungsstrategie können die Änderungszeitpunkte der Daten haben. Gibt es Zeitpunkte, an denen anwendungsbezogen der Komplettdatenbestand gesichert werden muß (z.B. nach buchhalterischen Tages-, Wochen-, Monats- oder Jahresabschlüsse), so kommt zu diesen Zeitpunkten nur eine Vollsicherung in Frage.
Kenntnisse der IT-Benutzer:
Die Implementierung einer Datenspiegelung setzt entsprechende Kenntnisse des Systemadministrators voraus, erfordert jedoch auf Seiten der IT-Benutzer keinerlei Kenntnisse. Eine Volldatensicherung läßt sich auch von einem IT-Benutzer mit geringen Systemkenntnissen durchführen. Demgegenüber erfordert eine inkrementelle Datensicherung schon mehr Systemkenntnisse und Erfahrungen im Umgang mit Datensicherungen.

Häufigkeit und Zeitpunkte der Datensicherung
Tritt ein Datenverlust ein (z.B. durch Headcrash auf der Festplatte), so müssen zur Restaurierung der Daten sämtliche Datenänderungen seit der letzten Datensicherung nochmals vollzogen werden. Je kürzer der zeitliche Abstand der Datensicherungen ist, um so geringer ist i. allg. auch der für eine Restaurierung und Nacherfassung erforderliche Zeitaufwand. Gleichzeitig muß beachtet werden, daß der Zeitpunkt der Datensicherung nicht nur periodisch (täglich, wöchentlich, werktags, ...) gewählt werden kann, sondern daß auch ereignisabhängige Datensicherungen (z.B. nach x Transaktionen, nach Ausführung eines bestimmten Programms, nach Systemänderungen) notwendig sein können.

Zur Auswahl der Häufigkeit und Zeitpunkte der Datensicherung sind folgende Einflußfaktoren zu beachten.

Verfügbarkeitsanforderungen, Rekonstruktionsaufwand ohne Datensicherung und Änderungsvolumen:
Der zeitliche Abstand der Datensicherungen ist so zu wählen, daß die Restaurierungs- und Nacherfassungszeit (Rekonstruktionsaufwand der geänderten Daten, für die keine Datensicherung vorhanden ist) der in diesem Zeitraum geänderten Daten (Änderungsvolumen) kleiner als die maximal tolerierbare Ausfallzeit ist.

Änderungszeitpunkte der Daten:
Gibt es Zeitpunkte, an denen sich die Daten in großem Umfang ändern (z.B. Programmlauf für Gehaltszahlung oder Versionswechsel der Software) oder an denen der Komplettdatenbestand vorliegen muß, so bietet es sich an, unmittelbar danach eine Volldatensicherung durchzuführen. Dazu sind neben den periodischen die ereignisabhängigen Datensicherungszeitpunkte festzulegen.

Anzahl der Generationen
Einerseits werden Datensicherungen in kurzen Zeitabständen wiederholt, um eine Kopie eines möglichst aktuellen Datenbestandes verfügbar zu haben, andererseits muß die Datensicherung gewährleisten, daß gesicherte Daten möglichst lange aufbewahrt werden. Bezeichnet man eine Volldatensicherung als Generation, so bedarf es einer Festlegung der Anzahl der aufzubewahrenden Generationen und des zeitlichen Abstandes, der zwischen den Generationen liegen muß. Diese Anforderungen lassen sich an folgenden Beispielen erläutern:

- Wird eine Datei absichtlich oder unabsichtlich gelöscht, so ist diese Datei in allen späteren Datensicherungen nicht mehr verfügbar. Stellt sich heraus, daß diese gelöschte Datei dennoch benötigt wird, so muß zur Restaurierung auf eine ältere Datensicherung zurückgegriffen werden, die zeitlich vor dem Löschen erstellt wurde. Ist eine solche Generation nicht mehr vorhanden, so muß die Datei neu erfaßt werden.

- Tritt ein Integritätsverlust in einer Datei auf (z.B. durch einen technischen Defekt, durch unbeabsichtigtes Ändern einer Datei oder durch einen Computer-Virus), so ist es wahrscheinlich, daß dies nicht direkt, sondern erst zeitlich versetzt bemerkt wird. Um die Integrität der Datei wiederherstellen zu können, muß dann auf eine Generation zurückgegriffen werden, die vor dem Integritätsverlust erstellt wurde.

- Es kann nicht ausgeschlossen werden, daß die Erstellung einer Datensicherung fehlerhaft oder unvollständig durchgeführt wurde. In diesem Fall ist es oftmals hilfreich, wenn auf eine weitere Generation zurückgegriffen werden kann.

Um diese Vorteile des Generationenprinzips aufrechterhalten zu können, muß jedoch eine Randbedingung eingehalten werden: der zeitliche Abstand der Generationen darf ein Mindestmaß nicht unterschreiten. Beispiel: In einem automatisierten Datensicherungsverfahren kommt es zu wiederholten Abbrüchen des Datensicherungslaufs. Hierdurch würden nacheinander sämtliche Generationen überschrieben werden. Verhindert werden kann dies, indem vor Überschreiben einer Generation das Mindestalter überprüft und nur dann überschrieben wird, wenn dieses Alter überschritten ist.

Charakterisieren läßt sich ein Generationsprinzip durch zwei Größen: das Mindestalter der ältesten Generation und die Anzahl der verfügbaren Generationen. Dabei gilt:

- je höher das Mindestalter der ältesten Generation ist, je größer ist die Wahrscheinlichkeit, daß zu einer Datei mit Integritätsverlust (eine gelöschte Datei, die im nachhinein

als notwendig erkannt wird, ist ebenfalls darunter zu fassen) noch eine Vorläuferversion vorhanden ist,

- je größer die Anzahl der verfügbaren Generationen ist, um so aktueller ist die angeforderte Vorläuferversion.

Die Anzahl der Generationen steht aber im direkten Zusammenhang mit den Kosten der Datensicherung, da Datenträger in ausreichender Zahl zur Verfügung stehen müssen. Dies folgt aus der Notwendigkeit, daß für jede Generation eigene Datenträger benutzt werden sollten. Aus Wirtschaftlichkeitsgründen muß daher die Anzahl der Generationen auf ein sinnvolles Maß beschränkt werden.
Für die Wahl der Parameter des Generationsprinzips ergeben sich folgende Einflüsse:

Verfügbarkeitsanforderungen und Integritätsbedarf der Daten:
Je höher die Verfügbarkeitsanforderungen oder der Integritätsbedarf der Daten sind, um so mehr Generationen müssen vorhanden sein, um im Fall des Integritätsverlustes die Restaurierungszeit zu minimieren. Wenn der Verlust einer Datei oder eine Integritätsverletzung möglicherweise erst sehr spät bemerkt werden kann, sind zusätzliche Quartals- oder Jahressicherungsdatenbestände empfehlenswert.

Rekonstruktionsaufwand ohne Datensicherung:
Sind die Daten zwar umfangreich, aber auch ohne Datensicherung rekonstruierbar, so kann dies als eine weitere „Pseudo-Generation“ ins Kalkül gezogen werden.

Datenvolumen:
Je höher das Datenvolumen ist, desto höher sind auch die Kosten einer Generation aufgrund des benötigten Speicherplatzes. Ein hohes Datenvolumen kann deshalb die Anzahl der Generationen aus wirtschaftlichen Gründen beschränken.

Änderungsvolumen:
Je höher das Änderungsvolumen ist, um so kürzer sollten die Zeitabstände zwischen den Generationen sein, um eine möglichst zeitnahe Version der betreffenden Datei zu haben, um den Restaurierungsaufwand durch Nachbearbeitung gering zu halten.

Vorgehensweise und Speichermedium
Nach der Festlegung der Art der Datensicherung, der Häufigkeit und des Generationenprinzips gilt es nun, die Vorgehensweise einschließlich des erforderlichen und wirtschaftlich angemessenen Datenträgers auszuwählen. Zunächst sollen einige gängige Datensicherungsverfahren beispielhaft aufgezeigt werden:

Beispiel 1: Manuelle dezentrale Datensicherung am PC
Bei nichtvernetzten PCs wird die Datensicherung vom IT-Anwender meist manuell als Vollsicherung der Anwendungsdaten durchgeführt. Als Speichermedium werden Disketten verwendet.

Beispiel 2: Manuelle zentrale Datensicherung im Unix-System
Für Unix-Systeme mit angeschlossenen Terminals oder PCs mit Terminalemulation bietet sich aufgrund des zentralen Datenbestandes die zentrale Datensicherung an. Sie wird oft als Kombination von wöchentlichen Vollsicherungen und täglichen inkrementellen Datensicherungen mittels Streamer-Tapes vom Unix-Administrator manuell durchgeführt.

Beispiel 3: Manuelle zentrale Datensicherung im lokalen Netz
Im Bereich eines lokalen Netzes mit angeschlossenen PCs wird vielfach die Datensicherung dergestalt durchgeführt, daß der angeschlossene PC-Benutzer seine zu sichernden Anwendungsdaten auf einem zentralen Server im Netz ablegt und daß dann der Netzadministrator die Daten dieses Servers zentral sichert, wozu eine wöchentliche Vollsicherung und eine tägliche inkrementelle Sicherung durchgeführt werden.

Beispiel 4: Automatische zentrale Datensicherung im Großrechnerbereich
Vergleichbar dem Beispiel 2 werden im Großrechnerbereich zentrale Datensicherungen als Kombination von wöchentlichen Vollsicherungen und täglichen inkrementellen Datensicherungen durchgeführt. Vielfach wird dies automatisch mit Hilfe eines Tools (HSM) initiiert. Für einzelne IT-Anwendungen werden vielfach noch zusätzliche ereignisorientierte Volldatensicherungen vollzogen.

Beispiel 5: Automatische zentrale Datensicherung im verteilten System
Eine weitere Variante besteht aus der Kombination der Beispiele 3 und 4. Die lokalen Daten der verteilten Systeme werden auf einen zentralen Großrechner bzw. auf einen zentralen Server übertragen, auf dem die Datensicherung als Kombination von Vollsicherungen und inkrementellen Datensicherungen durchgeführt wird.

Beispiel 6: Voll-automatische zentrale Datensicherung dezentral gespeicherter Daten im verteilten System
Im Gegensatz zum vorangegangenen Beispiel erfolgt hier der Transfer vom dezentralen zum zentralen System automatisch. Mittlerweile werden Tools angeboten, die einen Zugriff von einem zentralen Datensicherungsserver auf die dezentralen Datenbestände erlauben. Eine Datensicherung kann somit transparent für den dezentralen Anwender zentral erfolgen.

Um das Datenvolumen auf dem Speichermedium zu minimieren, können zusätzlich Datenkompressionsalgorithmen angewandt werden. Teilweise kann das Datenvolumen damit um bis zu 80 % reduziert werden. Es ist bei Anwendung der Kompression sicherzustellen, daß die gewählten Parameter und Algorithmen im Rahmen der Datensicherung dokumentiert und für die Datenrestaurierung (Dekompression) vorgehalten werden.

Für die Vorgehensweise gibt es zwei Parameter, die festgelegt werden müssen: den Automatisierungsgrad und die Zentralisierung (Speicherort).

Beim Automatisierungsgrad ist zwischen manuell und automatisch zu unterscheiden:

- Manuelle Datensicherung bedeutet, daß der Anstoß zur Datensicherung manuell gegeben wird. Vorteilhaft kann sein, daß der Ausführende individuell den Termin der Datensicherung dem Arbeitsablauf anpassen kann. Nachteilig ist, daß die Wirksamkeit und Güte der Datensicherung dann von der Motivation und Disziplin des Ausführenden abhängt. Durch Krankheit oder sonstige Abwesenheitsgründe können Datensicherungen ausfallen.

- Automatische Datensicherungen werden programmgesteuert zu bestimmten Terminen angestoßen. Vorteilhaft ist, daß die Disziplin und Zuverlässigkeit der Ausführenden nachrangig ist, wenn der Terminplan vollständig und aktuell ist. Nachteilig kann sein, daß die Steuerungsprogramme Kosten verursachen, der Terminplan aktuellen Änderungen angepaßt werden muß oder wichtige Änderungen nicht unmittelbar gesichert werden.

Bezüglich der Zentralisierung sind zentral und dezentral durchgeführte Datensicherungen zu unterscheiden:

- Zentrale Datensicherungen zeichnen sich dadurch aus, daß der Speicherort und die Durchführung der Datensicherung am zentralen IT-System von einem Ausführenden durchgeführt werden. Diese Verfahrensweise hat den Vorteil, daß nur ein Mitarbeiter intensiv geschult werden muß und die IT-Anwender des IT-Systems von dieser Arbeit entlastet werden. Vorteilhaft ist weiterhin, daß durch das höhere zentrale Datenaufkommen kostengünstigere Speichermedien verwendet werden können. Nachteilig ist, daß evtl. vertrauliche Daten übertragen und von nicht Befugten eingesehen werden könnten.

- Dezentrale Datensicherungen werden von den IT-Anwendern selbst durchgeführt, ohne daß die Daten auf ein zentrales IT-System übertragen werden müssen. Vorteilhaft ist, daß der IT-Anwender die Kontrolle über die Daten und die Backup-Datenträger behält, insbesondere wenn es sich um vertrauliche Daten handelt. Nachteilig ist, daß die konsequente Datensicherung damit von der Zuverlässigkeit der IT-Anwender abhängt und daß dezentrale Lösungen den IT-Anwendern Zeitaufwand abfordern.

Nach der Entscheidung, ob die Datensicherung manuell oder automatisch, zentral oder dezentral durchgeführt wird, muß nun der geeignete Datenträger für die Datensicherung gefunden werden. Dazu können folgende Parameter betrachtet werden:

- Datenträger-Anforderungszeit: der Zeitaufwand für die Vorbereitung der Daten-Restaurierung ist bestimmt durch die Zeit, die benötigt wird, den erforderlichen Datensicherungs-Datenträger zu identifizieren und im System verfügbar zu machen. Kassetten in einem Roboter-System können innerhalb von Minuten zur Restaurierung bereit stehen, ausgelagerte Bänder müssen unter Umständen erst aufwendig transportiert und aufgelegt werden.

- Zugriffszeit, Transferrate: der Zeitaufwand für die Erstellung und Restaurierung der Daten selbst hängt von der mittleren Zugriffszeit auf die Daten des Datenträgers und von der Datentransferrate ab. Festplatten erlauben einen Zugriff auf bestimmte Dateien im Millisekunden-Bereich, ein Magnetband muß erst zur entsprechenden Stelle gespult werden. Bei der Auswahl des Datenträgers ist zu berücksichtigen, daß bei entsprechend hohen Transferraten es nicht zu einer Überlastung der Übertragungskanäle kommen darf.

- Praktikabilität/ Speicherkapazität: je umständlicher die Datensicherung ist, um so größer ist die Gefahr, daß sie fehlerhaft vollzogen oder von den Verantwortlichen überhaupt nicht durchgeführt wird. Datenträger mit zu kleiner Speicherkapazität verhindern eine effektive Datensicherung, da der ständige Wechsel zeitaufwendig und fehleranfällig ist.

- Kosten: die Kosten für die Datensicherung, also Beschaffungskosten für Lese-/ Schreibgeräte und Datenträger, erforderliche Rechen- und Arbeitszeit müssen in einem angemessenen Verhältnis zum Sicherungszweck stehen. Hierbei ist auch die Lebensdauer der Datenträger und der Zuverlässigkeit zu berücksichtigen. Auf keinen Fall dürfen die laufenden Datensicherungskosten die Summe der Restaurierungskosten ohne Datensicherung und der Folgeschäden übersteigen.

Um bei der Auswahl der Verfahrensweise und des Speichermediums Anhaltspunkte für die Beschaffungskosten, die Zugriffszeiten und Transferzeiten zu haben, sind in der nachfolgenden Tabelle mit Stand von 1995 einige Eckdaten dargestellt:

Tabelle H.3: Speichermedien: Zugriffszeiten und Transferzeiten

Speichermedium	Kapazität MB	Kosten DM	Kosten pro MB	Mittlere Zugriffszeit in Sek.	Datentransfer in KB/Sek.
DIN-A4-Papier	0,002	0,03	15,00	-	-
IDE Festplatte HDD 1 GB	1000	400,00	0,400	0,01	3000
SCSI Festplatte 4 GB	4000	2000,00	0,500	0,08	6000
3.5 "HD Floppy	1,44	1,00	0,700	0,10	60
WORM 5.25"	800	700,00	0,870	0,02	6000
Mikrofilm	0,6	0,50	0,830	10,00	40
MO/ROD 3,5" 5,25"	230 1300	40,00 120,00	0,170 0,090	0,03	lesen 3000 schreiben 1000
CD-WORM	680	15,00	0,022	0,15	300-600
CD-ROM	680	2,00	0,003	0,15	600-1200
Data Cartridge QIC DAT	2500 4000	60,00 30,00	0,020 0,008	10,00	200 ... 800
Magn. Wechselplatten	270	100,00	0,370	0,015	2000

Aufgrund des Preisverfalls im Bereich der Speichermedien und der technologischen Fortschritte können diese Zahlen nur als grobe Näherungswerte betrachtet werden. Aktuelle Zahlen sind bei der Speichermedien-Auswahl zu eruieren.
Die folgenden Einflußgrößen müssen dabei beachtet werden:

Verfügbarkeitsanforderungen:
Je höher die Verfügbarkeitsanforderungen sind, desto schneller muß auf die Datenträger als Speichermedium der Datensicherung zugegriffen werden können und desto schneller müssen die benötigten Daten vom Datenträger wieder einspielbar sein.
Aus Verfügbarkeitsgründen muß sichergestellt sein, daß die Speichermedien auch bei Ausfall eines Lesegerätes zur Restaurierung genutzt werden können. Die Kompatibilität und Funktion eines Ersatzgerätes ist zu gewährleisten.

Daten- und Änderungsvolumen:
Mit zunehmenden Datenvolumen werden i. allg. preisgünstige Bandspeichermedien wie Magnetbänder oder Bandkassetten (Data Cartridge) benutzt.
Fristen:
Müssen Löschfristen eingehalten werden (z. B. bei personenbezogenen Daten), so muß das ausgewählte Speichermedium die Löschung ermöglichen. Speichermedien, die nicht oder nur mit großem Aufwand löschbar sind (z. B. WORM), sollten in diesem Fall vermieden werden.

Vertraulichkeitsbedarf und Integritätsbedarf der Daten:
Ist der Vertraulichkeits- oder Integritätsbedarf der zu sichernden Daten hoch, so überträgt sich dieser Schutzbedarf auch auf die zur Datensicherung eingesetzten Datenträger. Ist eine Verschlüsselung der Datensicherung nicht möglich, kann über die Auswahl von Datenträgern nachgedacht werden, die aufgrund ihrer kompakten Bauart und Transportabilität in Datensicherungsschränken oder Tresoren untergebracht werden können.

Kenntnisse der IT-Benutzer:
Die Kenntnisse und datenverarbeitungsspezifische Fähigkeiten der IT-Benutzer entscheiden darüber, ob eine Verfahrensweise gewählt werden kann, in der der IT-Benutzer selbst manuell für die Datensicherung tätig wird, ob andere ausgebildete Personen die Datensicherung dezentral durchführen oder ob eine automatisierte Datensicherung praktikabler ist.

Verantwortlichkeit für die Datensicherung
Für die Entscheidung, wer für die Durchführung der Datensicherung verantwortlich ist, kommen drei Personengruppen in Frage. Zunächst kann es der IT-Benutzer selbst sein (typischerweise bei dezentralen und nichtvernetzen IT-Systemen), der Systemverwalter oder ein für die Datensicherung speziell ausgebildeter Administrator. Wird die Datensicherung nicht vom Benutzer selbst durchgeführt, sind die Verantwortlichen auf Verschwiegenheit bezüglich der Dateninhalte zu verpflichten und ggf. eine Verschlüsselung in Betracht zu ziehen.

Darüber hinaus sind die Entscheidungsträger zu benennen, die eine Daten-Restaurierung veranlassen können. Zu klären ist weiterhin, wer berechtigt ist, auf Datensicherungsträger zuzugreifen, insbesondere wenn sie in Datensicherungsarchiven ausgelagert sind. Es muß sichergestellt sein, daß nur Berechtigte Zutritt erhalten. Abschließend ist zu definieren, wer berechtigt ist, eine Daten-Restaurierung des Gesamtdatenbestandes oder ausgewählter, einzelner Dateien operativ durchzuführen. Bei der Festlegung der Verantwortlichkeit ist insbesondere der Vertraulichkeits-,

Integritätsbedarf der Daten und die Vertrauenswürdigkeit der zuständigen Mitarbeiter zu betrachten. Es muß sichergestellt werden, daß der Verantwortliche erreichbar ist und ein Vertreter benannt und eingearbeitet wird.

Als Einflußfaktor ist zu beachten:
Kenntnisse der IT-Anwender:
Die Kenntnisse und datenverarbeitungsspezifischen Fähigkeiten der IT-Benutzer entscheiden darüber, ob die Datensicherung eigenverantwortlich je IT-Benutzer durchgeführt werden sollte. Sind die Kenntnisse der IT-Benutzer nicht ausreichend, ist die Verantwortung dem Systemadministrator oder einer speziell ausgebildeten Person zu übertragen.

Aufbewahrungsort
Grundsätzlich sollten Datensicherungsmedien und Originaldatenträger in unterschiedlichen Brandabschnitten aufbewahrt werden. Werden Datensicherungsmedien in einem anderen Gebäude oder außerhalb des Betriebsgeländes aufbewahrt, so sinkt die Wahrscheinlichkeit, daß in einem Katastrophenfall die Datensicherungen in Mitleidenschaft gezogen werden. Je weiter jedoch die Datenträger von der zur Restaurierung notwendigen IT-Peripherie (z.B. Bandstation) entfernt ist, desto länger können die Transportwege und Transportzeiten sein, und desto länger ist die Gesamtrestaurierungszeit. Als Einflußfaktor ist daher zu betrachten:

Verfügbarkeitsanforderungen:
Je höher die Verfügbarkeitsanforderungen sind, um so schneller müssen die Datenträger der Datensicherung verfügbar sein. Werden aus Sicherheitsgründen die Datenträger extern ausgelagert, so ist bei sehr hohen Verfügbarkeitsanforderungen zu erwägen, Kopien der Datensicherung zusätzlich in unmittelbarer Nähe des IT-Systems vorzuhalten.

Vertraulichkeitsbedarf und Integritätsbedarf der Daten:
Je höher dieser Bedarf ist, um so besser muß verhindert werden, daß an den Datenträgern manipuliert werden kann. Die notwendige Zutrittskontrolle läßt sich i.allg. nur durch entsprechende infrastrukturelle und organisatorische Maßnahmen erreichen, vgl. Kapitel 4.3.3 - Datenträgerarchiv in [BSI1998].

Datenvolumen:
Mit steigendem Datenenvolumen gewinnt die Sicherheit des Aufbewahrungsortes an Bedeutung.

Anforderungen an das Datensicherungsarchiv
Aufgrund der Konzentration von Daten auf Datensicherungsmedien besitzen diese einen mindestens ebenso hohen Schutzbedarf bezüglich Vertraulichkeit und Integrität wie die gesicherten Daten selbst. Bei der Aufbewahrung in einem zentralen Datensicherungsarchiv sind daher entsprechend wirksame IT-Sicherheitsmaßnahmen wie z.B. Zutrittskontrolle notwendig.
Zusätzlich muß durch organisatorische und personelle Maßnahmen (Datenträgerverwaltung) sichergestellt werden, daß der schnelle und gezielte Zugriff auf benötigte Datenträger möglich ist. Hierzu sind die Maßnahme M 2.3 - Datenträgerverwaltung und Kapitel 4.3.3 - Datenträgerar-

chiv in [BSI1998] zu beachten.

Folgende Einflußfaktoren müssen beachtet werden:
Verfügbarkeitsanforderungen:
Je höher die Verfügbarkeitsanforderungen sind, um so schneller muß der gezielte Zugriff auf benötigte Datenträger möglich sein. Wenn eine manuelle Bestandsführung den Verfügbarkeitsanforderungen nicht genügt, können automatisierte Zugriffsverfahren (z.B. Roboter-Kassettenarchiv) zum Einsatz kommen.

Datenvolumen:
Das Datenvolumen bestimmt letztendlich die Anzahl der aufzubewahrenden Datenträger. Für entsprechend große Datenvolumen ist eine ausreichende Aufbewahrungskapazität im Datenträgerarchiv vorzusehen.

Fristen:
Sind Löschungsfristen einzuhalten, muß die Organisation des Datensicherungsarchivs dem angepaßt sein und ggf. müssen auch die erforderlichen Löscheinrichtungen vorhanden sein. Zu den vorgegebenen Löschungszeitpunkten ist im Datensicherungsarchiv die Löschung zu initiieren bzw. durchzuführen und zu dokumentieren. Ist eine Löschung technisch nicht möglich, so ist durch organisatorische Maßnahmen eine Wiederverwendung zu löschender Daten zu verhindern.

Vertraulichkeits- und Integritätsbedarf der Daten:
Je höher dieser Bedarf ist, um so besser muß verhindert werden, daß an den Datenträgern manipuliert werden kann. Die notwendige Zutrittskontrolle läßt sich i.allg. nur durch entsprechende infrastrukturelle und organisatorische Maßnahmen erreichen vergleichbar dem Kapitel 4.3.3 - Datenträgerarchiv in [BSI1998].
Transportmodalitäten
Bei der Durchführung einer Datensicherung werden Daten transportiert. Sei es, daß sie über ein Netz oder eine Leitung übertragen werden, sei es, daß Datenträger zum Datenträgerarchiv transportiert werden. Dabei gilt es folgendes zu beachten:

Verfügbarkeitsanforderungen:
Je höher die Verfügbarkeitsanforderungen sind, desto schneller müssen die Daten zur Restaurierung bereitstellbar sein. Dies ist bei der Auswahl des Datenübertragungsmediums bzw. bei Auswahl des Datenträger-Transportweges zu berücksichtigen.

Datenvolumen:
Wenn zur Datenrestaurierung die Daten über ein Netz übertragen werden, so muß bei der Auswahl der Übertragungskapazität des Netzes das Datenvolumen beachtet werden. Es muß gewährleistet sein, daß das Datenvolumen innerhalb der erforderlichen Zeit (Verfügbarkeitsanforderung) übertragen werden kann.

Änderungszeitpunkte der Daten:

Werden Datensicherungen über ein Netz durchgeführt (insbesondere zu ausgewählten Terminen), kann aufgrund des zu übertragenen Datenvolumens ein Kapazitätsengpaß entstehen. Daher ist zum Zeitpunkt der Datensicherung eine ausreichende Datenübertragungskapazität sicherzustellen.

Vertraulichkeits- und Integritätsbedarf der Daten:
Je höher dieser Bedarf ist, um so besser muß verhindert werden, daß die Daten auf dem Transport abgehört, unbefugt kopiert oder manipuliert werden. Bei Datenübertragungen ist schließlich eine Verschlüsselung oder ein kryptographischer Manipulationsschutz zu überdenken, beim physikalischen Transport sind sichere Behältnisse und Wege zu benutzen und ggf. auch der Nutzen und Aufwand einer Verschlüsselung abzuwägen.

Aufbewahrungsmodalität
Im Rahmen des Datensicherungskonzeptes sollte mitbetrachtet werden, ob für bestimmte Daten Aufbewahrungs- oder Löschfristen einzuhalten sind.

Fristen:
Falls Aufbewahrungsfristen einzuhalten sind, kann dem durch die Archivierung einer Datensicherungsgeneration nachgekommen werden. Sind die Aufbewahrungsfristen lang, so ist zusätzlich sicherzustellen, daß die erforderlichen Lesegeräte bevorratet werden und daß unter Umständen ein Refresh (erneutes Aufspielen der magnetisch gespeicherten Daten) bei magnetischen Datenträgern erforderlich werden kann, da diese mit der Zeit ihre Magnetisierung und damit den Dateninhalt verlieren.

Falls Löschfristen einzuhalten sind, muß der organisatorische Ablauf festgelegt werden und ggf. müssen auch die erforderlichen Löscheinrichtungen vorhanden sein. Zu den vorgegebenen Löschungszeitpunkten ist die Löschung zu initiieren bzw. durchzuführen.

M 6.36 Festlegung des Minimaldatensicherungskonzeptes
Für ein Unternehmen/eine Behörde ist festzulegen, welche Minimalforderungen zur Datensicherung eingehalten werden müssen. Damit können viele Fälle, in denen eingehende Untersuchungen und die Erstellung eines Datensicherungskonzeptes zu aufwendig sind, pauschal behandelt werden. Weiterhin ist damit eine Grundlage gegeben, die generell für alle IT-Systeme gültig ist und auch für neue IT-Systeme, für die noch kein Datensicherungskonzept erarbeitet wurde.

Ein Beispiel soll dies erläutern: Minimaldatensicherungskonzept

- *Software:*
  Sämtliche Software, erworben oder selbst erstellt, ist einmalig mittels einer Vollsicherung zu sichern.

- *Systemdaten:*
  Systemdaten sind mindestens einmal monatlich mit einer Generation zu sichern.

- *Anwendungsdaten:*
  Alle Anwendungsdaten sind mindestens einmal monatlich mittels einer Vollsicherung im Drei-Generationen-Prinzip zu sichern.

- *Protokolldaten:*
  Sämtliche Protokolldaten sind mindestens einmal monatlich mittels einer Vollsicherung im Drei-Generationen-Prinzip zu sichern.

M 6.37 Dokumentation der Datensicherung
In einem Datensicherungskonzept muß festgelegt werden, wie die Dokumentation der Datensicherung zu erfolgen hat. Für eine ordnungsgemäße und funktionierende Datensicherung ist eine Dokumentation erforderlich. So ist bei der Erstellung der Datensicherung für jedes IT-System zu dokumentieren:

- das Datum der Datensicherung,
- der Datensicherungsumfang (welche Dateien/Verzeichnisse wurden gesichert),
- der Datenträger, auf dem die Daten im operativen Betrieb gespeichert sind,
- der Datenträger, auf dem die Daten gesichert wurden,
- die für die Datensicherung eingesetzte Hard- und Software (mit Versionsnummer) und
- die bei der Datensicherung gewählten Parameter (Art der Datensicherung usw.).

Darüber hinaus bedarf es einer Beschreibung der Vorgehensweise für die Wiederherstellung eines Datensicherungsbestandes. Auch hier muß eine Beschreibung der erforderlichen Hard- und Software, der benötigten Parameter und der Vorgehensweise, nach der die Datenrekonstruktion zu erfolgen hat, erstellt werden.

M 6.38 Sicherungskopie der übermittelten Daten
Sind die zu übertragenden Daten nur zum Zweck der Datenübertragung erstellt bzw. zusammengestellt worden und nicht auf einem weiteren Medium gespeichert, sollte eine Sicherungskopie dieser Daten vorgehalten werden. Bei Verlust oder Beschädigung des Datenträgers kann der Versand mit geringfügigem Aufwand erneut erfolgen.

M 6.39 Auflistung von Händleradressen zur Fax-Wiederbeschaffung
Es sollte in den Not- und Katastrophenplan eine Liste von Fachhändlern für Fax-Geräte aufgenommen werden, bei denen im Notfall unverzüglich neue Geräte beschafft werden können, wenn eine Reparatur aus Zeitgründen nicht möglich ist.

M 6.40 Regelmäßige Batterieprüfung/-wechsel
Batterien und Akkumulatoren verlieren mit der Zeit ihre Kapazität. Daher sollten bei Anrufbeantwortern mit digitaler Ansagetext- oder Anrufspeicherung diese Energiequellen für die

Notstromversorgung regelmäßig ausgewechselt werden. In der Regel sollte ein Batteriewechsel im Jahresrhythmus erfolgen.

M 6.41 Übungen zur Datenrekonstruktion
Die Rekonstruktion von Daten mit Hilfe von Datensicherungsbeständen muß sporadisch, zumindestens aber nach jeder Änderung des Datensicherungsverfahrens, getestet werden. Hierbei muß zumindest einmal nachgewiesen werden, daß eine vollständige Datenrekonstruktion (z.B. der Gesamtdatenbestand eines Servers) möglich ist. Auf diese Weise kann zuverlässig ermittelt werden, ob

- die Datenrekonstruktion überhaupt möglich ist,
- Verfahrensweise der Datensicherung praktikabel ist,
- eine ausreichende Dokumentation der Datensicherung vorliegt, damit ggf. auch ein Vertreter die Datenrekonstruktion vornehmen kann und
- die erforderliche Zeit zur Datenrekonstruktion den Anforderungen an die Verfügbarkeit entspricht (siehe M 6.1 - Erstellung einer Übersicht über Verfügbarkeitsanforderungen).

Bei Übungen zur Datenrekonstruktion sollte auch berücksichtigt werden, daß

- die Daten ggf. auf einem Ausweich-IT-System installiert werden müssen,
- für die Datensicherung und Datenrekonstruktion unterschiedliche Schreib-/Lesegeräte benutzt werden.

M 6.42 Erstellung von Rettungsdisketten für Windows NT
Für jedes unter Windows NT betriebene System, das über ein Diskettenlaufwerk verfügt, sollte ein Satz von Reparaturdisketten bereitgehalten werden. Dieser besteht für Rechner mit Intel-Prozessoren aus den drei Setup-Disketten, die mit Windows NT geliefert werden, sowie einer Notfalldiskette, mit der sich der anfängliche Setup-Status wiederherstellen läßt, wenn Dateien beschädigt werden. Für jeden Rechner muß eine eigene Notfalldiskette erstellt werden, da diese Disketten nicht zwischen verschiedenen Rechnern ausgetauscht werden können.
Während des Windows NT Setup wird der Benutzer gefragt, ob er eine Notfalldiskette erstellen will. Zur Erstellung der Notfalldiskette muß eine leere 3 1/2"-Diskette auf Anforderung in Laufwerk A: eingelegt werden, auf der dann die zur Reparatur des Systems benötigten Informationen gespeichert werden.

Sofern bei der Installation keine Notfalldiskette erstellt wurde, kann diese auch nachträglich mit dem Dienstprogramm RDISK (im Windows-Systemverzeichnis %SystemRoot%\SYSTEM32, z.B. \WINNT\SYSTEM32) erzeugt werden. Das Programm ist mit dem Parameter /s zu starten, wenn die Benutzerkonten und die Zugriffsberechtigungen mit gesichert werden sollen. Die Wahl dieses Parameters kann jedoch dazu führen, daß die Sicherung nicht mehr auf eine Diskette paßt, wenn auf dem betreffenden System eine größere Anzahl von Benutzerprofilen

definiert ist. Daher sollte zunächst die Option „Notfall-Informationen aktualisieren“ gewählt werden, um den aktuellen Systemzustand zu retten, und dann sollte mit der Option „Erstellen einer Notfalldiskette“ die eigentliche Notfalldiskette generiert werden.
Hinweis: Dieser Prozeß sollte nach jeder Veränderung der Systemkonfiguration wiederholt werden, damit die Notfalldiskette stets den aktuellen Systemzustand widerspiegelt. Nur so wird sichergestellt, daß in den Reparaturinformationen neue Angaben zur Konfiguration, wie Zuweisung von Laufwerkbuchstaben, Stripe Sets, Datenträgersätzen, Spiegelungen usw. berücksichtigt werden. Im anderen Fall kann der Zugriff auf bestimmte Laufwerke nach Systemfehlern unmöglich sein. Die Erstellung der Notfalldiskette sollte nach dem nächsten erfolgreichen Systemstart durchgeführt werden, um sicher zu sein, daß eine lauffähige Systemversion gesichert wird.

Falls keine Setup-Disketten verfügbar sind, können diese mit dem Windows NT Setup-Programm (WINNT für das Setup von MS-DOS oder Windows 95, WINNT32 für das Setup von Windows NT aus) der Windows NT Installations-CD erzeugt werden, indem dieses Programm mit dem Parameter /ox aufgerufen wird. Das Programm fordert dann drei leere 3 1/2 ¨Disketten in Laufwerk A: an und kopiert die zum Starten von Windows NT benötigten Dateien auf diese Disketten.

Falls Systemdateien, Bootvariablen oder der Bootsektor beschädigt werden, und sich die vorherige Startkonfiguration mit der Methode der letzten als funktionierend bekannten Konfiguration nicht wiederherstellen läßt, muß der Reparaturprozeß im Windows NT Setup verwendet werden, um den ursprünglichen Systemzustand wiederherzustellen.

Zum Reparieren einer Windows NT Installation benötigt das Setup-Programm entweder die Konfigurationsinformationen, die im Unterverzeichnis REPAIR des Windows-Verzeichnisses %SystemRoot%, z.B. in \WINNT\REPAIR, gespeichert sind, oder die Notfalldiskette. Zum Wiederherstellen einer beschädigten Windows NT Installation ist die erste der drei Setup-Disketten in Laufwerk A: einzulegen und der Rechner dann von diesem Laufwerk aus zu booten. Im Textbildschirm des Setup-Programms, in dem gefragt wird, ob Windows NT installiert oder Dateien repariert werden sollen, ist der Parameter r einzugeben. Das Setup-Programm fragt dann nach der Notfalldiskette. Falls keine Notfalldiskette vorhanden ist, zeigt das Setup-Programm eine Liste der vorhandenen Windows NT Installationen an, die auf dem Computer gefunden wurden, und fragt, welche Installation repariert werden soll. Nach Erscheinen der abschließenden Meldung ist die Notfalldiskette aus Laufwerk A: zu entfernen und der Rechner neu zu starten.

Der Reparaturprozeß im Setup-Programm ermöglicht es, verschiedene Elemente zur Reparatur auszuwählen:

- Systemdateien - Das Setup-Programm überprüft die Übereinstimmung des Verzeichnisbaumes von Windows NT mit der Protokolldatei auf der Notfalldiskette, um sicherzustellen, daß alle Systemdateien vorhanden und unbeschädigt sind. Fehlen Dateien oder werden beschädigte Dateien gefunden, so werden diese von der jeweiligen Windows NT

Setup-Quelle (z.B. CD-ROM) wiederhergestellt. Das Setup-Programm überprüft auch die Windows NT Dateien auf der System-Partition, um sicherzustellen, daß alle Bootdateien vorhanden und unbeschädigt sind.

- Standard-Systemkonfiguration - Das Setup-Programm bietet die Möglichkeit, fehlerhafte Dateien der Registrierung aus denjenigen wiederherzustellen, die bei der Installation von Windows NT angelegt wurden. Dabei ist zu beachten, daß Benutzerkonten und Berechtigungen, die seit der ersten Installation bzw. der letzten Aktualisierung der Notfalldiskette eingerichtet wurden, verlorengehen.
- Bootvariablen - Bei Wahl dieser Option stellt das Setup-Programm die Bootvariablen für die spezielle Installation von Windows NT auf der Festplatte von der Notfalldiskette wieder her.
- Bootsektor (nur bei Computern mit x86-Prozessor) - Bei Wahl dieser Option legt das Setup-Programm auf der System-Partition einen neuen Bootsektor an.

Falls andere Dateien fehlen oder beschädigt sind, so stellt das Setup-Programm diese von der entsprechenden Windows NT Setup-Diskette oder von CD-ROM wieder her. Falls die System-Partition auf einem Computer mit x86-Prozessor irrtümlich formatiert oder geändert wurde, so daß Windows NT nicht mehr startet, stellt das Reparaturprogramm die ursprüngliche Bootkonfiguration wieder her.
Hinweis: Wenn die Systemdateien repariert werden, entfernt Setup die Sicherheitseinstellungen von diesen Dateien, falls diese sich auf einer NTFS-Partition befinden. Dies ist sinnvoll, um falsch vergebene Berechtigungen für Systemdateien zurücksetzen zu können, die sonst verhindern würden, daß Windows NT auf die Systemdateien zugreifen kann, die zum Starten des Systems erforderlich sind. Es ist aus diesem Grund unbedingt erforderlich, die Notfalldiskette und die Setup-Disketten so zu verwahren, daß sie gegen Mißbrauch geschützt sind.

M 6.43 Einsatz redundanter Windows NT Server
In Abhängigkeit von den Verfügbarkeitsanforderungen der Daten und Anwendungen ist eine Redundanz zu schaffen, die einem Totalverlust der Daten mit akzeptablem Aufwand vorbeugt. Je nach diesen Anforderungen sind Teile des Datenbestandes oder auch der gesamte Datenbestand parallel auf mehreren Plattenspeichern zu führen, so daß auch bei Ausfall eines Plattenlaufwerks dessen Daten nicht verloren sind und die Benutzer weiterarbeiten können, ohne auf das Wiedereinspielen einer Datensicherung warten zu müssen.
Die Systeme können je nach den definierten Verfügbarkeitsanforderungen so ausgelegt werden, daß bei Ausfall eines Servers dessen Aufgaben von einem oder mehreren anderen Servern übernommen werden können. Dabei muß jedoch dafür gesorgt werden, daß diese verteilten Datenbestände konsistent bleiben, und dies muß auch bei Ausfall einzelner Geräte gewährleistet bleiben. In dieser Beziehung bestehen gravierende Unterschiede hinsichtlich der Leistungsfähigkeit verschiedener Redundanzkonzepte:

- Eine direkte physikalische Redundanz läßt sich mit RAID-Plattensystemen (RAID: Redundant Array of Independent Disks) erreichen. Zu beachten ist bei der Entscheidung

für dieses Verfahren, daß der räumliche Abstand zwischen den einzelnen Platten eines RAID-Systems starken Einschränkungen unterworfen ist, so daß im Falle eines Brandes oder eines ähnlichen Schadens alle Parallelkopien gleichermaßen zerstört werden. RAID-Systeme sind daher kein Ersatz für Datensicherungen.

- Durch Einsatz von Windows NT Clustern können parallele Kopien des Datenbestandes verteilt auf verschiedene Platten und unter Kontrolle verschiedener Rechner geführt werden. Durch die Verwendung leistungsstarker Cluster mit bis zu vier Servern läßt sich die Zahl der Serversysteme reduzieren, was wiederum zu einer Reduktion des Administrationsaufwandes und damit zu einer Verbesserung der Sicherheit führt.

- Die Replikation einzelner Verzeichnisse erlaubt eine ähnlich weite Verteilung der Daten, doch stehen hier keine Synchronisationsmechanismen zur Verfügung, die es erlauben, auch die aktuell in Bearbeitung befindlichen Dateien konsistent parallel zu führen. Ein Ausfall des primären Plattenlaufwerks führt hier somit immer zu mehr oder weniger großen Datenverlusten. Der Einsatz der Replikatordienste unter Windows NT sollte daher auf die Fälle beschränkt bleiben, in denen nur an einer Stelle geändert wird, und er darf keinesfalls als Ersatz für die regelmäßige Durchführung von Datensicherungen angesehen werden.

Um einem Ausfall der Server-Rechner vorzubeugen, sind diese bei Bedarf redundant auszulegen. Hier stehen mehrere Möglichkeiten zur Verfügung, unter denen, ausgehend von der tolerierbaren Ausfallzeit, eine geeignete Alternative auszuwählen ist:

- Wenn Ausfälle in der Größenordnung einer halben Stunde tolerierbar sind, ist ein separater Rechner zur Verfügung zu stellen, der bei Ausfall eines Servers dessen Aufgaben übernimmt. Um Zugriff auf die Daten des ausgefallenen Servers zu erhalten, müssen dessen Plattenlaufwerke auf den Ausweichrechner umgeschaltet werden.

- Wenn Ausfälle von maximal einigen Minuten tolerierbar sind, ist ein Cluster-System mit Zugriff aller Rechner auf alle Platten einzusetzen. Das System ist so zu konfigurieren, daß bei Ausfall eines Servers automatisch auf einen Ersatzrechner innerhalb des Systems umgeschaltet wird.

- Wenn äußerstenfalls Ausfälle im Sekundenbereich toleriert werden können, ist der Einsatz eines voll redundanten, ausfallsicheren Systems mit parallel arbeitenden mehrfachen CPUs erforderlich. In diesem Fall bleibt ein Ausfall einer CPU oder eines Hauptspeichermoduls für den Benutzer unbemerkbar. Diese Lösung bietet somit die größte Ausfallsicherheit, doch ist sie gleichzeitig auch erheblich aufwendiger und teurer als die beiden anderen Lösungen, so daß man nur bei extremen Anforderungen an die Verfügbarkeit auf sie zurückgreifen wird. Windows NT kann derzeit so hohe Anforderungen nicht erfüllen, so daß in diesem Fall Spezialsysteme einzusetzen sind, die unter anderen Betriebssystemen laufen.

Es muß in jedem Fall anhand einer sorgfältigen Analyse festgestellt werden, welche konkreten Verfügbarkeitsanforderungen gegeben sind, und im Rahmen einer detaillierten Planung

der System- und Netzarchitektur muß dann eine geeignete Kombination redundanter Rechner und/oder Plattenlaufwerke gefunden werden, die diesen Anforderungen genügt.

M 6.44 Datensicherung unter Windows NT
Unter Windows NT kann die Datensicherung mit dem zum System gehörigen Dienstprogramm NTBACKUP.EXE durchgeführt werden, wobei zu beachten ist, daß dieses Programm nur Sicherungen auf Band unterstützt und auch nicht in der Lage ist, die Sicherungsbänder zu verschlüsseln, so daß diese gesichert aufbewahrt werden müssen.
Bei der Durchführung der Datensicherung sind die folgenden Punkte zu beachten:

- Für die Datensicherung sind Zugriffsrechte auf das Windows-Systemverzeichnis %SysRoot%\SYSTEM32 (in der Regel \WINNT\SYSTEM32) notwendig, da NTBACKUP dort temporäre Dateien und Log-Dateien anlegt.

- Die Sicherungssoftware ist in der Lage, die Registrierung des lokalen Rechners zu sichern. Dies sollte in regelmäßigen Abständen und nach größeren Änderungen der Konfiguration durchgeführt werden.

- In regelmäßigen Abständen (nach jeweils etwa 20 Nutzungen) sollten zur Datensicherung verwendete Viertelzoll-Bänder durch Wahl der Option „Band spannen“ sauber aufgewickelt werden, um lockere Stellen und dadurch mögliche Beschädigung des Bandes durch Abrieb zu vermeiden. 4 mm (DAT-) und 8 mm (Video 8-) Bänder erfordern diese Maßnahme nicht; die entsprechende Operation steht für diese Bänder nicht zur Verfügung.

- Bei Angabe der Option „Band löschen“ sollte „Sicheres Löschen“ gewählt werden, wenn schutzwürdige Daten auf dem Band waren, da hiermit die alten Daten überschrieben werden. Sofern diese Option nicht gewählt wird, bleibt der größte Teil der ursprünglich auf diesem Band gespeicherten Daten erhalten und kann ohne großen Aufwand wieder rekonstruiert werden.

- Bei der Durchführung der Sicherungsoperation ist unbedingt die Möglichkeit zu nutzen, eine Protokolldatei anzulegen. Nach Abschluß der Operation ist die Protokolldatei daraufhin zu überprüfen, ob alle zu sichernden Daten auch tatsächlich gesichert werden konnten oder ob während der Sicherung Fehler aufgetreten sind. Dabei ist die Option „Alle Angaben protokollieren“ empfehlenswert, da man damit auch feststellen kann, ob alle zu sichernden Daten gesichert wurden und ob überhaupt die Verzeichnisse in die Datensicherung einbezogen wurden, die gesichert werden sollen.

- Bei der Wiederherstellung gesicherter Dateien wird deren Zugriffsschutz ebenfalls wiederhergestellt, sofern diese Dateien in einem Verzeichnis wiederhergestellt werden, das keine explizite Zugriffskontrolle für die darin gespeicherten Dateien vorgibt. Ist jedoch eine solche Vorgabe im Verzeichnis spezifiziert, so wird diese übernommen, und die ursprüngliche Zugriffskontrollinformation wird ignoriert.

- Die Auswahl der zu sichernden Dateien und Verzeichnisse kann unter der graphischen Bedienoberfläche nicht gespeichert werden. Um regelmäßig dieselben Verzeichnisse zu

sichern, können Skripten angelegt werden; diese sind jedoch nicht für Dateiauswahl geeignet.

Wegen der durch das Dienstprogramm NTBACKUP.EXE gegebenen Einschränkungen sollte für umfangreichere Installationen bzw. bei hohen Verfügbarkeitsanforderungen zusätzliche Software zur Durchführung von Datensicherungen eingesetzt werden. Bei der Auswahl derartiger Sicherungssoftware sollte darauf geachtet werden, daß sie die folgenden Anforderungen erfüllt:

- Die eingesetzten Dateisysteme, also FAT, NTFS und ggf. auch HPFS sollten bei der Sicherung und Wiederherstellung unterstützt werden.
- Es sollte möglich sein, Sicherungen automatisch zu vorwählbaren Zeiten bzw. in einstellbaren Intervallen durchführen zu lassen, ohne daß hierzu manuelle Eingriffe (außer dem eventuell notwendigen Bereitstellen von Sicherungsdatenträgern) erforderlich wären.
- Es sollte möglich sein, einen oder mehrere ausgewählte Benutzer automatisch über das Sicherungsergebnis und eventuelle Fehlermeldungen per E-Mail oder ähnliche Mechanismen zu informieren.
- Die Sicherungssoftware sollte die Sicherung des Backup-Mediums durch ein Paßwort, oder noch besser durch Verschlüsselung unterstützen. Weiterhin sollte sie in der Lage sein, die gesicherten Daten in komprimierter Form abzuspeichern.
- Durch Vorgabe geeigneter Include- und Exclude-Listen bei der Datei- und Verzeichnisauswahl sollte genau spezifiziert werden können, welche Daten zu sichern sind und welche nicht. Es sollte möglich sein, diese Listen zu Sicherungsprofilen zusammenzufassen, abzuspeichern und für spätere Sicherungsläufe wieder zu benutzen.
- Es sollte möglich sein, die zu sichernden Daten in Abhängigkeit vom Datum ihrer Erstellung bzw. ihrer letzten Modifikation auszuwählen.
- Die Sicherungssoftware sollte die Erzeugung logischer und physischer Vollkopien sowie inkrementeller Kopien (Änderungssicherungen) unterstützen.
- Die Sicherung sollte auch auf Festplatten und Netzlaufwerken erfolgen können.
- Die Sicherungssoftware sollte in der Lage sein, nach der Sicherung einen automatischen Vergleich der gesicherten Daten mit dem Original durchzuführen und nach der Wiederherstellung von Daten einen entsprechenden Vergleich zwischen den rekonstruierten Daten und dem Inhalt des Sicherungsdatenträgers durchzuführen.
- Bei der Wiederherstellung von Dateien sollte es möglich sein auszuwählen, ob die Dateien am ursprünglichen Ort oder auf einer anderen Platte bzw. in einem anderen Verzeichnis wiederhergestellt werden. Ebenso sollte es möglich sein, das Verhalten der Software für den Fall zu steuern, daß am Zielort schon eine Datei gleichen Namens vorhanden ist. Dabei sollte man wählen können, ob diese Datei immer, nie oder nur in dem Fall, daß sie älter als die zu rekonstruierende Datei ist, überschrieben wird, oder daß in diesem Fall eine explizite Anfrage erfolgt.

Zusätzlich zur Durchführung der normalen Datensicherungen ist es empfehlenswert, die aktuelle Systemkonfiguration nach jeder größeren Änderung mit dem Dienstprogramm RDISK in den Rettungsverzeichnis %SystemRoot%\REPAIR (z.B. \WINNT\REPAIR) sowie auf eine Notfalldiskette zu sichern, um sie bei eventuellen Inkonsistenzen wiederherstellen zu können (siehe auch M 6.42 - stellung von Rettungsdisketten für Windows NT). Dabei ist zu beachten, daß die aktuellen Sicherheitseinträge der Registrierung (in den Bereichen SECURITY und SAM) nur dann gesichert werden, wenn RDISK mit dem Parameter /s aufgerufen wird. Dies kann jedoch dazu führen, daß die Sicherung nicht mehr auf eine Diskette paßt, wenn auf dem betreffenden System eine größere Anzahl von Benutzerprofilen definiert ist.
Eine Sicherung der Registrierung ist auch mit dem Dienstprogramm REGBACK.EXE des Windows NT Resource Kits möglich; die Wiederherstellung erfolgt in diesem Fall mit dem Dienstprogramm REGREST.EXE des Windows NT Resource Kits.

M 6.45 Datensicherung unter Windows 95
Generell zu beachten sind die Anforderungen aus M 6.32 - Regelmäßige Datensicherung. Nachfolgend soll aufgezeigt werden, welche besonderen Aspekte unter Windows 95 zu berücksichtigen sind.
Unter Windows 95 sollten nach Möglichkeit nur Programme zur Datensicherung eingesetzt werden, die lange Dateinamen unterstützen (zum Beispiel das Windows 95 Programm BACKUP.EXE). Zur Konvertierung langer Dateinamen in die 8.3-Dateinamen-Konvention steht das zum Lieferumfang gehörenden Programm LFNBK.EXE zur Verfügung. Allerdings ist beim Einsatz dieses Programmes besondere Vorsicht geboten, da möglicherweise Dateinamen oder sogar einzelne Dateien nicht rekonstruiert werden können, falls nach der Sicherung Veränderungen an der Verzeichnisstruktur auf dem PC, von dem gesichert wurde, vorgenommen worden sind.

M 6.46 Erstellung von Rettungsdisketten für Windows 95
Für jeden Windows 95-Rechner sollten Rettungsdisketten erstellt werden, um bei Systemproblemen den Rechner wieder starten und ggf. benutzerspezifischen Profile wieder herstellen zu können.
Dazu benötigt man zum einen eine startfähige Systemdiskette, die für alle Rechner gemeinsam genutzt werden kann, zum anderen eine rechner- und benutzerspezifische Diskette, die die individuellen Einstellungen des Benutzers und des jeweiligen Rechners enthält.

Erzeugen der startfähigen Systemdiskette
Eine für alle Rechner nutzbare Systemdiskette kann mit der Registerkarte Startdiskette unter der Systemsteuerungsoption Software erzeugt werden. Allerdings benötigt man dazu eine Windows 95 CD. Stattdessen kann der erfahrene Benutzer alle relevante Dateien auch manuell auf die Diskette kopieren. Dazu gehören beispielsweise COMMAND.COM, IO.SYS, DRVSPACE.BIN und MSDOS.SYS. In diesem Fall sollten außerdem der deutsche Tastaturtreiber KEYB.COM sowie KEYBOARD.SYS, COUNTRY.SYS und ggf. weitere Systemdateien (z.B. einen CD-ROM-Treiber) kopiert werden. Die deutsche Tastatur stellt man dann mit dem Befehl KEYB GR„KEYBOARD.SYS ein. Für andere notwendige Dateien, z.B. einen Editor, Programme zur Festplattendekomprimierung oder Backup-Programme, kann ggf. eine zusätz-

liche Diskette verwendet werden.

Erzeugen von rechner- und benutzerspezifischen Disketten
Hierzu wird für jeden Rechner eine vorformatierte Diskette und das Programm Emergency Recovery Utility (ERU) benötigt, welches zum Systemumfang gehört. Dieses wird zwar nicht standardmäßig installiert, befindet sich aber auf der mitgelieferten Windows 95 CD-ROM. Mit diesem Programm lassen sich in einfacher Weise die relevanten und aktuellen Systemdateien, insbesondere die Datei mit den Benutzereinstellungen USER.DAT bzw. die Datei mit den Systemeinstellungen SYSTEM.DAT, auf Diskette kopieren. Die Dateien USER.DAT und SYSTEM.DAT beinhalten die entsprechenden Informationen, die unter Windows 3.x in den ini-Dateien gespeichert sind. Diese Diskette sollte bei umfangreichen oder wichtigen Änderungen an der Rechnerkonfiguartion oder an den Benutzereinstellungen aktualisiert werden.
Nach dem Erstellen der Rettungsdisketten sollten diese auf Computer-Viren überprüft und danach schreibgeschützt werden.

Nutzung der Start-Diskette
Um von der Systemdiskette zu starten, wird diese in das Diskettenlaufwerk eingelegt, die Start-Reihenfolge im BIOS zugunsten des Diskettenlaufwerkes priorisiert und der Rechner neu gestartet. Der Rechner fährt dann im Zeilenmodus hoch.

Nutzung der rechner- und benutzerspezifischen Diskette
Falls der Rechner ordnungsgemäß startet (mit oder ohne Start-Diskette), die rechner- und benutzerspezifischen Dateien jedoch zerstört sind, können diese mit dem Programm ERD.EXE, das sich auf der rechner- und benutzerspezifischen Diskette befindet, zurückgespielt werden. Die korrespondierende Dateien auf der Festplatte werden zuvor in das Verzeichnis C:\WINDOWS\ERUNDO verschoben und können mit den Befehl ERD /UNDO ggf. rekonstruiert werden.
Hinweis: Für die Nutzung des Programmes ERD.EXE ist es notwendig, den Rechner im Zeilenmodus zu starten. Dies erreicht man zum Beispiel, indem man von der Startdiskette startet, beim Beenden von Windows 95 Computer im MS-DOS Modus starten wählt oder beim Starten des Rechners während der Nachricht „Windows 95 wird gestartet“ die F8-Taste betätigt und anschließend „5. Nur Eingabeaufforderung“ wählt. Letzteres ist allerdings nur dann möglich, wenn in der Datei MSDOS.SYS die Zeile BootKeys=1 eingetragen ist.

M 6.48 Verhaltensregeln nach Verlust der Datenbankintegrität
Falls sich das Datenbanksystem in nicht vorgesehener Weise verhält (zum Beispiel undefiniertes Systemverhalten, nicht auffindbare Tabellen oder Datensätze, veränderte Tabelleninhalte, unerklärlich langes Antwortzeitverhalten), kann ein Verlust der Datenbankintegrität vorliegen, der unter Umständen auch durch mißbräuchliche Nutzung des Systems verursacht wurde (zum Beispiel unautorisierte Administration, Veränderungen der Systemeinstellungen, Überschreiten der maximal zulässigen Connects).
Dann sollten die Benutzer folgende Punkte beachten:

- Ruhe bewahren!

- Benachrichtigen Sie den Datenbankadministrator.
- Greifen sie nicht mehr auf die Datenbank zu.

Der Datenbankadministrator sollte folgende Schritte durchführen:

- Benachrichtigung aller betroffenen Benutzer,
- Herunterfahren des Datenbanksystems,
- Hochfahren des Datenbanksystems im Exklusiv-Modus (falls dies vom Datenbanksystem unterstützt wird),
- Sichern aller Dateien, die Aufschluß über die Art und Ursache des aufgetretenen Problems geben könnten (z. B. ob tatsächlich ein Angriff erfolgt ist und auf welche Weise der Angreifer eindringen konnte), d. h. insbesondere Sichern aller relevanten Protokolldateien,
- Überprüfung und ggf. Zurücksetzen der Zugriffsrechte auf Systemtabellen,
- Überprüfung der Datenbanksoftware auf sichtbare Veränderungen, z. B. Erstellungsdatum und Größe der entsprechenden Dateien (Da diese von einem Angreifer auch wieder auf ihre Ursprungswerte zurückgesetzt werden können, sollte die Integrität der Dateien mit Prüfsummenverfahren überprüft werden.),
- ggf. Löschen der Datenbanksoftware und Wiedereinspielen der Original-Dateien von schreibgeschützten Datenträgern (vgl. M 6.21 Sicherungskopie der eingesetzten Software). Programme aus existierenden Datensicherungen sollten nicht wiedereingespielt werden, die diese den Fehler schon enthalten können),
- Überprüfung der Protokolldateien nach Auffälligkeiten (in Zusammenarbeit mit dem Revisor),
- Benachrichtigung der Benutzer mit der Bitte, ihre Bereiche auf Unregelmäßigkeiten zu prüfen.

Falls Daten gelöscht oder unerwünscht geändert wurden, können diese aus den Datensicherungen wiedereingespielt werden (siehe M 6.51 Wiederherstellung einer Datenbank).

M 6.49 Datensicherung einer Datenbank
Die Sicherung der Daten eines Datenbanksystems kann in aller Regel nicht mit den Datensicherungsprogrammen auf Betriebssystemebene vollständig abgedeckt werden. Letztere bilden in den meisten Fällen lediglich das Bindeglied, um die zu sichernden Daten auf ein Sicherungsmedium zu schreiben. Zur Sicherung des DBMS und der Daten müssen dagegen für die meisten Datenbankprodukte zusätzlich die jeweiligen Dienstprogramme des DBMS eingesetzt werden.

Die einfachste Möglichkeit einer Datenbanksicherung, die zugleich die sicherste darstellt, ist eine Komplettsicherung der Datenbank in heruntergefahrenem Zustand. Dabei werden alle zur

Datenbank gehörenden Dateien auf dem Sicherungsmedium gesichert. Meist ist dieses Vorgehen allerdings aus Gründen der Verfügbarkeitsanforderungen an die Datenbank oder aufgrund des zu sichernden Datenvolumens nicht durchführbar.
Eine Alternative zur oben beschriebenen Komplettsicherung ist eine Online-Sicherung der Datenbank. Die Sicherung erfolgt dann während des laufenden Betriebs, d.h. die Datenbank muß nicht heruntergefahren werden. Die Nachteile dieser Sicherungsart sind, daß Inkonsistenzen nicht explizit ausgeschlossen werden können, und daß auch in diesem Fall bei einer Zerstörung der Datenbank eine (Offline-) Komplettsicherung existieren muß, auf der aufbauend die Online-Sicherungen zurückgespielt werden können. Online-Sicherungen sollten aus diesem Grund nur dann durchgeführt werden, wenn eine permanente Verfügbarkeit der Datenbank gefordert ist. Auf eine Offline-Komplettsicherung, die in vertretbar großen Zeitabständen durchgeführt werden kann, sollte trotzdem nicht verzichtet werden.

Partielle Datenbanksicherungen stellen eine weitere Möglichkeit dar. Sie sollten immer dann verwendet werden, wenn das zu sichernde Datenvolumen zu groß ist, um eine vollständige Sicherung durchführen zu können. Dies kann daraus resultieren, daß die Kapazitäten der Sicherungsmedien nicht ausreichen oder daß der zur Verfügung stehende Zeitrahmen je Sicherung nicht genügt, um eine vollständige Sicherung durchführen zu können. Falls möglich, so sollten in jedem Fall alle Transaktionen zwischen zwei Offline-Komplettsicherungen archiviert werden. Oracle bietet dazu beispielsweise die Möglichkeit an, indem der sogenannte ARCHIVE-Mode für die Datenbank aktiviert wird. Transaktionen werden bei Oracle in sogenannten Log-Dateien protokolliert, von denen es mehrere gibt. Diese werden nacheinander beschrieben und sobald alle Log-Dateien voll sind, so wird wieder die erste Log-Datei überschrieben. Der ARCHIVE-Mode erstellt von diesen Log-Dateien eine Sicherungskopie, bevor sie wieder überschrieben werden. Auf diese Art und Weise können bei einer Zerstörung der Datenbank alle Transaktionen komplett rekonstruiert werden. Auch hierfür ist allerdings die Existenz einer Komplettsicherung der Datenbank die Voraussetzung. Die Dauer eines solchen Recovery wächst mit der Anzahl der zurückzuspielenden Archiv-Log-Dateien an.

Für die Datensicherung eines Datenbanksystems muß ein eigenes Datensicherungskonzept erstellt werden. Einflußfaktoren für ein solches Konzept sind:

- Verfügbarkeitsanforderungen an die Datenbank
  Wenn beispielsweise eine Datenbank werktags rund um die Uhr zur Verfügung stehen muß, so kann eine Komplettsicherung nur am Wochenende durchgeführt werden, da dies im allgemeinen ein Herunterfahren der Datenbank erfordert.

- Datenvolumen
  Das gesamte zu sichernde Datenvolumen muß mit den zur Verfügung stehenden Sicherungskapazitäten verglichen werden. Dabei muß festgestellt werden, ob die Sicherungskapazitäten (z.B. ein DAT-Tape pro Sicherungslauf) für das entsprechende Datenvolumen der Datenbank ausreichend dimensioniert sind.
  Falls dies nicht der Fall ist, muß ein Konzept zur Teilsicherung des Datenvolumens erstellt werden. Dies kann z.B. bedeuten, daß die Daten einzelner Anwendungen oder

einzelner Bereiche der Datenbank immer im Wechsel gesichert werden bzw. nur die aktuellen Änderungen. Die Möglichkeiten einer Teilsicherung hängen von der verwendeten Datenbank-Software ab.

- Maximal verkraftbarer Datenverlust
  Hier muß festgelegt werden, ob bei einer Zerstörung der Datenbank der Datenverlust eines Tages verkraftbar ist, oder ob die Datenbank bis zur letzten Transaktion wiederherstellbar sein muß. Dies ist im allgemeinen bei einer hohen Anforderung an die Verfügbarkeit bzw. Integrität der Daten der Fall.

- Wiederanlaufzeit
  Auch die maximal zulässige Zeitdauer des Wiederherstellens der Datenbank nach einem Absturz muß festgelegt werden, um den Verfügbarkeitsanforderungen zu genügen.

- Datensicherungsmöglichkeiten der Datenbank-Software
  Im allgemeinen werden von einer Datenbank-Standardsoftware nicht alle denkbaren Datensicherungsmöglichkeiten unterstützt, wie z.B. eine partielle Datenbanksicherung. Im konkreten Fall gilt es also zu prüfen, ob das erstellte Datensicherungskonzept mit den zur Verfügung stehenden Mechanismen auch umgesetzt werden kann.

Anhand dieser Informationen kann ein Konzept für die Datensicherung der Datenbank erstellt werden. In diesem Sicherungskonzept wird u.a. festgelegt (siehe hierzu auch [BSI1998] Kapitel 3.4 - Datensicherungskonzept)

- wer für die ordnungsgemäße Durchführung von Datensicherungen zuständig ist,
- in welchen Zeitabständen eine Datenbanksicherung durchgeführt wird,
- in welcher Art und Weise die Datenbanksicherung zu erfolgen hat,
- zu welchem Zeitpunkt die Datenbanksicherung durchgeführt wird,
- die Spezifikation des zu sichernden Datenvolumens je Sicherung.
- wie die Erstellung von Datensicherungen zu dokumentieren ist, und
- wo die Datensicherungsmedien aufbewahrt werden.

Beispiel:
Sicherung von Montag bis Samstag:

- Startzeit: morgens um 3.00h
- Es erfolgt eine vollständige Sicherung der Daten, wobei die Datenbank nicht heruntergefahren, sondern die Möglichkeit der Online-Sicherung des DBMS genutzt wird.

Sicherung am Sonntag

- Startzeit: morgens um 3.00h

- Die Datenbank wird heruntergefahren und es erfolgt eine Komplettsicherung der Datenbank.

M 6.50 Archivierung von Datenbeständen
Ist eine Archivierung von Daten eines Datenbanksystems erforderlich, so muß dazu ein entsprechendes Konzept erstellt werden, um die Datenbestände zu einem späteren Zeitpunkt wieder zur Verfügung stellen zu können. Hierbei sind folgende Punkte zu berücksichtigen:
Archivierung

- Die zur Verfügung stehenden Archivierungsmöglichkeiten müssen identifiziert werden.
- Es muß dokumentiert werden, welches Datenmodell den zu archivierenden Daten zugrunde liegt.
- Der Zeitpunkt der Archivierung ist zu dokumentieren.
- Aufbau, Systematik und Ordnungskriterien des Archivs müssen spezifiziert werden.
- Für alle Archivierungsmedien ist anhand von Herstellerangaben und Erfahrungswerten eine maximale Lebensdauer zu bestimmen. Entsprechend dessen müssen Zeitpunkte für die Auffrischung des archivierten Datenbestandes festgelegt werden.
- Die geforderte Verfügbarkeit der archivierten Datenbestände ist zu überprüfen und gegebenenfalls an die konkreten Anforderungen anzupassen. Es kann beispielsweise gefordert sein, archivierte Datenbestände der letzten sechs Monate kurzfristig zur Verfügung zu stellen, während Datenbestände älteren Datums nur auf Anfrage und mit längeren Vorlaufzeiten wiedereingespielt werden müssen. Dieses Kriterium hat u.a. Auswirkungen auf die Wahl des Archivierungsmediums sowie auf die Art und Weise der Archivierung. Bei hohen Verfügbarkeitsanforderungen muß evtl. ein redundantes Archiv geführt werden.
- Es muß sichergestellt sein, daß vorgegebene Aufbewahrungsfristen eingehalten werden.

Wiedereinspielen

- Der aktuelle Datenbestand darf von dem archivierten Datenbestand nicht beeinflußt werden.
- Für die Wiedereinspielung von archivierten Datenbeständen muß genügend Speicherplatz zur Verfügung gestellt werden.
- Der archivierte Datenbestand muß wiederherstellbar sein, auch wenn sich zwischenzeitlich das Datenmodell geändert hat. In diesem Fall muß das Datenmodell zum Archivierungszeitpunkt bekannt sein, um den alten Stand wiederherstellen zu können.
- Wenn die wiedereingespielten Daten von einer Anwendung verarbeitet werden sollen, muß auch von dieser Anwendung eine Version vorhanden sein, die das „alte“ Datenmodell unterstützt.

- Es muß sporadisch überprüft werden, ob sich der archivierte Datenbestand wiedereinspielen läßt.

Bei der Archivierung von Datenbeständen, die personenbezogene Daten enthalten, muß darüber hinaus berücksichtigt werden, daß die Betroffenen ein Recht auf Berichtigung, Sperrung bzw. Löschung der über sie gespeicherten Daten haben. Um dies zu gewährleisten, sind entsprechende technisch-organisatorische Verfahren zu entwickeln. Insbesondere müssen auch nach dem Wiedereinspielen alter Datenbestände vorher durchgeführte Berichtigungen, Sperrungen bzw. Löschungen erhalten bleiben.

M 6.51 Wiederherstellung einer Datenbank
Es ist ein Konzept zu erstellen, wie das Wiedereinspielen von Datenbanksicherungen durchzuführen ist. Dem Konzept zugrunde gelegt werden müssen

- das Datensicherungskonzept (siehe M 6.49 - Datensicherung einer Datenbank) und
- die möglichen Fehlersituationen, die ein Wiedereinspielen von Datenbanksicherungen erforderlich machen können.

Anhand dieser beiden Punkte ist abzuleiten, welche Datenbanksicherungen in welcher Form wiedereingespielt werden müssen. Die Wiederherstellung einer Datenbank ist eine komplexe Aufgabe, die ein äußerst sorgfältiges Vorgehen und viel Übung erfordert. Trotzdem sollte immer damit gerechnet werden, daß eine Wiederherstellung nicht reibungslos und fehlerfrei funktionieren wird. Daher sollte die zerstörte Datenbank nicht durch ein einfaches Zurückspielen der Datenbanksicherung überschrieben werden.

Häufig läßt sich die für korrupt gehaltene Datenbank wieder bereinigen. Um jedoch die Wiederanlaufzeit zu minimieren, sollte parallel zur Fehlersuche mit der Wiederherstellung der Datenbank in einem getrennten Speicherbereich begonnen werden. Auch wenn sich die beschädigte Datenbank nicht mehr reparieren läßt, sollte sie dennoch erhalten bleiben, um sie analysieren und die Fehlerursache feststellen zu können.
Bei der Wiederherstellung sollte die Datenbanksicherung daher zuerst auf getrennten Speichermedien eingespielt werden. Dabei ist zu beachten, daß hierfür das gleiche Volumen an Speicherkapazität benötigt wird wie für die defekte Datenbank.

Diese Speicherkapazitäten müssen für den Notfall vorgehalten werden, um einem Verlust der Datenbankintegrität vorzubeugen und die Verfügbarkeitsanforderungen zu erfüllen. Ist dies nicht möglich, so ist festzulegen, auf welche Weise kurzfristig die erforderlichen Speicherkapazitäten zur Verfügung gestellt werden können. Selbstverständlich darf dies nicht zu einem zusätzlichen Datenverlust führen, wenn beispielsweise Festplattenbereiche mit anderen Daten gelöscht werden sollen, um die erforderlichen Ressourcen für das Wiedereinspielen der Datenbanksicherung zur Verfügung zu stellen. Müssen aufgrund mangelnder Speicherkapazitäten andere Daten gelöscht werden, so sind diese sorgfältig zu sichern, damit gewährleistet werden kann, daß die Daten nach Abschluß der Restaurierungsmaßnahme wieder ordnungsgemäß zur

Verfügung stehen.

Für den Fall, daß keine vollständige Restaurierung der Datenbank notwendig ist, sondern lediglich einzelne Datenbestände wiederherzustellen sind, so ist ein Wiedereinspielen der Daten immer getrennt von den Originaldatenbeständen durchzuführen. Auch hier sind dann entsprechende Speicherkapazitäten erforderlich. Es ist an dieser Stelle sinnvoller, hierfür parallel eine eigene Datenbank einzurichten, damit die Datenbestände der Originaldatenbank auf jeden Fall unbeeinfußt bleiben. Dies gilt selbst dann, wenn die Möglichkeit besteht, die Daten in der Originaldatenbank gesondert einzuspielen.