

1 Datensicherung und Notfallwiederherstellung

1.1 Datensicherung

- 1.1.1 Regelmäßige Datensicherung
- 1.1.2 Schriftliche Aufzeichnungen der Konfigurationsdaten
- 1.1.3 Entwicklung eines Datensicherungskonzepts
- 1.1.4 Geeignete Aufbewahrung der Backup-Datenträger
- 1.1.5 Datensicherung bei mobilen IT-Systemen (Notebooks, PDA, ...)

1.2 Notfallvorsorge und -wiederherstellung

- 1.2.1 Erhebung der wichtigsten Anwendungen
- 1.2.2 Notfallvorsorge und eingeschränkter Ersatzbetrieb
- 1.2.3 Notfallwiederherstellung

2 Internetzugang und Netzwerke

2.1 Sichere Anbindung an das Internet

- 2.1.1 Einsatz einer Firewall
- 2.1.2 Personal Firewalls
- 2.1.3 Wireless LAN (WLAN)
- 2.1.4 Festlegung einer WWW-Sicherheitsstrategie
- 2.1.5 Sicherheit von Internet-Browsern

2.2 Sicherheit des Firmennetzwerks

- 2.2.1 Update/Upgrade von Soft- und Hardware im Netzbereich
- 2.2.2 Festlegung einer Sicherheitsstrategie für ein Client-Server-Netz

2.3 Sicherheit beim Serverbetrieb

- 2.3.1 Sicherer Betrieb eines Mail-Servers
- 2.3.2 Sicherer Betrieb eines WWW-Servers
- 2.3.3 Betrieb eines Webservers bei einem Internet-Provider (Webhosting, Serverhousing)

3 Virenschutz

3.1 Schadprogramme und Schutzmaßnahmen

- 3.1.1 Verschiedene Formen von Bedrohungen
- 3.1.2 Generelle Maßnahmen zur Vorbeugung gegen Virenbefall

3.2 Virenschutzkonzepte

- 3.2.1 Erstellung eines mehrstufigen Virenschutzkonzepts
- 3.2.2 Virenschutzmaßnahmen auf Firewall- und Gateway-Ebene
- 3.2.3 Virenschutzmaßnahmen auf Server-Ebene
- 3.2.4 Virenschutzmaßnahmen auf Einzelplatzrechnern
- 3.2.5 Notfallmaßnahmen im Fall von Vireninfektionen

3.3 Virenschutz durch die Benutzer

- 3.3.1 Vermeidung bzw. Erkennung von Viren durch den Benutzer
- 3.3.2 Maßnahmen bei ausgehender E-Mail:
- 3.3.3 Verhalten bei Downloads aus dem Internet

4 Computersicherheit

4.1 Sichere Konfiguration

- 4.1.1 Gefahrenquelle Wechselmedien
- 4.1.2 Nutzung der BIOS-Sicherheitsmechanismen
- 4.1.3 Vorsichtiger Gebrauch von Administratorrechten
- 4.1.4 Protokollierung

4.2 Sicherheit und Software

- 4.2.1 Einsatz eines Verschlüsselungsproduktes für Arbeitsplatzsysteme
- 4.2.2 Update von Software
- 4.2.3 Nutzungsverbot nicht-betrieblicher Software
- 4.2.4 Sicherheitsfunktionen in Anwendungsprogrammen
- 4.2.5 Überprüfen von Dateien vor deren Weitergabe
- 4.2.6 Datenformate

5 Personelle Maßnahmen

5.1 Regelungen für Mitarbeiter

- 5.1.1 Clear Desk-Policy
- 5.1.2 Verpflichtung der PC-Benutzer zum Abmelden
- 5.1.3 Verfahrensweise beim Ausscheiden von Mitarbeitern
- 5.1.4 Vertretungsregelungen
- 5.1.5 Kontrolle der Einhaltung der organisatorischen Vorgaben
- 5.1.6 Regelungen für den Einsatz von Fremdpersonal

5.2 Sicherheitssensibilisierung und -schulung

- 5.2.1 Schulung und Sensibilisierung zu IT-Sicherheitsmaßnahmen
- 5.2.2 Geregelt Einarbeitung/Einweisung neuer Mitarbeiter
- 5.2.3 Betreuung und Beratung von IT-Benutzern
- 5.2.4 Auswahl von Passwörtern
- 5.2.5 Aktionen bei Auftreten von Sicherheitsproblemen (Incident Handling Pläne)
- 5.2.6 Nutzung und Aufbewahrung mobiler IT-Geräte

5.3 Telearbeit

- 5.3.1 Geeignete Einrichtung eines häuslichen Arbeitsplatzes

6 Bauliche und infrastrukturelle Maßnahmen

6.1 Bauliche und organisatorische Maßnahmen

- 6.1.1 Schützenswerte Gebäudeteile und Einbruchschutz
- 6.1.2 Zutrittskontrolle und Empfang
- 6.1.3 Schließplan

6.2 Geeignete Aufstellung und Aufbewahrung

- 6.2.1 Geeignete Aufstellung eines Arbeitsplatz-IT-Systems
- 6.2.2 Geeignete Aufstellung von Servern und anderen besonders schützenswerten IT-Komponenten

6.3 Brandschutz

- 6.3.1 Einhaltung von Brandschutzvorschriften und Auflagen
- 6.3.2 Brandbekämpfung

6.4 Stromversorgung, Maßnahmen gegen elektrische Risiken

- 6.4.1 Angepasste Aufteilung der Stromkreise
- 6.4.2 Lokale unterbrechungsfreie Stromversorgung
- 6.4.3 Not-Aus-Schalter
- 6.4.4 Blitzschutzeinrichtungen, Überspannungsschutz

1 Datensicherung und Notfallwiederherstellung

Ziel der Datensicherung und Notfallwiederherstellung ist die Schadensbegrenzung im Fall von Systemausfällen, Datenverlust oder im schlimmsten Fall Zerstörung der vorhandenen IT-Infrastruktur. Durch verschiedene Maßnahmen (Datensicherung, Definition eines eingeschränkten Notbetriebs, Dokumentation der Wiederherstellungsverfahren etc.) soll im Schadensfall der Wiederanlauf der IT-Systeme innerhalb eines definierten Zeitraums gewährleistet werden.

1.1 Datensicherung

Unabdingbare Voraussetzung für jede Notfallvorsorge ist die Planung und Durchführung der Datensicherung. Da sie eine der wichtigsten IT-Sicherheitsmaßnahmen darstellt, müssen auch die Mitarbeiter zur Einhaltung und Unterstützung der Datensicherungsmaßnahmen verpflichtet werden. Regelmäßige Motivation zur Datensicherung und Information über die getroffenen Maßnahmen kann sich in diesem Fall positiv auf Mitarbeiter auswirken.

1.1.1 Regelmäßige Datensicherung

*Datensicherungen müssen in regelmäßigen Abständen erfolgen. Dazu muss geklärt sein, **welche Daten von wem zu welchem Zeitpunkt gesichert werden.***

Folgende Punkte müssen in jedem Fall festgelegt werden:

- Umfang der zu sichernden Daten
- Sicherungstechnologie und -medien
- Zeitintervall und Zeitpunkt der Sicherungen
- Anzahl der aufzubewahrenden Sicherungen aus der Vergangenheit
- Zuständigkeit für Durchführung, Überwachung und Dokumentation der Sicherungen

Vorrangig sollten die selbst erstellten Daten (Produktionsdaten, z.B.: Dokumente, Kundendatei, Buchhaltung etc.) gesichert werden, außerdem noch die Konfigurationsdateien der eingesetzten Software. Ob es sinnvoll ist, auch Systemdateien zu sichern (bis hin zur vollständigen Sicherung von Betriebssystem und installierter Software), hängt u.a. von den zeitlichen Erfordernissen zur Wiederherstellung und den Fähigkeiten der Sicherungssoftware ab.

Datensicherungen können mittels verschiedener Methoden erfolgen:

- **Volldatensicherung:**
Bei dieser Methode werden sämtliche zur Sicherung vorgesehenen Dateien gesichert. Volldatensicherungen sind einfach durchzuführen und auch die Wiederherstellung der Daten funktioniert relativ einfach. Allerdings verbrauchen sie üblicherweise viel Speicherplatz auf den Sicherungsdatenträgern und dauern lange. Sie sind im Allgemeinen ideal für unbeaufsichtigte, in der Nacht oder am Wochenende durchgeführte Sicherungsläufe.
- **Inkrementelle Sicherung:**
Bei inkrementellen Sicherungen werden nur die seit der letzten Sicherung geänderten Dateien gesichert. Der Vorteil liegt darin, dass deutlich weniger Daten zu sichern sind, die Sicherungen also zeitsparender erfolgen und weniger Platz auf den Sicherungsmedien verbrauchen. Der Nachteil dieser Methode ist, dass eine einzige fehlgeschlagene Sicherung ausreicht, um alle darauf folgenden Sicherungen unbrauchbar zu machen. In regelmäßigen Abständen (z.B. wöchentlich) sollten daher Volldatensicherungen durchgeführt werden, auf denen die inkrementellen Sicherungen aufbauen. Ein weiterer Nachteil besteht in der deutlich komplizierteren Wiederherstellung von Daten, da für diese der gesamte Sicherungssatz (d.h. die letzte Volldatensicherung sowie alle darauf folgenden inkrementellen Sicherungen) benötigt wird.
- **Datenträgerimages:**
Dabei handelt es sich um eine Methode, die häufig zur Systemwiederherstellung oder zum Aufsetzen neuer Rechner verwendet wird. Von der Festplatte eines PCs wird ein "Image", d.h. ein Abbild, erstellt und auf Datenträger gespeichert. Im Bedarfsfall kann dieser PC, wenn er z.B. durch die Zerstörung oder Kompromittierung des Betriebssystems unbrauchbar geworden ist, anhand des Images in wenigen Minuten wieder in den exakten Zustand zum Zeitpunkt der Imageerstellung versetzt werden. Problematisch ist dabei, dass die Imageerstellung üblicherweise nicht im laufenden Betrieb erfolgen kann; sondern der PC zuvor via Boot-Diskette oder Boot-CD-ROM gestartet werden muss. Außerdem werden Datenträgerimages relativ groß. Die Verwendung dieser Methode bietet sich vor allem für Wiederherstellungszwecke an, als Datensicherungsmethode im eigentlichen Sinn

wird sie bisher kaum genutzt.

Grundsätzlich sind alle Arten von Wechseldatenträgern als Sicherungsmedien geeignet. In einfachen Fällen kann es ausreichen, die Produktionsdaten wöchentlich auf eine CD-ROM oder DVD zu brennen. Auch die Verwendung von Wechselfestplatten oder USB-Sticks ist möglich. Allerdings erfordern solche Datensicherungstechnologien einen relativ hohen Arbeits- und Zeitaufwand und lassen sich schlecht automatisieren. Ab einer bestimmten Datenmenge ist es daher sinnvoller, für diesen Zweck eine eigene Datensicherungssoftware und spezielle Wechsellaufwerke einzusetzen. Oft liegen dem Betriebssystem bereits einfachere Versionen von Backup-Software bei, die von ihren Funktionen her meist völlig ausreichend sind. Als Sicherungshardware können Bandlaufwerke eingesetzt werden, die in den verschiedensten Ausführungen und Speicherkapazitäten erhältlich sind. Alternativ dazu lassen sich auch Wechselfestplattensysteme verwenden. Voraussetzung für den Einsatz solcher Systeme ist die zentrale Speicherung der Daten auf einem eigenen Server (Fileserver), auf dem die Sicherungshardware installiert werden kann. Diese Anordnung ist hinsichtlich der Datensicherheit aber ohnehin empfehlenswert.

Für kleinere Datenmengen lässt sich auch die Möglichkeit der Online-Datensicherung nützen. Verschiedene Anbieter ermöglichen es, Daten über eine verschlüsselte Internetverbindung auf zentrale Server zu übertragen, von denen sie im Notfall wieder abgerufen werden können. Der Vorteil dieser Methode ist, dass die Daten außer Haus gespeichert werden und somit die räumliche Trennung der Sicherungsmedien von den Originaldaten bereits mit der Sicherung gegeben ist. Bei einer Online-Sicherung der Daten ist aber auch großes Augenmerk auf die Seriosität des Anbieters zu legen. Die generelle Sinnhaftigkeit dieser Methode hängt stark von der zu sichernden Datenmenge und der Kapazität des Internetzugangs ab.

Um weiter zurückliegende Sicherungszeitpunkte abzurufen, ist es oft sinnvoll, einzelne Sicherungsmedien auszugliedern. Z.B. können die am Monatsersten erstellten Sicherungen und die Sicherung am Jahresende zurückbehalten werden, um bei Bedarf auch alte Datenstände einsehen zu können.

Die Zuständigkeit für Durchführung, Überwachung und Dokumentation der Sicherungen sollte schriftlich festgelegt werden. In Notfällen kann der Fortbestand des Unternehmens von den Datensicherungen abhängen. Es ist auch zu bedenken, dass ein Unbefugter durch den Diebstahl oder das Austauschen eines Sicherungsmediums Einblick in den gesamten Datenbestand des Unternehmens erhalten könnte. Die Durchführung der Sicherungen ist also eine überaus verantwortungsvolle Aufgabe, die nur an unbedingt zuverlässige Personen übertragen werden sollte.

Um sicherzustellen, dass die Datensicherung tatsächlich funktioniert, muss **unbedingt** die Wiederherstellung der gesicherten Daten ausprobiert werden. Besonders gilt dies für die Wiederherstellung komplexer Server (Datenbank-, Mailserver, Domänen-Controller): Die Notfallwiederherstellung solcher Server, vom leeren System bis zur produktionsreifen Maschine, muss mindestens einmal durchgeführt und dokumentiert werden. Es ist **nicht** davon auszugehen, dass eine ungetestete Wiederherstellungsmethode im Notfall tatsächlich funktionieren wird.

1.1.2 Schriftliche Aufzeichnungen der Konfigurationsdaten

Zusätzlich zur eigentlichen Datensicherung ist es oft sinnvoll, schriftliche Aufzeichnungen über verschiedene Konfigurationsdetails anzulegen.

Selbst wenn sämtliche Konfigurationseinstellungen in elektronischer Form gespeichert werden können, bieten zusätzliche Ausdrucke der wichtigsten Einstellungen, auf die im Notfall rasch zugegriffen werden kann, Vorteile. Die Zugangsdaten zum Internet-Provider, einschließlich der Konfigurationsdetails für den Netzwerkzugang und der Passwörter (z.B. für evtl. Mail-Accounts), sollten unbedingt an sicherer Stelle hinterlegt werden. Auch für Konfigurationseinstellungen der Netzwerkrouter und Switches sind schriftliche Aufzeichnungen oder Bildschirmausdrucke bei der Wiederherstellung nach einem Notfall wichtig.

Die Aufzeichnungen müssen an sicherer Stelle, d.h. vor Zerstörung und unbefugten Zugriffen geschützt, gelagert werden. Bei Änderungen an den Einstellungen oder Passwörtern sollten sie umgehend aktualisiert werden.

1.1.3 Entwicklung eines Datensicherungskonzepts

Im Rahmen eines Datensicherungskonzepts sind u.a. folgende Faktoren zu berücksichtigen: Datenvolumen, Änderungsfrequenz der Daten und die jeweiligen Verfügbarkeitsanforderungen. Das Datensicherungskonzept sollte Lösungen für sämtliche betroffenen IT-Systeme enthalten und diese detailliert beschreiben. Es muss daher regelmäßig aktualisiert werden und erweiterbar sein. Des Weiteren müssen darin die verschiedenen Verantwortlichkeiten im Bereich der Datensicherung festgelegt werden. Sinnvoll ist es auch, das korrekte Vorgehen bei der Datensicherung darin genau zu dokumentieren.

Festlegung des Minimaldatensicherungskonzepts

In einem Minimaldatensicherungskonzept sind jene Daten festzuhalten, die in jedem Fall gesichert werden müssen. Festzulegen sind dabei Umfang und Häufigkeit der Sicherungen nach Datenart. Beispielsweise wird darin festgelegt, dass

- die eingesetzte Software (Standardsoftware, Eigenentwicklungen) einmalig,
- die System- und Konfigurationsdaten aller Server einmal monatlich,
- die Protokolldaten aller Server einmal monatlich und
- alle Produktionsdaten zumindest einmal wöchentlich

gesichert werden müssen.

In einfacheren Fällen, in denen die Erstellung eines umfassenden Datensicherungskonzepts zu aufwändig erscheint, kann ein solches Minimaldatensicherungskonzept ausreichen, um die Sicherungsstrategie festzulegen. Es kann außerdem auch als Ausgangspunkt für die detaillierten Regelungen des Datensicherungskonzepts dienen.

Sicherungskopie der eingesetzten Software

Von den Datenträgern der eingesetzten Software (Installations-CDs für Betriebssysteme und Anwendungsprogramme, eigenentwickelte Software, etc.) sind Sicherungskopien zu erstellen, die getrennt von den Originaldatenträgern aufbewahrt werden sollten. Um eventuelle Wiederherstellungsarbeiten rasch durchführen zu können, müssen die zuständigen Mitarbeiter jederzeit auf diese Medien zugreifen können.

Die Einrichtung einer zentralen Datenträgersammlung, die sämtliche aktuelle Software in Form von Sicherheitskopien enthält, ist empfehlenswert. Im Wiederherstellungsfall können so Zeitverluste, die durch das Suchen der benötigten Medien entstehen, vermieden werden. Die zuständigen Mitarbeiter sollten auf diese Datenträger jederzeit zugreifen können, unerlaubte Zugriffe, z.B. zur Erstellung von Raubkopien, müssen durch geeignete Platzierung ausgeschlossen werden.

1.1.4 Geeignete Aufbewahrung der Backup-Datenträger

Bei der Aufbewahrung der Backup-Datenträger ist besondere Sorgfalt angebracht. Zum ersten sind auf ihnen die wichtigsten Unternehmensdaten gespeichert, sodass der Diebstahl eines Sicherungsmediums erhebliche Folgen nach sich ziehen kann. Zum zweiten bieten sie im Katastrophenfall, etwa bei der Zerstörung der IT-Systeme durch einen Brand, die einzige Möglichkeit, den elektronisch gespeicherten Datenbestand wiederherzustellen.

Folgende Anforderungen sind zu beachten:

- Der Zugriff auf Backup-Datenträger darf nur befugten Personen möglich sein. Backup-Medien sollten idealerweise in einem Safe, jedenfalls aber vor unbefugten Zugriffen geschützt, gelagert werden. Auch die Sicherungslaufwerke, z.B. Bandlaufwerke oder Wechselfestplatten, sollten nur den zuständigen Mitarbeitern zugänglich sein.
- Die Datenträger müssen räumlich von den zu sichernden Rechnern getrennt aufbewahrt werden, um zu vermeiden, dass z.B. durch einen Brand gleichzeitig Rechner und Sicherungsmedien zerstört werden.
- In regelmäßigen Abständen - z.B. einmal wöchentlich -, sollte ein vollständiger Sicherungssatz an einen anderen Ort (ein Nebenstandort, ein Bankschließfach, evtl. auch versperrt in der Wohnung eines zuständigen Mitarbeiters) ausgelagert werden.
- Im Notfall muss es möglich sein, auf die benötigten Sicherungsmedien ohne übermäßige

Verzögerung zugreifen zu können.

1.1.5 Datensicherung bei mobilen IT-Systemen (Notebooks, PDA, ...)

Beim Einsatz von mobilen IT-Systemen ist es unvermeidbar, dass Daten zumindest zeitweise nicht auf einem zentralen Server gespeichert und daher nicht von der üblichen Datensicherung erfasst werden. Sofern es sich bei diesen Daten um wichtige Produktionsdaten handelt, müssen Maßnahmen getroffen werden, um den Verlust dieser Daten zu verhindern.

Dazu bieten sich folgende Verfahren an:

- **Datensicherung auf externen Datenträgern:**
Es ist zu beachten, dass solche Datenträger (externe Festplatten, USB-Memory-Sticks, DVD-ROMs etc.) getrennt von den zugehörigen IT-Systemen aufbewahrt werden, um den gleichzeitigen Verlust, etwa bei einem Diebstahl, zu vermeiden.
- **Datensicherung über Verbindung mit dem Firmennetzwerk:**
Dabei werden die Daten vom Standort des Mitarbeiters direkt zum zentralen Server übertragen. Es ist vor allem für eine ausreichende Übertragungsgeschwindigkeit sowie eine sichere (verschlüsselte) Übertragung der Daten zu sorgen.
- **Datensicherung bei der Rückkehr ins Firmennetzwerk:**
Dieses Verfahren ist allerdings nur dann empfehlenswert, wenn die Rückkehr des mobilen IT-Systems in regelmäßigen (z.B. wöchentlichen) Abständen erfolgt und der mögliche Verlust der zwischenzeitlich lokal gespeicherten Daten tragbar erscheint.

Die ersten beiden Verfahren bringen auch zusätzlichen Aufwand sowie zusätzliche Verantwortung für die jeweiligen Benutzer mit sich. Durch den Einsatz geeigneter Software-Tools ist es unter Umständen möglich, den nötigen Arbeitsaufwand zu verringern. Mitarbeiter mit mobilen IT-Systemen sollten aber besonders auf die Wichtigkeit regelmäßiger Datensicherungen und über die möglichen Folgen einer Unterlassung hingewiesen werden.

1.2 Notfallvorsorge und -wiederherstellung

Vor allem in Betrieben, in denen ein großer Teil der Wertschöpfung auf dem Funktionieren der IT-Infrastruktur beruht, ist es wichtig, rechtzeitig Überlegungen zum Abwenden und Bewältigen von Notfällen anzustellen. Notfälle sind kostspielig; ihre Kosten entstehen nicht nur durch Maßnahmen zu ihrer Behebung, sondern vor allem auch durch den Verlust an produktiver Arbeitszeit. Ein Notfallkonzept hilft, diese Ausfallszeiten zu minimieren und möglichst rasch zum normalen Produktionsbetrieb zurückzukehren.

1.2.1 Erhebung der wichtigsten Anwendungen

Erster Schritt jeder Notfallvorsorge ist das Festlegen von Prioritäten für die einzelnen Anwendungen.

Für die Notfallvorsorge ist es unerlässlich, die Anwendungen mit den höchsten Verfügbarkeitsanforderungen ausfindig zu machen. Im nächsten Schritt müssen jene Teile der IT-Systeme (wie z.B. Server, Daten, Datenleitungen), die für den Betrieb dieser Anwendungen nötig sind, identifiziert werden. Die Notfallplanung sollte sich vorwiegend auf diese zentralen Komponenten konzentrieren.

Viele Anwendungen sind auf das Funktionieren verschiedener Systemteile angewiesen: Eine Web-Applikation benötigt z.B. neben dem eigentlichen Webserver oft einen Datenbankserver sowie verschiedene Netzwerkkomponenten (Firewall, Router, Switch ...), die den Zugang aus dem Internet ermöglichen. Das Funktionieren des Domänen-Controllers einer Windows-Domäne ist Voraussetzung für die meisten Benutzeraktivitäten. Für E-Mail-Verkehr wird die Internetanbindung inklusive aller zugehörigen Netzwerkkomponenten, ein E-Mail-Client sowie evtl. auch ein Mailserver und ein Domänen-Controller gebraucht. In jedem dieser Fälle sind die einzelnen Komponenten als zusammengehörige Gruppe zu betrachten, an die die gleichen Verfügbarkeitsanforderungen gestellt werden und für die gleichermaßen Überlegungen zu Notfallmaßnahmen angestellt werden müssen.

1.2.2 Notfallvorsorge und eingeschränkter Ersatzbetrieb

Durch verschiedene Maßnahmen ist es möglich, Notfälle abzuwenden oder ihre Auswirkungen abzumildern.

Es ist oft möglich, mit relativ kleinem Aufwand Notfälle drastisch zu verkürzen: Ein einziger Ersatzrechner, z.B. ein Firmennotebook, das zeitweise auch für andere Zwecke genutzt werden kann, kann ausreichen, um den Ausfall einzelner Clientrechner vollständig zu überbrücken. Als Ersatzgeräte für zentrale Netzwerkkomponenten können veraltete Geräte zurückbehalten werden, als Ersatz für einen Breitband-Internetzugang bietet sich z.B. ein (ansonsten deaktiviertes) (ISDN-)Modem an.

Für wichtige Serversysteme, deren Ausfall zu finanziellen Einbußen führen kann (z.B. stark frequentierte Webshops), empfiehlt es sich, "gespiegelte Systeme" vorrätig zu halten, die bei Bedarf aktiviert werden können. Grundsätzlich müssen Backup-Rechner, da sie nicht dafür vorgesehen sind, über einen längeren Zeitraum eingesetzt zu werden, nicht den gleichen technischen Leistungsstandards entsprechen wie die Systeme, die sie ersetzen sollen. Dadurch können unter Umständen auch alte Rechner, die bereits durch neue Systeme ersetzt wurden oder auch weniger leistungsstarke und dadurch kostengünstigere Neu-Systeme für diese Aufgabe herangezogen werden.

In vielen Notfällen ist es möglich, trotz des Ausfalls einzelner Systemkomponenten einen eingeschränkten Notbetrieb aufrechtzuerhalten. Dazu können verschiedene Szenarien entwickelt werden - Ausfall des Domänen-Controllers, Ausfall der Internetanbindung, Ausfall aller zentralen Server... - und für diese Fälle Lösungen ausfindig gemacht werden, um die wichtigsten Unternehmensfunktionen aufrechtzuerhalten. Diese Szenarien sollten in jedem Fall schriftlich dokumentiert werden, zum einen, um im Notfall rasch abrufbar zu sein.

1.2.3 Notfallwiederherstellung

Für die Rückkehr zum Normalbetrieb ist es notwendig, die ausgefallenen Systemkomponenten wiederherzustellen. Durch das Planen und Testen von Wiederherstellungsverfahren lässt sich dieser Prozess verkürzen. Vor allem kann dadurch aber vermieden werden, dass sich verschiedene Datenbestände erst beim Wiederherstellungsversuch als nicht mehr rekonstruierbar herausstellen.

Bei Servern oder Clientrechnern sind verschiedenste Methoden der Notfallwiederherstellung möglich: Das Betriebssystem kann manuell oder skriptgesteuert vom Installationsmedium neu installiert werden, auch ein Datenträger-Image kann dazu verwendet werden. Danach erfolgt das Einspielen der Daten aus der letzten Datensicherung. Verschiedene Backup-Programme ermöglichen auch die automatisierte Notfallwiederherstellung von damit gesicherten Servern. Diese Methoden unterscheiden sich stark in Geschwindigkeit, Arbeitsaufwand und Zuverlässigkeit; sie müssen unbedingt getestet werden, um ihre Funktionsfähigkeit im Notfall sicherzustellen. Um im Notfall sicher und rasch reagieren zu können, ist es unbedingt anzuraten, die Backup/Restore-Methoden detailliert und ausführlich zu dokumentieren. Eine ausführliche Dokumentation des Wiederherstellungsverfahrens hilft außerdem in Fällen, in denen der für die Wiederherstellung Verantwortliche nicht greifbar ist. Sie sollte ausreichen, um anderen technisch geschulten Personen die Durchführung des Verfahrens zu ermöglichen.

Die Grundlage für die Wiederherstellung zentraler Rechner, insbesondere von Serversystemen, ist beinahe immer die Datensicherung. Nach dem Festlegen und Testen von Wiederherstellungsverfahren müssen die Einstellungen der Datensicherung häufig überprüft und korrigiert werden.

Häufige Ursache für Notfälle sind Hardwareprobleme, wie z.B. Defekte an Netzteilen oder Festplatten von Serversystemen. Besonders bei Marken-Systemen wird oft Hardware eingesetzt, die bei Ausfällen nur schwer oder zu sehr hohen Kosten wiederzubeschaffen ist. Für zentrale, wichtige Systeme sollten daher Wartungsverträge abgeschlossen werden, um den raschen Ersatz defekter Komponenten sicherzustellen. Oft sind derartige Wartungsverträge nur zum Zeitpunkt der Anschaffung der Komponenten günstig erhältlich. Diese Gelegenheit sollte daher möglichst genutzt werden.

2 Internetzugang und Netzwerke

2.1 Sichere Anbindung an das Internet

Die Vernetzung vorhandener Firmennetzwerke mit dem Internet (oder anderen Fremdnetzen) lässt Gefährdungen entstehen, da prinzipiell nicht nur vom Firmennetzwerk auf das Internet, sondern auch vom Internet auf das Firmennetz zugegriffen werden kann. Darüber hinaus gefährdet die Möglichkeit "remote" d.h. von einem entfernten Rechner aus, Befehle auf Rechnern im lokalen Netz ausführen zu lassen, die Sicherheit der lokalen Rechner und dadurch auch die Vertraulichkeit der Firmendaten. Weitere Gefahren gehen von Schadprogrammen (Viren, Würmer, Spyware, Adware etc). aus.

IT-Systeme, die zeitweise oder dauernd mit dem firmeninternen Netzwerk verbunden sind, dürfen nur unter Verwendung ausreichender Sicherheitseinrichtungen mit dem Internet verbunden werden. Solche Sicherheitseinrichtungen werden als "Firewalls" bezeichnet.

Eine Firewall kontrolliert die Netzwerkverbindungen zwischen Firmennetzwerk und Internet und blockiert alle jene Verbindungen, die nicht explizit als "erlaubt" deklariert wurden. Firewalls sind in unterschiedlichsten Ausführungen und Preisklassen erhältlich, die Palette reicht von Breitband-Routern mit integrierter Paketfilter-Firewall bis zu hochleistungsfähigen Firewall-Appliances mit verschiedenen Schutzzonen. Sie unterscheiden sich stark in ihrer Leistungsfähigkeit und Schutzwirkung.

Weiters wird grundsätzlich zwischen Firewalls im klassischen Sinn und Personal Firewalls unterschieden. Bei ersteren handelt es sich um Hardware, die physisch zwischen Internet und Firmennetz installiert wird und somit das gesamte Netzwerk (mehrere Rechner) oder wesentliche Teile davon schützen. Eine Personal Firewall ist ein Programm, das den Datenverkehr eines einzelnen Rechners kontrolliert und gegebenenfalls unterbindet. Dies gilt sowohl für die Kommunikation zum Rechner als auch vom Rechner.

2.1.1 Einsatz einer Firewall

Die Firewall muss korrekt installiert und korrekt administriert werden. Damit sie einen wirkungsvollen Schutz des lokalen Netzes gegen Angriffe von außen bietet, müssen einige grundlegende Voraussetzungen erfüllt sein:

- Jede Kommunikation zwischen Firmennetz und Internet muss ausnahmslos über die Firewall geführt werden.
- Die Konfiguration und Administration der Firewall darf nur über einen gesicherten Weg möglich sein. Angreifen aus dem Internet darf es nicht möglich sein, die Konfiguration der Firewall zu verändern oder auszulesen. Auch aus dem Firmennetzwerk darf der Zugang nur befugten Personen möglich sein.
- Eine richtig konfigurierte Firewall gestattet nur die unbedingt notwendigen und tatsächlich gebrauchten Verbindungen.

Die Verbindungen aus dem Firmennetzwerk in das Internet richten sich nach den für die Arbeit benötigten Internetdiensten, die zunächst je Arbeitsplatz erhoben werden müssen. Im Allgemeinen werden folgende typische Internetdienste bzw. Ports (Kanäle) genutzt:

- WWW via HTTP und HTTPS: TCP-Ports 80 und 443
- FTP: TCP/UDP-Ports 20 und 21
- SMTP (E-Mail-Versand und -Empfang): TCP/UDP-Port 25
- POP3 (E-Mailabruf beim Internet-Provider): TCP/UDP-Port 110
- IMAP (E-Mailabruf beim Internet-Provider): TCP/UDP-Port 143
- NNTP (Network News-Dienst): TCP/UDP-Port 119

- DNS: TCP/UDP-Port 53

Nicht alle diese Dienste sind auf allen Rechnern erforderlich; es sollten möglichst nur die tatsächlich benötigten Ports freigeschaltet werden.

Die korrekte Planung und Konfiguration einer Firewall ist komplex. Sie ist aber von höchster Wichtigkeit für die Sicherheit des Firmennetzwerkes und der verwendeten Daten und sollte in jedem Fall durch qualifiziertes Fachpersonal durchgeführt werden.

2.1.2 Personal Firewalls

In Fällen, in denen der Einsatz einer klassischen Firewall nicht möglich oder unangemessen erscheint, beispielsweise beim Betrieb eines einzelnen Rechners mit Internetanschluss, bieten Personal Firewalls zumindest minimalen Schutz gegen Fremdzugriffe. Bei korrekter Konfiguration können sie aber auch in Firmennetzen, die durch eine eigene Firewall geschützt sind, eingesetzt werden, um Schutz vor unzulässigen Verbindungen zu gewähren.

Typischerweise funktioniert eine Personal Firewall auf Anwendungsbasis und "erlernt" zulässige Verbindungen aufgrund von Benutzereingaben: Beim ersten Verbindungsversuch eines Programms (z.B. des Internet-Browsers) mit dem Netzwerk wird der Benutzer gefragt, ob diese Verbindung gestattet sein soll. Erlaubt dieser die Verbindung, wird sie in Zukunft ohne weitere Abfrage zugelassen.

Eine Personal Firewall kann den Schutz einzelner, mit dem Internet verbundener PCs verbessern. Es gibt allerdings auch einige Bedenken:

- Die Abfrage, welchen Programmen die Verbindung zum Internet gestattet werden soll, kann die Anwender überfordern. Einigen Programmen (insbes. jenen, die selbsttätig nach Produktaktualisierungen und Updates suchen, wie z.B. Virenschutzprogramme) ist diese Verbindung zu erlauben, bei anderen Programmen (insbes. Schadprogramme wie Trojaner oder Spyware) ist der Verbindungsversuch als Alarmsignal zu werten. Diese Unterscheidung kann selbst gut ausgebildeten Administratoren mitunter schwer fallen.
- Schadprogramme, die den Computer befallen haben, können prinzipiell auch die Personal Firewall manipulieren oder sogar ausschalten. In diesem Fall wäre der vermeintlich geschützte Rechner wieder problemlos aus dem Internet erreichbar.

Es ist umstritten, ob das Sicherheitsniveau einer Personal Firewall nicht ebenso gut durch andere Maßnahmen erzielt werden kann. Folgende Punkte können in jedem Fall helfen, die Sicherheit einzelner Rechner, die mit dem Internet verbunden sind, zu erhöhen:

- Zeitgerechtes Durchführen von Sicherheits-Updates, insbes. im Betriebssystembereich. Die automatische Durchführung solcher Updates ist unbedingt zu empfehlen.
- Betrieb einer Virenschutzlösung. Die regelmäßige Aktualisierung durch den automatischen Download der neuesten Virensignaturdateien ist dabei unerlässlich.
- Vorsichtiges Surf- und Downloadverhalten: Im Umgang mit dem Internet sollten nur vertrauenswürdige Webseiten aufgerufen werden; das Herunterladen und Installieren frei erhältlicher Zusatzprogramme aus dem Internet sollte möglichst vermieden werden, da diese oft Schadprogramme (insbes. Spyware) enthalten.

2.1.3 Wireless LAN (WLAN)

Drahtlose Netzwerke, so genannte WLAN (Wireless Local Area Networks) -Lösungen ergänzen zunehmend traditionelle LANs, bei denen der Netzwerkanschluss über Kabelverbindungen realisiert wird. Zum einen bieten sie Flexibilität bei der Arbeitsplatzgestaltung, zum anderen sind für ihren Aufbau keine aufwändigen Verkabelungsarbeiten notwendig. Die steigende Zahl von portablen Computern (Notebooks, PDAs, etc.) unterstreicht die Forderung nach einem WLAN. Sicherheitstechnisch entstehen neue Gefährdungen und es sind einige Maßnahmen zu beachten, um nicht durch die Einführung von WLANs die Sicherheit des gesamten lokalen Netzwerkes zu kompromittieren.

Sicherheitsmängel in WLAN-Netzwerken waren in den letzten Jahren häufig der Grund für erfolgreiche Attacken. Dabei handelte es sich zum Teil um Konfigurationsmängel, zum Teil aber

auch um Schwächen in den zugrundeliegenden Verschlüsselungsprotokollen. Die Entwicklungen der letzten Zeit zielen u.a. auf die Behebung dieser Schwachstellen mittels neuer Technologien und Standards ab; sicherheitstechnisch ist es daher wichtig, möglichst nur aktuelle WLAN-Komponenten einzusetzen bzw. wenn möglich, ältere Geräte mittels Firmware-Updates zu aktualisieren.

Die Bedrohung darf nicht unterschätzt werden; manchenorts ist das "War-Driving", d.h. das Aufspüren und Eindringen in WLAN-Netze, zu einer Art Sport geworden. Im Internet existieren Listen von WLAN-Netzen, die nicht gesichert und für jedermann zugänglich sind. Die Nutzung eines solchen ungeschützten Netzes als kostenloser drahtloser Internetzugang ist noch die harmloseste Art des Missbrauches, das Ausspionieren von Firmendaten die weitaus bedenklichere, aber nicht zwingend kompliziertere Variante. Vor der Planung und Installation einer WLAN-Lösung bzw. zur besseren Absicherung bereits bestehender Anlagen sollten daher unbedingt die neuesten Entwicklungen und Sicherheitshinweise recherchiert werden.

An dieser Stelle sind nur Hinweise auf einige Maßnahmen möglich, die von den zuständigen Administratoren beachtet werden sollten:

- Geeignete Positionierung und Ausrichtung der Zugriffspunkte und Antennen - außerhalb des Betriebsgeländes sollte der WLAN-Empfang möglichst verhindert werden.
- Deaktivieren des Sendens der Service Set ID (SSID)
- Verschlüsselungsoptionen aktivieren: mindestens WEP-128 Bit, die allerdings keinen sicheren Schutz bietet; besser: WPA/AES
- Ändern der Standardeinstellungen (Passwörter) an Access Point und Clients
- Aktivieren der MAC-Adressfilterung am Access Point
- Deaktivieren des DHCP-Servers am Access Point
- Verwendung von Authentifikationsmöglichkeiten nach IEEE 802.1X

2.1.4 Festlegung einer WWW-Sicherheitsstrategie

Sicherheitsstrategie für die Nutzung des World Wide Web (WWW)

In der Sicherheitsstrategie für die WWW-Nutzung sollten die folgenden Fragen beantwortet werden:

- Wer erhält WWW-Zugang?
- Welche Randbedingungen sind bei der WWW-Nutzung zu beachten?
- Wie werden die Benutzer geschult?
- Wie wird technische Hilfestellung für die Benutzer gewährleistet?

Durch organisatorische Regelungen oder durch die technische Umsetzung sind dabei insbesondere folgende Punkte zu gewährleisten:

- Die Browser der Benutzer müssen durch den Administrator so vorkonfiguriert sein, dass ohne weiteres Zutun der Benutzer maximale Sicherheit erreicht werden kann.
- Nach dem Download von Dateien sind diese explizit auf Viren zu überprüfen, soweit dies nicht durch eine zentrale Überprüfung gewährleistet wird.

Alle Regelungen und Bedienungshinweise zur Internet-Nutzung sollten schriftlich fixiert werden und den Mitarbeitern jederzeit zur Verfügung stehen.

Die Mitarbeiter müssen geschult werden, um Fehlbedienungen zu vermeiden und die Einhaltung der organisationsinternen Richtlinien zu gewährleisten. Insbesondere müssen sie hinsichtlich möglicher Gefährdungen aus dem Internet und einzuhaltender Sicherheitsmaßnahmen sensibilisiert werden.

2.1.5 Sicherheit von Internet-Browsern

Beim Zugriff auf das World Wide Web können verschiedene Sicherheitsprobleme auf den angeschlossenen Arbeitsplatzrechnern auftreten.

Ursachen dafür können sein:

- falsche Handhabung durch die Benutzer
- unzureichende Konfiguration der benutzten Browser (also der Programme für den Zugriff auf das WWW)
- Sicherheitslücken in den Browsern.

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. 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 Word- oder Excel-Dokumenten).

Im Umgang mit dem Internet sollten nur vertrauenswürdige Webseiten aufgerufen werden; das Herunterladen und Installieren frei erhältlicher Zusatzprogramme aus dem Internet sollte möglichst vermieden werden, da diese auch oft Schadprogramme (insbes. Spyware) enthalten.

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, Würmer und trojanische Pferde. Die Benutzer dürfen sich nie darauf verlassen, dass die geladenen Dateien oder Programme aus vertrauenswürdigen Quellen stammen.

Bei der Konfiguration des Browsers ist darauf zu achten, dass bei Dateitypen, die Makro-Viren enthalten können, die zugehörigen Anwendungen nicht automatisch gestartet werden.

Aktuelle Virenschutzprogramme sollten auf allen Rechnern mit Internetzugang installiert sein und automatisch ausgeführt werden. Die regelmäßige Aktualisierung durch den automatischen Download der neuesten Virensignatordateien ist dabei unerlässlich

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.

Regelungen:

Ein Großteil der oben beschriebenen Maßnahmen liegt im Verantwortungsbereich der Benutzer, da deren Umsetzung wie beispielsweise die Aktivierung bestimmter Optionen nicht ständig 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.

2.2 Sicherheit des Firmennetzwerks

2.2.1 Update/Upgrade von Soft- und Hardware im Netzbereich

Ähnlich wie bei Betriebssystemen können auch bei Netzwerkkomponenten (Router, Switches, Firewalls) Updates der Soft- bzw. Firmware durchgeführt werden, um neu entdeckte Schwachstellen zu beseitigen oder die Geräte um neue Funktionen zu erweitern.

Angesichts der hohen Wichtigkeit für die Sicherheit des Firmennetzwerks sollte vor allem bei Firewall- und Router-Software versucht werden, auf aktuellem Stand zu bleiben.

Falls im Firmennetzwerk WLAN-Komponenten betrieben werden, sollte ebenfalls regelmäßig überprüft werden, ob neue Firmware-Versionen zur Verfügung stehen. Die Entwicklung von Sicherheits-Features erfolgt in diesem Bereich sehr rasch, der Einsatz veralteter Technologien kann zur Bedrohung des gesamten Netzwerks und der Firmendaten führen. Unter Umständen kann auch ein Austausch bzw. Upgrade der WLAN-Hardware notwendig werden, wenn es nicht möglich ist, die bestehenden Komponenten durch Updates auf den letzten Stand zu bringen. Bevor ein Upgrade oder ein Update vorgenommen wird, muss die Funktionalität der neuen Komponenten genau geprüft werden. Auch mögliche Verfahren zum Rückgängigmachen des Updates sollten rechtzeitig recherchiert werden. Vor Durchführung der Änderungen müssen

außerdem zumindest die wichtigsten Konfigurationseinstellungen festgehalten werden; falls nicht anders möglich, kann das in Form von Screenshots oder schriftlichen Aufzeichnungen geschehen. Allgemein bekannte Passwörter wie z.B. jene Passwörter, die bestimmte IT-Komponenten im Auslieferungszustand aufweisen (Default-Passwörter), müssen in jedem Fall geändert werden. Das betrifft insbesondere Netzwerkkomponenten (Router, Switches ...), bei denen derartige Default-Passwörter weit verbreitet und auch weithin bekannt sind.

2.2.2 Festlegung einer Sicherheitsstrategie für ein Client-Server-Netz

Client-Server-Netze, wie sie z.B. durch MS Windows-Domänen realisiert werden können, bieten große Vorteile bei der Verwaltung von Benutzer- und Zugriffsrechten. Für den sicheren Betrieb sollten allerdings einige Punkte geklärt und schriftlich fixiert werden.

Folgende Punkte sind von besonderer Bedeutung:

- **Regelung der Verantwortlichkeiten:**
Ein Client-Server-Netz sollte von geschulten Netzadministratoren und deren Stellvertretern betrieben werden. Es ist ausschließlich den Administratoren vorbehalten, sicherheitsrelevante Einstellungen zu verändern. Sie allein dürfen Sicherheitsparameter im Netz verändern und wichtige Aufgaben wie z.B. das Anlegen neuer Benutzerkonten durchführen.
- **Festlegung von Namenskonventionen:**
Um die Verwaltung zu vereinfachen, sollten eindeutige Namen für Rechner, Benutzergruppen und Benutzer sowie Drucker und Freigabenamen verwendet werden. Diese Namen sollten nach Möglichkeit einem klaren Schema folgen. Beispielsweise können Benutzernamen aus dem Anfangsbuchstaben des Vornamens sowie dem vollständigen Nachnamen des jeweiligen Benutzers gebildet werden (fmaier, Imüller...). Rechnernamen sollten durchnummeriert werden (pc01, pc02, etc.). Die Namenskonventionen sollen den Administratoren und Benutzern das leichte Auffinden der gesuchten Objekte ermöglichen.
- **Festlegung der Regeln für Benutzerkonten:**
Vor der Einrichtung von Benutzerkonten sollten Restriktionen, die für diese Accounts gelten sollen, festgelegt werden. Dies betrifft insbesondere die Regelungen für Passwörter und für die Reaktion des Systems auf fehlerhafte Login-Vorgänge.
- **Einrichtung von Gruppen:**
Benutzerkonten, für die gleiche Anforderungen gelten, sollten zu Gruppen zusammengefasst werden. Benutzerrechte sowie Datei-, Verzeichnis- und Freigabeberechtigungen werden den Gruppen und nicht einzelnen Benutzeraccounts zugeordnet; die Benutzeraccounts erben die Rechte der Gruppen, denen sie angehören. Die Zuweisung von Berechtigungen an einzelne Benutzer sollte nur erfolgen, wenn dies unumgänglich ist, da sie z.B. bei Änderungen der Rechtevergabe oder beim Ausscheiden von Mitarbeitern nur sehr schwer nachverfolgbar ist.
- **Festlegung der Vorgaben für Protokollierung:**
Die Sicherheitsprotokollierung dient vor allem dazu, Sicherheitsverstöße wie z.B. unerlaubte Zugriffe oder Anmeldeversuche unbefugter Personen auffindig zu machen. Sie kann verschieden eingestellt werden, die Protokolle können in ihrem Umfang und ihrer Detailtiefe stark variieren. Hier sollte versucht werden, ein Gleichgewicht zwischen Sicherheitsbedarf und Protokollumfang zu erreichen, sodass es den Administratoren im Rahmen zumindest stichprobenartiger, regelmäßiger Kontrollen möglich ist, die relevanten Ereignisse aufzuspüren. Dabei sind außerdem die Anforderungen aus gesetzlichen Vorgaben (insbes. Datenschutzgesetz) einzuhalten.
- **Regelungen zur Datenspeicherung:**
Vor Aufnahme des Netzbetriebs muss festgelegt werden, wo Produktionsdaten gespeichert werden. Ein typisches Modell sieht beispielsweise vor, dass alle wichtigen Produktionsdaten ausschließlich auf Serverlaufwerken zu speichern sind, die im Rahmen regelmäßiger Backups gesichert werden; auf den (ungesicherten) Festplatten der Arbeitsplatzrechner dürfen dann ausschließlich entbehrliche Daten abgelegt werden. Im Rahmen dieser Regelungen sollte auch festgelegt werden, welche Daten auf "persönlichen", d.h. nur dem jeweiligen Benutzer zugänglichen Laufwerken und welche

auf anderen, abteilungs- oder unternehmensweit zugänglichen Serverlaufwerken gespeichert werden sollen. Diese Vorgabe ist u.a. im Vertretungsfall, z.B. bei Erkrankung eines Mitarbeiters, von großer Bedeutung.

- **Einrichtung einer geeigneten Verzeichnisstruktur:**
Um eine saubere Trennung von benutzer-, abteilungs- und projektspezifischen Daten untereinander durchzusetzen, sollte eine geeignete Verzeichnisstruktur festgelegt werden, mit der die entsprechende Dateiablage unterstützt wird. Dazu existieren verschiedene Modelle; die Auswahl der geeignetsten Struktur ist stark von den Arbeitsabläufen im jeweiligen Unternehmen abhängig. Es ist oft notwendig, die Dateistruktur nach einem ersten Probetrieb nachträglich an die tatsächlichen Erfordernisse anzupassen.
- **Vergabe der Zugriffsrechte:**
Es muss festgelegt werden, welche Verzeichnisse und Dateien für den Betrieb freizugeben und welche Zugriffsrechte ihnen zuzuweisen sind. Dies gilt auch für die Freigabe von Druckern und anderen Peripheriegeräten.
- **Verantwortlichkeiten für Administratoren und Benutzer im Client-Server-Netz:**
Neben der Wahrnehmung der Netzmanagementaufgaben müssen weitere Verantwortlichkeiten festgelegt werden. Administratoren kann beispielsweise die Verantwortung für folgende Aufgaben übertragen werden:
 - Auswertung der Protokolldateien auf den einzelnen Servern oder Clients
 - Vergabe von Zugriffsrechten
 - Hinterlegung und Wechsel von Passwörtern
 - Durchführung von Datensicherungen

Sofern den Endbenutzern administrative Funktionen übertragen wurden, müssen auch ihre Verantwortlichkeiten fixiert werden. Abgesehen davon sind sie zur Unterstützung der Administratoren in sicherheitsrelevanten Belangen zu verpflichten, z.B. durch das Melden verdächtiger Vorfälle oder die Benachrichtigung der Administratoren über das Ausscheiden oder den Eintritt von Mitarbeitern.

- **Schulungen:**
Abschließend muss festgelegt werden, welche Benutzer zu welchen Punkten geschult werden müssen. Erst nach ausreichender Schulung kann der Echtbetrieb aufgenommen werden. Insbesondere die Administratoren sind hinsichtlich der Verwaltung und der Sicherheit des Systems gründlich zu schulen.

Die so entwickelte Sicherheitsstrategie sollte angemessen dokumentiert und bei Veränderungen umgehend aktualisiert werden.

2.3 Sicherheit beim Serverbetrieb

2.3.1 Sicherer Betrieb eines Mail-Servers

Der sichere Betrieb eines Mailserver 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. Weiters reicht der Mailserver die gesendeten 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.

Für Mailserver gelten ähnliche Auflagen wie für andere Server: Sie müssen vor unbefugten physischen Zugriffen geschützt aufgestellt werden, sicherheitsrelevante Software-Updates sind umgehend einzuspielen, Konfigurations- und Produktionsdaten (in diesem Fall E-Mails) müssen regelmäßig gesichert werden.

Zusätzlich sind einige weitere Punkte zu berücksichtigen:

- Mailserver sind im Allgemeinen relativ wartungsintensiv. Für den sicheren Betrieb müssen ein geschulter Administrator sowie entsprechende Stellvertreter zur Verfügung stehen.
- Bei längerem Ausbleiben eingehender E-Mails sollte unbedingt die Funktion des Mailservers überprüft werden. Ein längerer (mehrtägiger) Stillstand des Mailservers kann unter Umständen zum Verlust von E-Mails, die an das Unternehmen übermittelt werden sollen, führen. Für die rechtzeitige Problembeseitigung sollten daher immer der betreffende Administrator oder ein fachkundiger Stellvertreter zur Verfügung stehen.
- Da E-Mails ein bevorzugtes Einfallstor für Viren und andere Schadprogramme darstellen, muss auf dem Mailserver ein aktuelles, gut gewartetes Virenschutzprogramm betrieben werden. Um die Trefferquote zu erhöhen, ist es günstig, am Mailserver andere Software als auf den Clients zu betreiben. Noch besser ist es, dem internen Mailserver einen gesonderten SMTP-Proxy mit eigener Virenschutzsoftware vorzuschalten; durch diese Anlage lässt sich auch eine bessere Absicherung des Firmennetzes gegen das Internet erzielen.
- Um E-Mails von Mailservern anderer Unternehmen empfangen zu können, muss der Mailserver über das Internet erreichbar sein. Er muss daher durch eine entsprechende Konfiguration der Firewall gegen unbefugte Zugriffe abgesichert werden. In den meisten Fällen ist es ausreichend, ausschließlich den Zugang über TCP-Port 25 (SMTP) zuzulassen, alle anderen eingehenden Verbindungen müssen blockiert werden.
- Der Versand und die Zustellung ein- und ausgehender E-Mails muss protokolliert werden. Die Protokolle können bei der Nachverfolgung verloren gegangener oder unzustellbarer E-Mails wichtige Informationen liefern.
- Falsch konfigurierte Mailserver werden häufig als Spam-Relays missbraucht, d.h. sie werden verwendet, um Spam-Mails in großer Menge an andere Empfänger zuzustellen. Auf die korrekte Konfiguration ist daher besonders zu achten. Vor allem sollte der Server nur Mails versenden, die von Rechnern im Firmennetzwerk stammen und die Zustellung eingehender Mails nur für jene E-Mail-Adressen akzeptieren, die im Firmennetzwerk tatsächlich vorhanden sind. Zum Test des Mailservers auf richtiges Verhalten kann z.B. auf <http://www.ordb.org> um eine kostenlose Überprüfung angesucht werden.
- Auf dem Mailserver kann auch das Ausfiltern eingehender Spam-Mails erfolgen. Das kann über verschiedene Filterregeln oder durch den Einsatz zusätzlicher Software geschehen. Mit Filterregeln können im Allgemeinen kaum gute Ergebnisse erzielt werden, abhängig von der tatsächlichen Belastung können sie aber ausreichen. Spezialisierte Software kann bei entsprechender Wartung zu sehr guten Erkennungsraten gelangen, eine hundertprozentige Trefferquote ist aber nie erreichbar. E-Mails, die als Spam erkannt wurden, sollten daher nie sofort verworfen werden. Als praktikable Lösung hat sich die Kennzeichnung dieser Mails im Betreff-Text erwiesen. Die mit "Spam" gekennzeichneten Mails können dann von den Benutzern rasch geprüft und anschließend gelöscht werden.

2.3.2 Sicherer Betrieb eines WWW-Servers

WWW-Server sind attraktive Ziele für Angreifer und müssen daher sehr sorgfältig konfiguriert werden, damit sie sicher betrieben werden können. Das Betriebssystem und die Software müssen so konfiguriert sein, dass der Rechner optimal gegen Angriffe geschützt wird. Solange der Rechner nicht entsprechend konfiguriert ist, darf er nicht ans Netz genommen werden.

Angriffe auf WWW-Server können verschiedene Formen annehmen: Am verbreitetsten ist die Veränderung der Inhalte, beispielsweise durch die auffällige Änderung der Homepage (Website Defacement). Ziel eines Angriffs kann aber auch sein, über den Webserver Zugriff auf das dahinterliegende Firmennetzwerk zu erhalten. Häufig wird auch versucht, auf schlecht gesicherten Webservern pornografische Inhalte oder raubkopierte Software (sogen. Warez) abzuspeichern und anderen Usern zur Verfügung zu stellen. Alle diese Angriffe können zumindest Imageschäden verursachen, unter Umständen können sie sogar rechtliche Konsequenzen für das Unternehmen nach sich ziehen.

Bei einem Webserver, der aus dem Internet erreichbar ist, müssen daher folgende Vorgaben beachtet werden:

- Auf dem Server sollte nur das absolut notwendige Minimum an Programmen vorhanden sein: Das Betriebssystem sollte auf die unbedingt erforderlichen Funktionalitäten reduziert werden, auch sonst sollten sich nur unbedingt benötigte Programme und Daten auf dem Server befinden.
- Ein WWW-Server sollte insbesondere keine unnötigen Netzdienste enthalten, öffentlich zugänglich dürfen nur der HTTP bzw. HTTPS-Dienst sowie gegebenenfalls der FTP-Dienst sein.
- Der Zugriff auf Dateien oder Verzeichnisse muss geschützt werden.
- Die Kommunikation zwischen Webserver und Internet muss durch eine entsprechend konfigurierte Firewall auf das Minimum beschränkt werden.
- Die Administration des WWW-Servers darf nur über sichere Verbindungen erfolgen. Im Idealfall ist sie nur nach starker Authentisierung aus dem Firmennetzwerk oder an der lokalen Konsole möglich. Sollte es notwendig sein, die Fernadministration über das Internet vorzusehen, muss diese über eine verschlüsselte Verbindung erfolgen.
- Die Kommunikation zwischen Firmennetzwerk und Webserver ist besonders gut abzusichern, am besten durch eine weitere Firewall-Stufe. Fehlkonfigurationen und erfolgreiche Angriffe auf den WWW-Server könnten bei ungenügender Absicherung Zugriffe auf firmeninterne Rechner und Daten ermöglichen; hier ist also besondere Vorsicht angebracht.
- Ein öffentlich zugänglicher Webserver darf keinesfalls Mitglied in einer eventuell vorhandenen, firmeninternen Windows-Domäne sein. Die Passwörter, die auf dem Server eingesetzt werden, dürfen nicht mit den intern verwendeten Passwörtern übereinstimmen.

Je nach Art des WWW-Servers bieten sich unterschiedliche Absicherungsmöglichkeiten an. Sie sind stark vom eingesetzten Betriebssystem und Produkt abhängig. Im Internet existieren verschiedene Anleitungen zur sicheren Konfiguration von Webservern, die unbedingt vor der Inbetriebnahme eingesehen werden sollten. Eine gute (allerdings englischsprachige) Quelle für derartige Konfigurationshilfen ist beispielsweise die amerikanische National Security Agency (<http://www.nsa.gov>).

2.3.3 Betrieb eines Webserver bei einem Internet-Provider (Webhosting, Serverhousing)

Alternativ zum Betrieb eines WWW-Servers im eigenen Unternehmen können auch entsprechende Angebote verschiedener Internet-Provider genutzt werden.

Der Betrieb eines Webserver im eigenen Unternehmen ist aufwendig: Ein eigener Server muss beschafft und gewartet werden. Ausreichend geschultes Personal ist notwendig, um den Betrieb des Rechners zu überwachen und regelmäßig die Zugriffsprotokolle auszuwerten. Die Firewallkonfiguration ist entsprechend anzupassen, evtl. muss eine angemessene Firewall auch erst gekauft und installiert werden. Die bestehende Internetanbindung des Unternehmens muss bezüglich Bandbreite und Transfervolumen an den steigenden Netzwerkverkehr angepasst werden.

In den meisten Fällen ist es besonders für kleinere Unternehmen wesentlich günstiger, die Webhosting-oder Serverhousing-Angebote verschiedener Internet-Provider zu nutzen. Bei ersteren wird die Homepage des Unternehmens auf einem Server betrieben, der vom Provider selbst verwaltet und gewartet wird. Die Kosten für Webhosting sind relativ niedrig, oft ist eine ausreichende Möglichkeit bereits in den Kosten der Internetanbindung inkludiert.

Beim Serverhousing wird dem Unternehmen dagegen ein eigenständiger Server innerhalb der Infrastruktur eines Internet-Providers zur Verfügung gestellt. Diese Lösung ist teurer als Webhosting und erfordert höhere Eigenleistungen bei der Administration. Sie bietet aber größere Freiheiten bei der Konfiguration des Webserver, ist also vor allem dann interessant, wenn komplexe Web-Applikationen umgesetzt werden sollen.

Bei beiden Varianten sinkt der Wartungsaufwand für das Unternehmen beträchtlich. Auch die Änderungen an der Firewall-Struktur und der Internetanbindung entfallen. Die Gefährdung des

internen Firmennetzwerks durch erfolgreiche Angriffe auf den WWW-Server ist auszuschließen, die Bedrohung durch Website-Defacement und das unbefugte Speichern unerwünschter Inhalte bleiben allerdings bestehen.

Vor der Inbetriebnahme eines eigenen Webservers sollten die oben angeführten alternativen Möglichkeiten in jedem Fall geprüft werden. Zur Einschätzung der geeignetsten Lösung sind zumindest die technischen Erfordernisse, der personelle Aufwand zur Installation und Administration und die Kosten für Erweiterungen der Netzwerkstruktur berücksichtigt werden.

3 Virenschutz

Computer-Viren (in weiterer Folge einfach als Viren bezeichnet) gehören zu den "Schadprogrammen" ("Malware"). Dies sind Programme, die verdeckte Funktionen enthalten und damit durch Löschen, Überschreiben oder sonstige Veränderungen unkontrollierbare Schäden an Programmen und Daten bewirken können. Damit verursachen sie zusätzliche Arbeit und Kosten und haben einen negativen Einfluss auf die Vertraulichkeit, Integrität und/oder Verfügbarkeit von Daten oder Programmen.

3.1 Schadprogramme und Schutzmaßnahmen

3.1.1 Verschiedene Formen von Bedrohungen

Zu den Schadprogrammen gehören:

Viren:

Nicht-selbständige, in andere Programme oder Dateien eingebettete Programmroutinen, die sich selbst reproduzieren und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornehmen.

Trojanische Pferde:

Selbständige Programme mit verdeckter Schadensfunktion, ohne Selbstreproduktion. Trojanische Pferde dienen vor allem dazu, Computer auszuspionieren. Der Trojaner verdankt seinen Namen dem Umstand, dass die Schadensroutinen oft in vermeintlich gutartigen Programmen versteckt sind. Ein Programm, das zum Zweck der Viren-Entfernung aus dem Internet heruntergeladen wird, kann unter Umständen genau das Gegenteil bewirken. Es ist daher immer auch notwendig, die Seriosität der Quelle, von der man Programme bezieht, zu überprüfen.

Würmer:

Selbständige, selbstreproduzierende Programme, die sich in einem System (vor allem in Netzen) ausbreiten. Zu diesem Zweck verwenden viele Würmer das Adressbuch des infizierten Rechners und versenden Mails mit gefälschten Absenderadressen. Das Öffnen solcher Mails kann bei einem ungeschützten System zu einer Infizierung führen.

Spyware:

Programme, die den User und/oder sein Surfverhalten ohne sein Wissen ausspionieren. Diese Daten werden an den Hersteller der Software oder auch an Dritte, meist mit dem Zweck, personalisierte Werbung und Pop-ups einzublenden, weitergeleitet. Mittels Spyware können aber auch sensible persönliche Daten an Unbefugte übertragen werden.

Spam:

Mit Spam bezeichnet man unerwünschte Werbemails, die mittlerweile rund zwei Drittel des gesamten E-Mail-Verkehrs ausmachen. Auch bei kleineren Unternehmen ist es durchaus möglich mehrere hundert Spam-Mails pro Tag zu erhalten. Gefährlich ist Spam grundsätzlich nicht, allerdings geht beim Löschen von Werbe-Mails wertvolle Arbeitszeit verloren. Mittels eigener Spam-Filter können entweder bereits auf Provider/Mail-Server-Ebene oder auch erst am lokalen Rechner unerwünschte Mails gefiltert und gelöscht werden.

Phishing:

Phishing ist ein Kunstwort aus den beiden Begriffen "Password" und "Fishing" und bezeichnet den Versuch mittels gefälschter E-Mails an fremde Nutzerdaten (Login, Passwort, TAN etc.) zu

gelangen. Normalerweise wird der Empfänger eines solchen Mails unter Vorspiegelung falscher Tatsachen (Userdaten gingen verloren, Neuidentifikation ist notwendig ...) aufgefordert, die Webseite einer Bank (Online Shop, Kreditkarteninstitut, Auktionshaus etc.) aufzusuchen und dort seine Zugangsberechtigungen einzutippen. Diese Webseiten sind ebenfalls gefälscht und sehen den Originalen zum Verwechseln ähnlich. Die dort eingetippten Daten landen natürlich nicht bei der eigenen Bank, sondern auf den Servern von Betrügern, die dann mit den Nutzerdaten Transaktionen zum Schaden des Users durchführen. Grundsätzlich fordert kein seriöses Unternehmen seine Kunden auf, seine Userdaten über das Internet zu bestätigen. Es sind also alle diesbezüglichen Mails zu ignorieren. In Zweifelsfällen sollte man sich telefonisch mit dem (vermeintlichen) Absender in Verbindung setzen.

Dialer:

Diese Einwahl-Programme bauen, nachdem sie am Computer aktiviert wurden, eine Internetverbindung über eine 0190-Mehrwertnummer auf. Der User bleibt weiterhin online und bemerkt möglicherweise gar nicht den Wechsel der Internetverbindung. Die Aktivierung eines Dialers erfolgt in der Regel durch den User selbst, der dem Download oder der Installation eines Programms zustimmt. Die Kosten für eine Internetverbindung über einen Dialer betragen in der Regel mehrere Euro pro Minute. Betroffen davon sind allerdings "nur" Nutzer von sog. Einwahl-Internetverbindungen mittels analoger und ISDN-Modems. Bei Internetzugängen über ADSL, XDSL, Kabelmodem oder andere Breitbanddienste besteht keine Gefahr von Mehrkosten. Mittels spezieller Software kann der Rechner auf Dialer überprüft werden. Die Entfernung kann aber sehr schwierig sein.

Während früher Viren meist durch den Austausch verseuchter Datenträger verbreitet wurden, ist heute zunehmend die Verbreitung über Internet bzw. E-Mail das Problem. Bei den meisten über E-Mail verbreiteten "Viren" handelt es sich eigentlich um Würmer, die - unabhängig von der eigentlichen Schadensfunktion - schon durch ihr massenhaftes Auftreten und ihre rasante Verbreitung großes Aufsehen erregen und zu hohen Schäden führen.

Das nachfolgende Kapitel beschäftigt sich vorwiegend mit dem Schutz gegen Viren und Würmer. Die angeführten Maßnahmen sind großteils auch gegen andere Arten von Software mit Schadensfunktion, wie z.B. Trojanische Pferde anwendbar.

3.1.2 Generelle Maßnahmen zur Vorbeugung gegen Virenbefall

Die nachfolgend angeführten Maßnahmen dienen der Vorbeugung gegen Virenbefall bzw. einer Verringerung des Schadens im Falle eines Befalls.

- Regelmäßige Durchführung einer Datensicherung
- Sichere Aufbewahrung der Sicherheitskopien von Datenträgern
- Setzen des Schreibschutzes bei allen Disketten, auf die nicht geschrieben werden muss (gilt insbesondere für die meisten Programmdisketten) und bei allen ausgehenden Datenträgern.
- Überprüfung aller ein- und ausgehenden Datenträger
- Überprüfung aller vorinstallierten Neugeräte und gewarteten Geräte.
- Überprüfung aller ein- und ausgehenden Dateien über externe Netzwerke (E-Mails, Internet etc.).
- Als vorbeugende Maßnahme gegen Virenbefall empfiehlt es sich, die Boot-Reihenfolge der PCs im BIOS-Setup auf C:, A: einzustellen oder das Booten von Diskette ganz zu unterbinden.
- Es sollten nur vertrauenswürdige Programme zugelassen werden, in besonderem Maß gilt das für E-Mail-Programme. Private Software sollte auf Arbeitsplatz-Rechnern nicht zugelassen werden, um die Sicherheit des Gesamtsystems nicht zu gefährden.
- Für Probleme oder Fragen sollte den Benutzern ein zentraler Ansprechpartner bekannt sein.

3.2 Virenschutzkonzepte

3.2.1 Erstellung eines mehrstufigen Virenschutzkonzepts

Um für ein komplexes IT-System effektiven Virenschutz zu erreichen, ist ein mehrstufiges Schutzkonzept empfehlenswert, bei dem in jeder Stufe angemessene und aufeinander abgestimmte Schutzmaßnahmen realisiert werden.

Schutzmaßnahmen sind zu treffen:

- auf Ebene der Firewall
- auf Server-Ebene
- auf Client-Ebene

Ein einzelnes Virenschutzprodukt ist selbst bei guter Wartung nicht in der Lage, sämtliche in Umlauf befindlichen Virentypen zu erkennen und abzuwehren. Bei einstufigen Virenschutzlösungen, bei denen ausschließlich auf einer Ebene des IT-Systems (z.B. auf allen Client-PCs) ein Virenschutzprogramm betrieben wird, besteht daher immer das Restrisiko des Befalls durch unerkannte Schadprogramme. Mehrstufige Konzepte, bei denen einlangende Daten (insbes. E-Mails) auf verschiedenen Ebenen mehrfach von Antivirus-Produkten verschiedener Hersteller geprüft werden, können dieses Restrisiko deutlich verringern.

Die korrekte Konfiguration der Firewall schützt einerseits vor möglichen Attacken durch Schadprogramme, andererseits kann sie auch helfen, die Folgen eines Befalls durch Viren oder Trojanische Pferde zu minimieren, indem sie Verbindungsversuche solcher Schadprogramme unterbindet.

Neben den technischen Schutzmaßnahmen sollten auch organisatorische und personelle Maßnahmen eingesetzt werden, um einem Virenbefall soweit wie möglich vorzubeugen bzw. den dadurch entstehenden Schaden zu begrenzen. Eine der wichtigsten solchen Maßnahmen ist die Schulung der Benutzer im richtigen Umgang mit "verdächtigen" E-Mails oder Software.

3.2.2 Virenschutzmaßnahmen auf Firewall- und Gateway-Ebene

Viele Schadfunktionen (Nachladen von Code aus dem Internet; Übermittlung von vertraulichen Informationen aus dem geschützten Netz) benötigen definierte Verbindungswege in das Internet (Ports, Adressen), um ihre Wirkung entfalten zu können. Durch eine restriktive Politik bei den Filterregeln der Firewalls ist eine wesentliche Erhöhung der Sicherheit erreichbar.

Falls Gateway- oder Proxy-Rechner betrieben werden, können auf diesen Maßnahmen implementiert werden, um der Verbreitung von Schadprogrammen entgegenzuwirken. Auf einem Mail-Gateway (auch als Smart-Host bekannt) können beispielsweise eigene Virenschannerprodukte betrieben werden, die einlangende E-Mails prüfen, bevor sie den eigentlichen Mail-Server bzw. die Benutzer-PCs erreichen. Ebenso ist das Ausfiltern von Mails, die bestimmte, häufig zur Verbreitung von Schadprogrammen genutzte Dateitypen (*.vbs, *.wsh, *.bat, *.exe, *.scr) enthalten, auf derartigen Gateways möglich. Zusätzlich kann auf einem solchen Mail-Gateway auch ein Spam-Filter betrieben werden, um unerwünschte Massenmails auszufiltern.

Auf einem Web-Proxy, über den sämtliche HTTP-Zugriffe der Internet-Browser geleitet werden, kann Software betrieben werden, die schädliche Inhalte ausfiltert, Downloads auf Viren überprüft und den Zugriff auf unerwünschte Webseiten sperrt. Durch diese Maßnahmen ist es möglich, die Sicherheit bei Zugriffen auf das WWW deutlich zu erhöhen.

3.2.3 Virenschutzmaßnahmen auf Server-Ebene

Grundsätzlich sollte auf sämtlichen Rechnern des Unternehmens Virenschutzprogramme betrieben werden.

Auch auf File- und Datenbankservern sollte eine Virenschutzlösung eingesetzt werden. Die darauf abgelegten Daten müssen in regelmäßigen Abständen mittels vollständiger Laufwerksüberprüfungen auf Schadprogramme untersucht werden. Idealerweise erfolgt das in Form von automatischen, in der Nacht durchgeführten Prüfläufen. Auf E-Mail-Servern sollten Virenschutzprogramme zur zentralen Überprüfung des E-Mail-Verkehrs installiert werden.

3.2.4 Virenschutzmaßnahmen auf Einzelplatzrechnern

- Einsatz eines aktuellen Virenschutzprogrammes mit aktuellen Signatur-Dateien, das im Hintergrund läuft (resident) und bei bekannten Viren Alarm schlägt.
- Aktivierung der Anzeige aller Dateitypen und -endungen im Datei-Manager, Browser bzw. Mailprogramm um potenzielle Schadprogramme besser zu erkennen.
- Aktivierung des Makro-Virenschutzes von Anwendungsprogrammen (z.B. MS Word, Excel, Powerpoint) und Beachtung von Warnmeldungen.
- Wahl der höchstmöglichen Stufe in den Sicherheitseinstellungen von Internet-Browsern (Gefährdung kann von aktiven Inhalten (ActiveX, Java, JavaScript) und Skript-Sprachen (z.B. Visual Basic Script) ausgehen).
- Die Ausführung von aktiven Inhalten in E-Mail-Programmen immer unterbinden (entsprechende Optionen setzen).
- Die Konfiguration der E-Mail-Clients sollte so eingestellt sein, dass Attachments nicht automatisch geöffnet werden. Außerdem sollten als E-Mail-Editor keine Programme mit der Funktionalität von Makro-Sprachen (z.B. MS Word) oder Scripts eingesetzt werden. Bei der Verwendung des HTML-Formates ist ebenfalls Vorsicht geboten.
- Durch den Einsatz eines Firewall-Produkts auf den Einzelplatzrechnern (Personal Firewall), das Verbindungsversuche unbekannter Programme zum Internet blockiert, kann Schadsoftware ebenfalls gezielt entgegengewirkt werden. Eine zentrale Firewall, die über keine Informationen zu den aufrufenden Programmen verfügt, wird durch derartige Software wirkungsvoll ergänzt.

3.2.5 Notfallmaßnahmen im Fall von Vireninfektionen

Für Notfälle, die in Folge einer Virusinfektion auftreten können, sollten Vorkehrungen getroffen werden, um die weitere Ausbreitung der Viren zu verhindern und möglichst rasch die Rückkehr zum Normalbetrieb einleiten zu können.

- Ein Programm an Erstmaßnahmen, die eine Weiterverbreitung von Viren verhindern, sollte erstellt werden. Dazu können u.a. das Herunterfahren des Mail-Servers und der betroffenen Clients, das Trennen der Internetverbindung etc. gehören.
- Den Benutzern sollte eine Ansprechperson bekannt sein, die sie in Notfällen erreichen können, um die weiteren Maßnahmen einzuleiten und zu koordinieren.
- Es muss sichergestellt sein, dass bei Vorliegen eines neuen Virus die Updates der Virenschutzprogramme möglichst rasch auf Servern, Gateways und Clients eingespielt werden. Im Fall einer zentralen Update-Verwaltung sind die entsprechenden Verteilwege und Maßnahmen vorzubereiten und regelmäßig zu testen.
- Für den Notfall sind Backup- und Restore-Strategien zu erarbeiten, die festlegen, welche Rechner in welcher Reihenfolge in betriebsbereiten Zustand zu bringen sind, damit in kürzester Zeit eine zumindest eingeschränkte Funktionsfähigkeit hergestellt werden kann.
- Falls infizierte E-Mails an andere Unternehmen (Kunden, Partner) versandt wurden, sollten diese Unternehmen darüber rasch informiert werden.
- Sollte der Virus Daten gelöscht oder verändert haben, so muss versucht werden, die Daten aus den Datensicherungen und die Programme aus den Sicherungskopien der Programme zu rekonstruieren.

3.3 Virenschutz durch die Benutzer

3.3.1 Vermeidung bzw. Erkennung von Viren durch den Benutzer

Die Sensibilisierung der Endanwender für die Virenproblematik stellt eine wichtige Komponente beim Schutz gegen Viren dar. Daher sollte in Schulungen regelmäßig auf die Gefahr von Viren, die Möglichkeiten zu ihrer Erkennung und Vermeidung sowie die notwendigen Handlungsanweisungen im Falle eines (vermuteten) Virenbefalls hingewiesen werden. Auch laufende Informationen zu diesem Thema, etwa über das Intranet oder in Form interner Publikationen, sind empfehlenswert. Erkennen potentieller Gefahren bei eingehender E-Mail und Abwehrmaßnahmen:

- Bei E-Mail auch von vermeintlich bekannten bzw. vertrauenswürdigen Absendern prüfen, ob der Text der Nachricht auch zum Absender passt (englischer Text von deutschem Partner, zweifelhafter Text oder fehlender Bezug zu konkreten Vorgängen etc.) und ob die Anlage (Attachment) auch erwartet wurde.
- Vorsicht bei mehreren E-Mails mit gleichlautendem Betreff.
- Kein "Doppelklick" bei ausführbaren Programmen (*.COM, *.EXE) oder Scripts (*.VBS, *.BAT, etc.)
- Auch E-Mails im HTML-Format oder Office-Dokumente (*.DOC, *.XLS, *.PPT, etc.) sowie Bildschirmschoner (*.SCR) können aktive Inhalte mit Schadensfunktion enthalten.
- Nur vertrauenswürdige E-Mail-Attachments öffnen (in letzter Konsequenz: nur nach telefonischer Absprache). Es ist zu beachten, dass die Art des Datei-Anhangs (Attachment) bei Sabotageangriffen oft getarnt ist und über ein Icon nicht sicher erkannt werden kann.

3.3.2 Maßnahmen bei ausgehender E-Mail:

Durch Beachtung der nachfolgenden Maßnahmen kann die Gefahr reduziert werden, dass ein Endanwender unabsichtlich Viren verteilt.

- Vermeidung aktiver Inhalte in E-Mails.
- Keine unnötigen E-Mails mit Scherz-Programmen und ähnlichem versenden, da diese evtl. einen Computer-Virus enthalten können.
- Keinen Aufforderungen zur Weiterleitung von Warnungen, Mails oder Anhängen an Freunde, Bekannten oder Kollegen folgen. Es handelt sich nämlich meist um irritierende und belästigende Mails mit Falschmeldungen (Hoax oder "elektronische Ente", Kettenbrief).
- Gelegentlich prüfen, ob E-Mails im Ausgangs-Postkorb stehen, die nicht vom Benutzer selbst verfasst wurden.

3.3.3 Verhalten bei Downloads aus dem Internet

Daten und Programme, die aus dem Internet abgerufen werden, stellen einen Hauptverbreitungsweg für Viren und Trojanische Pferde dar, um Benutzerdaten auszuspähen, weiterzuleiten, zu verändern oder zu löschen. Es muß darauf hingewiesen werden, dass auch Office-Dokumente (Text-, Tabellen- und Präsentations-Dateien) Makro-Viren enthalten können.

- Programme sollten nur von vertrauenswürdigen Seiten geladen werden, also insbesondere von den Originalseiten des Erstellers. Private Homepages, die bei anonymen Webspaces-Providern eingerichtet werden, stellen hierbei eine besondere Gefahr dar.
- Die Angabe der Größe von Dateien, sowie einer evtl. auch angegebenen Prüfsumme, sollte nach einem Download immer überprüft werden. Bei Abweichungen von der vorgegebenen Größe oder Prüfsumme ist zu vermuten, dass unzulässige Veränderungen, meist durch Viren, vorgenommen worden sind. Daher sollten solche Dateien sofort gelöscht werden.
- Mit einem aktuellen Virenschutzprogramm sollten vor der Installation die Dateien immer überprüft werden.
- Gepackte (komprimierte) Dateien sollten erst entpackt und auf Viren überprüft werden. Installierte Entpackungsprogramme sollten so konfiguriert sein, dass zu entpackende Dateien nicht automatisch gestartet werden.

4 Computersicherheit

4.1 Sichere Konfiguration

4.1.1 Gefahrenquelle Wechselmedien

Wechselmedien, wie etwa Disketten, CD-ROMs, USB-Sticks, etc., ermöglichen raschen und einfachen Transfer von Daten und Programmen, bringen aber auch eine Reihe von Risiken mit sich.

Als derartige Risiken wären unter anderem zu nennen:

- unkontrolliertes Booten, etwa von Diskette, CD-ROM oder USB-Stick,
- unbefugte Installation von Software und
- unberechtigtes Kopieren von Daten auf Wechselmedien (Datendiebstahl, Verlust der Vertraulichkeit, z.B. Kundenbuchhaltung, Kommunikationen mit sensiblem Inhalt).

In vielen Fällen ist eine völlige Sperre der Wechselmedien entweder technisch nicht möglich oder aus betrieblichen Gründen nicht durchsetzbar. Hier sind zusätzliche personelle (Anweisungen, Verbote) und organisatorische Maßnahmen (Kontrollen) erforderlich.

Maßnahmen zur Abwehr von Bedrohungen durch Wechselmedien:

- Verzicht auf Disketten-, CD-ROM-, ... Laufwerke (bzw. ihr nachträglicher Ausbau)
- Verzicht auf die Verwendung von USB-Memory-Sticks
- (Physischer) Verschluss von Laufwerken (z.B. durch Einsatz von Diskettenschlössern)
- (Logische) Sperre von Schnittstellen durch Betriebssystemmechanismen: Viele Betriebssysteme bieten die Möglichkeit, Schnittstellen zu sperren
- Verblenden und Verplomben von Schnittstellen (z.B. durch Abdeckung der Computer-Rückwand oder anderer Anschlussfelder)
- Deaktivieren der Laufwerke oder Schnittstellen im BIOS-Setup (das BIOS-Setup muss danach in jedem Fall durch ein Passwort geschützt werden)

4.1.2 Nutzung der BIOS-Sicherheitsmechanismen

Moderne BIOS-Varianten bieten verschiedene Einstellmöglichkeiten, die sich zur Verbesserung der Computersicherheit nützen lassen:

- **Passwortschutz:**
BIOS-Passwörter können üblicherweise verwendet werden, um das Starten des Rechners oder die Änderung der BIOS-Einstellungen zu kontrollieren. Ersteres bietet; insbesondere bei Entwendung des Rechners (z.B. eines Notebooks) nur geringen Schutz. Die Daten können dennoch von der (ausgebauten) Festplatte ausgelesen oder das Passwort auf einfache Weise zurückgesetzt werden. Die zweite Möglichkeit, das Sperren des Zugangs zum BIOS-Setup, sollte dagegen in jedem Fall aktiviert werden, um andere sicherheitsrelevante Einstellungen zu schützen. Zur Kontrolle, ob die BIOS-Einstellungen zurückgesetzt oder verändert wurden, muss stichprobenartig überprüft werden, ob das BIOS-Passwort noch in Gebrauch ist.
- **Boot-Reihenfolge:**
Die Boot-Reihenfolge sollte so gesetzt werden, dass ausschließlich von der Festplatte gebootet werden kann. Durch diese Maßnahme kann das Einschleppen von Boot-Viren vermieden werden, vor allem aber wird dadurch der Start anderer Betriebssysteme, mit denen lokale, geschützte Daten ausgelesen werden könnten, unterbunden.
- **Virenschutz:**
Wird diese Funktion aktiviert, verlangt der Rechner vor einer Veränderung des Bootsektors bzw. des MBR (Master Boot Record) nach einer Bestätigung.
- **Deaktivieren nicht benötigter Laufwerke und Hardwarefunktionen:**
Nicht benötigte Laufwerke (Disketten-, CD-ROM-Laufwerk) können zur Abwehr von Gefahren durch Wechselmedien deaktiviert werden; bei Bedarf kann sie der Administrator rasch wieder in Betrieb nehmen. Ähnliches gilt für das Deaktivieren von Funktionalitäten,

die im täglichen Einsatz nicht gebraucht werden, z.B. können die USB-Ports und der Parallelport deaktiviert werden, um die Verwendung von USB-Sticks und anderen Wechseldatenträgern zu unterbinden.

4.1.3 Vorsichtiger Gebrauch von Administratorrechten

In vielen komplexen IT-Systemen gibt es eine Administratorrolle, die keinerlei Beschränkungen unterliegt. Durch fehlende Beschränkungen ist die Gefahr von Fehlern oder Missbrauch besonders hoch.

Durch das Verwenden eines Benutzerkontos, das mit Administratorrechten ausgestattet ist, können u.a. folgende Probleme auftreten:

- **Löschen, Überschreiben oder Verändern geschützter Systemdateien:**
Mit uneingeschränkten administrativen Rechten ist es problemlos möglich, Systemdateien zu manipulieren, die mit den Zugriffsrechten eines einfachen Users nicht verändert werden könnten. In weiterer Folge sind Stabilitätsprobleme, Funktionsstörungen oder die vollständige Unbrauchbarkeit des betroffenen Rechners zu erwarten.
- **Löschen, Überschreiben oder Verändern der Daten anderer Benutzer:**
Auch Daten, die durch Zugriffsschutzmechanismen des Betriebssystems vor fremden Zugriffen geschützt sind, können von Benutzern mit administrativen Rechten häufig eingesehen oder verändert werden. Die Gefahr der Vertraulichkeitsverlusts ist sehr hoch, die Rechte eines Administrators sollten daher ausschließlich uneingeschränkt vertrauenswürdigen Mitarbeitern zugewiesen werden.
- **Erhöhtes Risiko durch Viren und andere Schadprogramme:**
Häufig übernehmen Computerviren, die in Folge einer Benutzeraktion wie z.B. der Ausführung eines verseuchten Programms gestartet wurden, die Rechte des auslösenden Benutzers. Ein Virus, der von einem Benutzer mit Administratorrechten gestartet wurde, hat deutlich bessere Möglichkeiten zur Ausübung seiner Schadensfunktionen und zur Ausbreitung im Computersystem.

Um Fehler zu vermeiden, soll unter dem Administrator-Login nur gearbeitet werden, wenn es notwendig ist. Andere Arbeiten darf auch der Administrator nicht unter dieser Kennung erledigen. Für alle Administratoren sollten daher zusätzliche Benutzerkonten eingerichtet werden, die nur über die eingeschränkten Rechte verfügen, die sie zur Aufgabenerfüllung außerhalb der Administration benötigen. Für alle Arbeiten, die nicht der Administration dienen, sollten ausschließlich diese zusätzlichen Benutzerkennungen verwendet werden.

Bekannte Benutzernamen, wie etwa root, guest oder administrator, sollten umbenannt oder nach Bedarf modifiziert werden. Beispielsweise kann der "Administrator"-Account unter MS-Betriebssystemen umbenannt werden und ein neues "Administrator"-Konto mit stark eingeschränkten Rechten eingerichtet werden. Falls danach in den Protokollen Anmeldeversuche mit der Benutzerkennung "Administrator" verzeichnet werden, deutet das auf einen Angriffsversuch hin.

4.1.4 Protokollierung

Um unerlaubte Zugriffe oder Anmeldeversuche von Unbefugten rechtzeitig erkennen und nachverfolgen zu können, müssen geeignete Strategien zur Sicherheitsprotokollierung entwickelt werden.

Die Protokollierung sicherheitsrelevanter Ereignisse wird verwendet, um Sicherheitsverstöße zu erkennen und nachzuverfolgen. Häufig ist sie das einzige Mittel, den Urheber eines bereits erfolgten Sicherheitsverstößes zu erkennen; ohne entsprechende Protokolldaten kann es auch schwer sein, die Tragweite eines solchen Vorfalls zu erkennen.

Die Auswertung der Sicherheitsprotokolle ist oft schwierig. Zur richtigen Interpretation der Einträge ist Übung nötig, die sich nur aus der Praxis ergeben kann, da sie stark von Eigenheiten der protokollierten Systeme und den gesetzten Einstellungen abhängt. Auch aus diesem Grund sollten die Administratoren regelmäßige, zumindest stichprobenartige Auswertungen der Sicherheitsprotokolle vornehmen.

Das eigentliche Ziel regelmäßiger Kontrollen der Protokolleinträge ist das rechtzeitige, proaktive Aufspüren von Sicherheitsverstößen. In den Protokollen lassen sich mit einiger Übung verschiedene kritische Vorgänge und Manipulationsversuche erkennen und unterbinden.

Geeignete Auswertungskriterien sind beispielsweise folgende Fragen:

- Häufen sich fehlerhafte Anmeldeversuche (Hinweis auf den Versuch, Passwörter zu erraten)?
- Liegen auffällige An- und Abmeldezeitpunkte außerhalb der Arbeitszeit (Hinweis auf Manipulationsversuche)?
- Häufen sich unzulässige Zugriffsversuche (Hinweis auf Versuche zur Manipulation)?

Die Protokolleinstellungen sind so zu setzen, dass alle für die Auswertung nötigen Ereignisse protokolliert werden, der Umfang der Protokolldateien aber nicht überhandnimmt. Ein geeignetes Gleichgewicht zu finden, kann schwierig sein. Bei Rechnern mit Windows-Betriebssystemen (NT, 2000, XP, 2003) sollten zumindest folgende Ereignisse in jedem Fall, auf Servern und Client-Rechnern, geloggt werden:

- Erfolgreiche und fehlgeschlagene Anmeldeversuche
- Erfolgreiche und fehlgeschlagene Anmeldeereignisse
- Erfolgreiche und fehlgeschlagene Änderungen in der Kontenverwaltung
- Fehlgeschlagene Verwendung von Benutzerrechten

Diese Einstellungen können, abhängig von Betriebssystem und Rechnertyp (Client, Server), mit Hilfe der "Überwachungsrichtlinien", der "Lokalen Sicherheitsrichtlinie" bzw. der Gruppenrichtlinien vorgenommen werden. Die maximale Protokollgröße des Sicherheitsprotokolls sollte deutlich angehoben werden, um auch länger zurückliegende Ereignisse untersuchen zu können.

Bei Rechnern mit Unix- oder Linux-Betriebssystemen sind folgende Vorgänge vorrangig zu protokollieren:

- Erfolgreiche und fehlgeschlagene Logins
- Aufruf von "su"
- Als "root" ausgeführte Befehle

Falls personenbezogene Daten, die den Bestimmungen des Datenschutzgesetzes unterliegen, verarbeitet werden, muss außerdem der Zugriff auf diese Daten protokolliert werden. In welcher Form diese Protokollierung erfolgen soll, hängt von den eingesetzten Anwendungen ab. Der Aufwand für die Protokollierung sollte den Schutzbedarf der Daten nicht übersteigen, **"Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen"** sollten aber **"im Hinblick auf ihre Zulässigkeit in notwendigem Ausmaß nachvollzogen werden können."** Solche Protokolle sind, wenn nicht gesetzlich ausdrücklich anders angeordnet, drei Jahre lang aufzubewahren.

4.2 Sicherheit und Software

4.2.1 Einsatz eines Verschlüsselungsproduktes für Arbeitsplatzsysteme

Sind auf einem Arbeitsplatzsystem besonders schutzwürdige Daten gespeichert und wird dieses System in einer nicht oder nur unzureichend geschützten Umgebung betrieben oder aufbewahrt, so ist der Einsatz eines Verschlüsselungsproduktes zu erwägen.

Besonders bei Notebooks und anderen mobilen Geräten sind aufgrund der erhöhten Diebstahls- und Verlustgefahr Datenverschlüsselungsmaßnahmen ratsam. Sensible Firmendaten oder E-Mails sollten darauf ausschließlich in verschlüsselter Form abgelegt werden.

Mit Hilfe der marktgängigen Produkte ist es möglich, die betreffenden Daten so zu verschlüsseln, dass nur derjenige, der über den geheimen Schlüssel verfügt, in der Lage ist, die Daten zu lesen und zu gebrauchen.

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.

4.2.2 Update von Software

Durch Software-Updates können Schwachstellen beseitigt oder Funktionen erweitert werden.

Ein Update ist erforderlich, wenn Schwachstellen bekannt werden, die Auswirkungen auf den sicheren Betrieb des Systems haben, wenn Fehlfunktionen wiederholt auftauchen oder eine Funktionserweiterung aus sicherheitstechnischen oder fachlichen Erfordernissen notwendig wird. Vor einem Update ist die Zuverlässigkeit der neuen Komponenten und ihr Zusammenwirken mit bestehenden Programmen zu prüfen. Im Idealfall geschieht das auf einem eigenen Testsystem, alternativ dazu kann das Update auch auf einem einzelnen Rechner getestet werden, bevor es in den produktiven Einsatz übernommen wird.

Updates und sicherheitsrelevante Patches, die bekannte Fehler und Sicherheitslücken in Programmen beheben, werden in der Regel durch den Hersteller bei Bedarf zur Verfügung gestellt. Es ist dabei zu beachten, dass derartige Updates und Patches unbedingt nur aus vertrauenswürdigen Quellen bezogen werden dürfen. Die Authentizität der Quelle ist nach Möglichkeit zu prüfen (beispielsweise anhand vorhandener Server-Zertifikate beim Download aus dem Internet).

4.2.3 Nutzungsverbot nicht-betrieblicher Software

Um sicherzustellen, dass keine Programme mit unerwünschten Auswirkungen eingebracht werden und das System nicht über den festgelegten Funktionsumfang hinaus unkontrolliert genutzt wird, muss das Einspielen von Software in Produktionssysteme bzw. ihre Nutzung verboten und - soweit technisch möglich - verhindert werden.

Im Allgemeinen sollte auch die Nutzung privater Software (Daten, Programme) und Hardware (CD/DVD/Disketten, Wechselfestplatten, Notebooks, USB-Memory-Sticks etc.) untersagt werden. Der Einsatz nicht betriebsnotwendiger Hard- und Software birgt neben dem "Einschleusen" von Schadprogrammen auch die Gefahr der Systeminstabilität mit sich.

- Eine Liste von Programmen sollte erstellt werden, deren Nutzung explizit untersagt ist. Beispiele dafür sind z.B. Instant Messaging-Clients (ICQ), Filesharing-Software (Kazaa, BitTorrent), Spiele oder Hacker-Tools.
- Das unautorisierte Einspielen und/oder Nutzen von Software ist - soweit möglich - mit technischen Mitteln zu verhindern.
- Das Nutzungsverbot nicht-betrieblicher Software sollte schriftlich fixiert und allen Mitarbeitern mitgeteilt werden.

4.2.4 Sicherheitsfunktionen in Anwendungsprogrammen

Standardprodukte im PC-Bereich bieten oft eine Reihe von nützlichen IT-Sicherheitsfunktionen, deren Qualität im Einzelnen unterschiedlich sein kann, die aber Unbefugte behindern bzw. mögliche Schäden verringern können.

Die Verwendung der folgenden Funktionen wird, abhängig von der Wichtigkeit oder Vertraulichkeit der verarbeiteten Daten, empfohlen:

- Passwortschutz beim Programmstart
- Automatische Zwischenspeicherung
- Zugriffsschutz zu einzelnen Dateien
- Verschlüsselung von Dateien

In vielen Programmen reichen die Sicherheitsfunktionen allerdings nur zur Abwehr einfacher Angriffe aus, beispielsweise kann der Dokumentschutz in Microsoft Office-Anwendungen mit spezieller Software in wenigen Minuten durchbrochen werden. Für sensible Daten sollten daher spezialisierte Verschlüsselungsprogramme eingesetzt werden. Grundsätzlich sollte immer die

Qualität der oben angeführten Schutzfunktionen recherchiert werden, bevor man sie zum Schutz wichtiger Daten nützt.

4.2.5 Überprüfen von Dateien vor deren Weitergabe

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. Die häufigsten Ursachen für solche Restinformationen sind im Folgenden beschrieben.

Vor der Weitergabe von Dateien sollten diese zumindest stichprobenartig auf unerwünschte Zusatzinformationen überprüft werden. Dazu sollte ein anderes Programm benutzt werden als das, mit dem die Datei erstellt wurde. Oft ist ein einfacher Texteditor ausreichend.

Um eventuell vorhandene Restinformationen zu beseitigen, kann die Datei in einem anderen Dateiformat abgespeichert werden, z.B. als "Nur-Text" oder als HTML. Eine weitere Möglichkeit besteht darin, die Daten in eine vollständig neue Datei zu kopieren.

- **Verborgener Text / Kommentare**
Eine Datei kann Textpassagen enthalten, die als "versteckt" oder "verborgen" formatiert sind, beispielsweise ausgeblendete Kommentare. Solche Textpassagen können Bemerkungen enthalten, die nicht für den Empfänger bestimmt sind; sie müssen vor der Herausgabe zuverlässig gelöscht werden.
- **Änderungsmarkierungen**
Bei der Bearbeitung von Dateien werden manchmal Änderungsmarkierungen verwendet. Da diese auf dem Ausdruck und am Bildschirm ausgeblendet werden können, muss vor der Weitergabe überprüft werden, ob solche Änderungsmarkierungen vorhanden sind.
- **Versionsführung**
Bei einer Vielzahl von Anwendungen gibt es die Möglichkeit, verschiedene Versionen eines Dokumentes in einer Datei zu speichern, um bei Bedarf auf frühere Überarbeitungsstände zurückgreifen zu können. Dies kann sehr schnell zu riesigen Dateien führen, diese Option ist daher nur bei tatsächlichem Bedarf zu wählen.
- **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 müssen manuell eingegeben werden. Vor der Weitergabe einer Datei an Externe ist zu überprüfen, welche zusätzlichen Informationen die Datei enthält.
- **Schnellspeicherung**
Textverarbeitungsprogramme nutzen die Option der Schnellspeicherung, um nur Veränderungen seit der letzten Sicherung und nicht das gesamte Dokument zu speichern, sodass das Speichern beschleunigt wird. Der entscheidende Nachteil ist jedoch, dass die Datei Textfragmente enthalten kann, die durch die Überarbeitung hätten beseitigt werden sollen. Grundsätzlich sollten Schnellspeicherungsoptionen daher abgeschaltet werden.

4.2.6 Datenformate

Durch die Vielzahl von Anwendungsprogrammen ist auch eine Vielzahl von Datenformaten in Verwendung. Bei gleichartigen Anwendungen verschiedener Hersteller, aber auch bei verschiedenen Versionen eines Programms können die gebräuchlichen Datenformate variieren. Besonders für den Zugriff auf ältere Unternehmensdaten, wie sie z.B. auf Datensicherungen vorliegen, ist darauf zu achten, dass diese Daten auch mit der neu angeschafften Software geöffnet werden können. Falls das nicht möglich sein sollte, muss eine Version der alten Anwendungssoftware zurückbehalten werden, um zu verhindern, dass ältere Datenbestände unlesbar werden. Unter Umständen ist auch das Abspeichern der alten Daten in einem anderen,

aktuellen Dateiformat zu überlegen.

5 Personelle Maßnahmen

IT-Sicherheit kann auch bei besten technischen Maßnahmen nur funktionieren, wenn die Mitarbeiter ausgeprägtes Sicherheitsbewusstsein besitzen und bereit und fähig sind, die Vorgaben in der täglichen Praxis umzusetzen. Andererseits stellen Mitarbeiter auch potenzielle Angriffs- oder Fehlerquellen dar. Aus diesen Gründen sind Schulung und Sensibilisierung für Fragen der IT-Sicherheit unbedingt notwendig.

5.1 Regelungen für Mitarbeiter

Bei der Einstellung von Mitarbeitern sind diese zur Einhaltung einschlägiger Gesetze (z.B. das Datenschutzgesetz), Vorschriften und interner Regelungen zu verpflichten.

Insbesondere empfiehlt es sich Regelungen zu folgenden Bereichen zu treffen, die dann auch in eine entsprechende Verpflichtungserklärung aufzunehmen sind:

- Einhaltung von PC-Benutzungsregeln
- Einhaltung der Regeln für die Benutzung des Internet
- Clear Desk Policy (falls vorgesehen)

Bei der Erstellung von Stellenbeschreibungen müssen auch alle sicherheitsrelevanten Aufgaben und Verantwortlichkeiten explizit in diese Beschreibungen aufgenommen werden. Dies gilt in besonderem Maße für Mitarbeiter mit speziellen Sicherheitsaufgaben (z.B. Datenschutzbeauftragte, IT-Sicherheitsbeauftragte, Applikations-/Projektverantwortliche). 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 und wissen nicht, welche IT-Sicherheitsmaßnahmen einzuhalten sind.

Es ist sinnvoll die Vorschriften und Regelungen auszuhändigen und gegenzeichnen zu lassen bzw. für die Mitarbeiter an zentraler Stelle zur Einsichtnahme aufzubewahren.

Administrator - eine Vertrauensposition

Administratoren von IT-Systemen und ihren Vertretern muss besonders großes Vertrauen entgegengebracht werden. Sie haben - in Abhängigkeit vom eingesetzten System - weitgehende und oftmals allumfassende Befugnisse. Sie sind in der Lage, auf alle gespeicherten Daten zuzugreifen, sie ggf. zu verändern und Berechtigungen so zu vergeben, dass erheblicher Missbrauch möglich wäre. Das hierfür eingesetzte Personal muss sorgfältig ausgewählt werden und absolut vertrauenswürdig sein.

5.1.1 Clear Desk-Policy

Bei Abwesenheit sollte jeder Mitarbeiter seine (vertraulichen) Unterlagen verschließen. Dies gilt insbesondere für Großraumbüros, aber auch in den anderen Fällen ist dafür Sorge zu tragen, dass keine unberechtigten Personen (Besucher, Reinigungspersonal, unbefugte Mitarbeiter etc.) Zugriff zu Schriftstücken oder Datenträgern mit sensiblen Inhalten haben.

5.1.2 Verpflichtung der PC-Benutzer zum Abmelden

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 Zugriffskontrolle nur dann erreicht werden, wenn jeder Benutzer sich nach Aufgabenerfüllung bzw. bei Verlassen des Arbeitsplatzes am PC abmeldet. Ist absehbar, dass nur eine kurze Unterbrechung der Arbeit erforderlich ist, kann an Stelle des Abmeldens auch eine manuelle oder nach einer gewissen Zeit automatische Aktivierung der Bildschirmsperre (z.B. passwortgeschützter Bildschirmschoner) erfolgen.

5.1.3 Verfahrensweise beim Ausscheiden von Mitarbeitern

Beim Ausscheiden von Mitarbeitern aus dem Unternehmen sollten folgende grundlegende Punkte beachtet werden:

- Sämtliche Unterlagen, ausgehändigte Schlüssel, ausgeliehene IT-Geräte (z.B. tragbare Rechner, Speichermedien, Dokumentationen) sind zurückzufordern.
- Es sind sämtliche 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. Nach Möglichkeit sollte eine Neuvergabe der Benutzerkennung an einen anderen Mitarbeiter vermieden bzw. ausgeschlossen werden.
- Nach Möglichkeit sollte eine Neuvergabe der Benutzerkennung an einen anderen Mitarbeiter vermieden bzw. ausgeschlossen werden.
- Ausgeschiedenen Mitarbeitern ist der unkontrollierte Zutritt zum Firmengelände, insbesondere zu Räumen mit IT-Systemen zu verwehren.
- Als ein praktikables Hilfsmittel haben sich Checklisten erwiesen, auf denen die einzelnen Aktivitäten des Ausscheidenden vorgezeichnet sind, die er vor Verlassen des Unternehmens zu erledigen hat.

Bei Versetzung eines Mitarbeiters oder einer wesentlichen Änderung seiner Tätigkeit sind seine Zugangsberechtigungen sowie Zugriffsrechte auf Übereinstimmung mit den neuen Anforderungen zu überprüfen und gegebenenfalls anzupassen.

5.1.4 Vertretungsregelungen

Besonders im Bereich der Informationsverarbeitung sind Vertretungsregeln von Bedeutung, da dafür meist Spezialwissen sowie eine zeitgerechte Einarbeitung unkundiger Mitarbeiter für den Vertretungsfall unbedingt erforderlich sind.

Für die Vertretungsregelungen sind folgende Randbedingungen einzuhalten:

- Der Verfahrens- oder Projektstand muss hinreichend dokumentiert sein.
- Der Vertreter muss so geschult werden, dass er die Aufgaben jederzeit übernehmen kann.
- 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.

5.1.5 Kontrolle der Einhaltung der organisatorischen Vorgaben

Mittels Protokollauswertung oder durch Stichproben sollte regelmäßig überprüft werden, ob die Benutzer eines IT-Systems die organisatorischen Vorgaben (z.B. Verpflichtung zur Abmeldung nach Aufgabenerfüllung oder Verbot der Weitergabe von Passwörtern) auch tatsächlich einhalten.

Für die Akzeptanz von Kontrollen ist es wichtig, dass allen Beteiligten das Ziel der Kontrollen erkennbar ist und dass dabei keine Personen bloßgestellt werden oder ungerechtfertigte Konsequenzen drohen. Wenn die Mitarbeiter dies befürchten müssen, besteht die Gefahr, dass sie nicht offen über ihnen bekannte Schwachstellen und Sicherheitslücken berichten, sondern versuchen, bestehende Probleme zu vertuschen.

5.1.6 Regelungen für den Einsatz von Fremdpersonal

Kurzfristig oder einmalig zum Einsatz kommendes Fremdpersonal ist wie Besucher zu behandeln, d.h. dass etwa der Aufenthalt in sicherheitsrelevanten Bereichen nur in Begleitung von Mitarbeitern des Unternehmens erlaubt ist.

Ist es nicht möglich, betriebsfremde Personen (z.B. Reinigungspersonal) ständig zu begleiten oder

zu beaufsichtigen, sollte zumindest der persönliche Arbeitsbereich abgeschlossen werden (Schreibtisch, Schrank, Abmeldung/Sperre am PC).

Sollten betriebliche Unterlagen temporär oder permanent im Wohnbereich gelagert werden (Telearbeitsplatz, Aufbewahrung von Datensicherungen usw.) so ist darauf zu achten, dass betriebsfremde Personen nicht ungehindert auf diese Unterlagen oder den Telearbeitsplatz zugreifen können.

Externe Mitarbeiter, die über einen längeren Zeitraum in einem Unternehmen tätig sind und evtl. Zugang zu vertraulichen Unterlagen und Daten bekommen könnten, sind ebenfalls schriftlich (im Rahmen von Geheimhaltungsverpflichtungen) auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen zu verpflichten. Sie müssen, soweit es zur Erfüllung ihrer Aufgaben und Verpflichtungen erforderlich ist, über hausinterne Regelungen unterrichtet werden.

5.2 Sicherheitssensibilisierung und -schulung

5.2.1 Schulung und Sensibilisierung zu IT-Sicherheitsmaßnahmen

Umfassende IT-Sicherheit kann nur dann gewährleistet werden, wenn alle beteiligten und betroffenen Personen über angemessene Kenntnisse zum sachgemäßen Umgang mit IT-Systemen und insbesondere zu den Gefahren und Gegenmaßnahmen in ihrem eigenen Arbeitsgebiet verfügen. Es liegt in der Verantwortung der Geschäftsführung, durch geeignete Schulungsmaßnahmen hierfür die nötigen Voraussetzungen zu schaffen. Darüber hinaus sollte jeder Benutzer dazu motiviert werden, sich auch in Eigeninitiative Kenntnisse anzueignen.

Die überwiegende Zahl von Schäden im IT-Bereich entsteht durch Nachlässigkeit. Das Aufzeigen der Abhängigkeit des Unternehmens und damit der Arbeitsplätze vom reibungslosen Funktionieren der IT-Systeme ist ein geeigneter Einstieg in die Sensibilisierung.

Weitere mögliche Inhalte dieser Schulung sind:

- Der richtige Umgang mit Passwörtern
- Richtiges Verhalten beim Auftreten von Sicherheitsproblemen
- Der Umgang mit personenbezogenen Daten:
An den Umgang mit personenbezogenen Daten sind besondere Anforderungen zu stellen. Mitarbeiter, die mit personenbezogenen Daten (sowohl in IT-Systemen als auch in schriftlichen Unterlagen) arbeiten müssen, sind für die gesetzlich erforderlichen Sicherheitsmaßnahmen zu schulen.
- Wirkungsweise und Arten von Schadprogrammen
- Erkennen eines Befalls mit Schadprogrammen
- Sofortmaßnahmen im Verdachtsfall und Maßnahmen zur Eliminierung von Schadprogrammen
- Das richtige Verhalten im Internet (Umgang mit WWW-Browsern)
- Risiken bei mobilen Datenträgern
- Die Bedeutung der Datensicherung und deren Durchführung
- Der geregelte Ablauf eines Datenträgeraustausches:
Die Festlegung, wann welchen Kommunikationspartnern welche Datenträger übermittelt werden dürfen, ist allen Beteiligten bekannt zu geben. Werden bestimmte IT-gestützte Verfahren zum Schutz der Daten während des Austausches eingesetzt (wie etwa Verschlüsselung, digitale Signaturen oder Checksummenverfahren), so sind die Mitarbeiter in die Handhabung dieser Verfahren ausreichend einzuarbeiten.
- 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.

Es sollte versucht werden, Schulungsthemen zur IT-Sicherheit soweit möglich in andere Schulungskonzepte, etwa in die Anwenderschulung, zu integrieren. Diese Einbindung hat den Vorteil, dass Sicherheit unmittelbar als Bestandteil des IT-Einsatzes wahrgenommen wird.

5.2.2 Geregelt 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.

Die Einarbeitung bzw. Einweisung sollte zumindest folgende Punkte umfassen:

- Vorstellung aller Ansprechpartner, insbesondere zu IT-Sicherheitsfragen,
- Erläuterung der interner Regelungen und Vorschriften zur IT-Sicherheit.

5.2.3 Betreuung und Beratung von IT-Benutzern

Neben der Schulung, die die IT-Benutzer in die Lage versetzt, die vorhandene Informationstechnik sachgerecht einzusetzen, bedarf es einer Betreuung und Beratung der IT-Benutzer für die im laufenden Betrieb auftretenden Probleme. Diese Probleme können aus Hardwaredefekten, fehlerhaften Softwareinstallationen, aber auch aus Bedienungsfehlern resultieren.

In größeren Unternehmen kann es daher sinnvoll sein, eine zentrale Stelle mit der Betreuung der IT-Benutzer zu beauftragen und diese allen Mitarbeitern bekannt zu geben ("Helpdesk"). Dabei hat sich die Wahl einer besonders leicht zu merkenden Telefonnummer besonders bewährt.

5.2.4 Auswahl von Passwörtern

Passwörter haben grundlegende Bedeutung beim Schutz der IT-Systeme und Daten. Die richtige Auswahl und der richtige Umgang mit Passwörtern können über die Sicherheit vor unbefugten Zugriffen und Manipulationen entscheiden.

Passwörter müssen ausreichend komplex sein, um nicht erraten werden zu können. Andererseits dürfen sie auch nicht so kompliziert sein, dass sie vergessen werden oder schriftlich notiert werden müssen. Dieser Kompromiss ist letztlich vom jeweiligen Benutzer abhängig, einige Grundregeln sollten dabei aber unbedingt beachtet werden:

- Namen, Vornamen, Geburtsdaten, tel. Durchwahlen, KFZ-Kennzeichen etc. dürfen nicht verwendet werden. Sie sind leicht ausfindig zu machen und werden bei Versuchen, ein Passwort zu erraten, mit Sicherheit getestet.
- Passwörter sollten nicht aus Begriffen bestehen, die in einem Wörterbuch (auch einer anderen Sprache) aufzufinden sein könnten. Programme, die zum Ausfindigmachen von Passwörtern verwendet werden, nützen Wortlisten mit mehreren tausend Begriffen, um Passwörter dieser Art innerhalb kürzester Zeit zu entschlüsseln. Auch Eigennamen, geografische Begriffe etc. sollten möglichst vermieden werden.
- Trivialpasswörter (aaaaaa, qwertz, asdf, 123456, 08/15, 4711 etc.) dürfen nicht verwendet werden. Abgesehen davon, dass auch solche Passwörter in Wortlisten vorkommen können, sind sie meistens schon beim Beobachten der Passworteingabe zu erkennen.
- Das Passwort muss ausreichend lang sein. Für normale Benutzer sollte es mindestens sechs Zeichen lang sein, für Benutzerkonten mit besonderen Rechten (administrator, root, Dienstkonten etc.) sollte es entsprechend länger gewählt werden.
- Ein Passwort sollte aus verschiedenen Arten von Zeichen zusammengesetzt sein. Im Idealfall besteht es aus Großbuchstaben, Kleinbuchstaben, Ziffern und/oder Sonderzeichen (Satzzeichen, Währungssymbole etc.).
- Passwörter - insbesondere das Passwort bei der Anmeldung am Computer - dürfen nicht an andere Personen weitergegeben werden. Auch anderen Mitarbeitern dürfen Passwörter

nur in absoluten Notfällen mitgeteilt werden; anschließend sollten sie sofort geändert werden.

Eine bewährte Methode, sichere und dennoch gut merkbare Passwörter zu erstellen, ist deren Bildung aus den Wortanfängen und Satzzeichen einfacher Merksätze. Aus einem Satz wie "Heute beschloss ich, mein Passwort zu ändern" lässt sich "Hbi,mPzä" bilden, ein Passwort, das alle oben angeführten Anforderungen problemlos erfüllt.

Passwörter sollten in regelmäßigen Abständen geändert werden (z.B. alle 90 Tage). Sie sollten aber auch immer dann geändert werden, wenn der Verdacht besteht, dass sie von einem Unbefugten ausfindig gemacht wurden. Jeder Mitarbeiter sollte wissen, auf welche Weise er sein Passwort ändern kann.

Nach Möglichkeit sollten für verschiedene Anmeldungen auch verschiedene Passwörter gebraucht werden. Auf keinen Fall darf z.B. für die Anmeldung am PC und das E-Mail-Konto beim Internet-Provider das gleiche Passwort verwendet werden. In einfachen Fällen kann es ausreichen, kleine Variationen einzufügen.

Administratoren sollten in Zusammenhang mit Passwörtern folgende Regeln beachten:

- Sämtliche Benutzerkonten sind mit einem Passwort zu versehen. Es ist unbedingt zu vermeiden, dass sich im System Konten befinden, die ohne Eingabe eines Passworts nutzbar sind (z.B. "Gast"-Konten, aber auch lokale Administratorkonten, für die kein Passwort festgelegt wurde).
- Default-Passwörter, die vom Hersteller bei der Auslieferung der Systeme festgelegt wurden, müssen durch eigene Passwörter ersetzt werden.
- Nach dreimaliger Fehleingabe des Passworts sollte automatisch das betreffende Benutzerkonto gesperrt werden. Sofern eine automatische Aufhebung dieser Sperre möglich ist, sollte diese erst nach mehreren Stunden erfolgen; im Allgemeinen sollte aber der Systemadministrator die Sperre aufheben.
- Aufgrund falscher Passwortheingaben gesperrte Benutzerkonten können ein Indiz für versuchtes Passwortraten sein. Die Ursache der Fehleingaben muss in jedem Fall ausfindig gemacht werden.
- Der Passwortwechsel sollte vom IT-System in regelmäßigen Abständen (z.B. 90 Tage) initiiert werden.

Die neuerliche Verwendung alter Passwörter beim Passwortwechsel sollte auf technischem Weg ("Passworthistorie") unterbunden werden.

5.2.5 Aktionen bei Auftreten von Sicherheitsproblemen (Incident Handling Pläne)

Die Aufgaben und Verantwortlichkeiten aller Mitarbeiter bei Auftreten von sicherheitsrelevanten Ereignissen sollten im Rahmen spezieller "Incident Handling Pläne" (IHPs) sowohl für einzelne Bereiche als auch für das gesamte Unternehmen festgelegt werden.

Unter sicherheitsrelevanten Ereignissen sind dabei zu verstehen:

- Angriffe und (vermutete) Angriffsversuche gegen ein IT-System
- (vermutete) Sicherheitsschwächen
- Funktionsstörungen von Systemen (etwa durch Schadprogramme)

Incident Handling Pläne sollen in schriftlicher Form verbindlich festlegen:

- wie auf sicherheitsrelevante Ereignisse zu reagieren ist,
- die Verantwortlichkeiten für die Meldung bzw. Untersuchung sicherheitsrelevanter Vorfälle,
- die einzuhaltenden Meldewege,
- die Protokollierung und Dokumentation sicherheitsrelevanter Vorfälle sowie
- die Ausbildung von Personen, die sicherheitsrelevante Vorfälle behandeln bzw.

Gegenmaßnahmen treffen müssen.

IHPs sind allen betroffenen Mitarbeitern bekannt zu machen.

5.2.6 Nutzung und Aufbewahrung mobiler IT-Geräte

Unter mobilen IT-Geräten sind alle für einen mobilen Einsatz geeigneten Geräte zu verstehen, so etwa Notebooks, Handhelds, Personal Digital Assistants (PDA) und Smartphones.

Beim Außer-Haus-Einsatz von mobilen IT-Geräten ist besonders auf die sichere Verwahrung von Daten zu achten. Die Mitarbeiter sollten speziell auf potenzielle Gefahren hin geschult und sensibilisiert werden:

- Bei Speicherung firmeninterner, vertraulicher bzw. personenbezogener sensibler Daten nach DSGVO ist die Installation eines Zugriffsschutzes (über Passwort oder Chipkarte) unbedingt vorzusehen sowie eine Festplatten- oder Dateiverschlüsselung dringend zu empfehlen.
- Auch mobile Datenträger sollten ausschließlich verschlüsselte Daten enthalten; unverschlüsselte Datenträger sollten keinesfalls unbeaufsichtigt (etwa im Hotel oder in einem Wagen) zurückgelassen werden.
- Ist dies nicht zu verhindern, sollte diese Zeitspanne unbedingt minimiert werden.
- Bei Nutzung in fremden Büroräumen vor Ort ist dieser Raum nach Möglichkeit auch bei kurzzeitigem Verlassen zu verschließen. Wird der Raum für längere Zeit verlassen, sollte zusätzlich das Gerät ausgeschaltet werden. Das Verwenden von Bootpasswörtern kann dann die unerlaubte Nutzung verhindern.

5.3 Telearbeit

Unter Telearbeit versteht man im Allgemeinen Tätigkeiten, die räumlich entfernt vom Standort des Arbeitgebers durchgeführt werden und deren Erledigung durch eine kommunikationstechnische Anbindung an die IT des Arbeitgebers unterstützt wird.

5.3.1 Geeignete Einrichtung eines häuslichen Arbeitsplatzes

Der häusliche Arbeitsplatz sollte von der übrigen Wohnung zumindest durch eine Tür abgetrennt sein und im Idealfall ausschließlich der beruflichen Tätigkeit dienen.

Aus dem Aspekt der Sicherheit entstehen folgende zusätzliche Anforderungen:

- Bereitstellung versperrbarer Behältnisse zur Aufbewahrung von Datenträgern und Dokumenten
- Überspannungsschutz

Sofern die IT nicht auch für private Zwecke benutzt werden soll, sollte sie vom Arbeitgeber bereitgestellt werden und ihre private Nutzung durch eine schriftliche Vereinbarung untersagt werden.

Arbeitsmittel:

Es kann festgeschrieben werden, welche Arbeitsmittel der Telearbeiter einsetzen kann und welche nicht genutzt werden dürfen (z.B. nicht freigegebene Software). So kann ein Internet-Anschluss für die E-Mail-Kommunikation zur Verfügung gestellt werden, aber die Nutzung von anderen Internet-Diensten wird untersagt. Weiters kann die Benutzung von mobilen Datenträgern (Gefahr von Viren) untersagt werden, wenn der Telearbeitsrechner dies nicht erfordert.

Datensicherung:

Der Telearbeiter ist zu verpflichten, regelmäßig eine Datensicherung durchzuführen. Darüber hinaus sollte vereinbart werden, dass jeweils eine Generation der Datensicherung im Unternehmen zur Unterstützung der Verfügbarkeit hinterlegt wird.

IT-Sicherheitsmaßnahmen:

Der Telearbeiter ist zu verpflichten, die für die Telearbeit notwendigen IT-Sicherheitsmaßnahmen zu beachten und zu realisieren. Die umzusetzenden IT-Sicherheitsmaßnahmen sind dem Telearbeiter in schriftlicher Form zu übergeben.

Datenschutz:

Der Telearbeiter ist auf die Einhaltung einschlägiger Datenschutzvorschriften zu verpflichten sowie auf die notwendigen Maßnahmen bei der Bearbeitung von personenbezogenen Daten am häuslichen Arbeitsplatz hinzuweisen.

6 Bauliche und infrastrukturelle Maßnahmen

Die in diesem Abschnitt beschriebenen Maßnahmen dienen dem Schutz von IT-Systemen mittels baulichen und infrastrukturellen Vorkehrungen. Dabei sind verschiedene Schutzebenen zu betrachten, wie etwa Serverräume, Datenträgerarchive, Räume für technische Infrastruktur etc.

6.1 Bauliche und organisatorische Maßnahmen

6.1.1 Schützenswerte Gebäudeteile und Einbruchsschutz

Besonders schützenswerte Räume oder Gebäudeteile sollten nicht in exponierten oder gefährdeten Bereichen untergebracht sein.

Insbesondere ist zu beachten:

- Kellerräume sind durch Wasser gefährdet.
- Räume im Erdgeschoß - zu öffentlichen Verkehrsflächen hin - sind durch 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.

Die nachfolgenden Fragen können bei der Beurteilung der baulichen und infrastrukturellen Sicherheit hilfreich sein:

- Lage des Gebäudes (Befindet es sich auf einem eigenen gesicherten Grundstück? Wie sind die benachbarten öffentlichen Verkehrsflächen beschaffen?)
- Steht das Gebäude der betreffenden Organisation zur Alleinbenützung zur Verfügung oder gibt es andere Mitbenutzer? Wenn ja, welche?
- Wer hat Zutritt zum Gebäude?
- Gibt es eine physische Zutrittskontrolle? Ist ein Portierdienst/Empfang eingerichtet?
- Stärke und Schutz/Überwachung von Wänden, Türen, Fenstern, Lüftungsschächten etc.
- Infrastruktur (Wasser-, Stromversorgung, Kommunikationsverbindungen, Klimaanlage, USV etc.)
- Welche Bereiche des Grundstückes bzw. des Gebäudes sind sicherheitsrelevant?

Weiters ist zu beachten, dass Bedingungen bzw. Auflagen von etwaigen Versicherungen eingehalten werden.

Die gängigen Maßnahmen zum Einbruchsschutz sollten den örtlichen Gegebenheiten entsprechend angepasst werden.

Dazu gehören:

- Sicherungen bei einstiegsgefährdeten Türen oder Fenstern,
- besondere Schließzylinder, Zusatzschlösser und Riegel,
- Sicherung von Kellerlichtschächten,
- Verschluss von nicht benutzten Nebeneingängen,
- einbruchgesicherte Notausgänge,

- Verschluss von Personen- und Lastenaufzügen außerhalb der Dienstzeit.

Den Mitarbeitern sind Regelungen bekannt zu geben, welche Maßnahmen zum Einbruchschutz beachtet werden müssen.

6.1.2 Zutrittskontrolle und Empfang

Die Überwachung des Zutritts zu Gebäuden, Rechenzentren und sicherheitssensiblen Geräten zählt zu den wichtigsten physischen Schutzmaßnahmen. Ein Zutrittskontrollsystem vereinigt verschiedene bauliche, organisatorische und personelle Maßnahmen.

Das Zutrittskontrollkonzept legt u.a. fest:

- Welche Bereiche sind besonders schützenswert (z.B. Serverräume, Räume mit Peripheriegeräten, Archive, Kommunikationseinrichtungen und die Haustechnik)? Die einzelnen Bereiche können unterschiedliche Sicherheitsstufen aufweisen.
- Welche internen und externen Personengruppen haben Zutritt zu welchen Bereichen?
- Welche Daten müssen bei Zutritt und Verlassen eines geschützten Bereichs protokolliert werden?
- Bestimmung eines Verantwortlichen für die Zutrittskontrolle, der Zutrittsberechtigungen an die einzelnen Personen entsprechend festgelegter Grundsätze vergibt.
- Dokumentation der Vergabe und Rücknahme von Zutrittsberechtigungen
- Festlegung der Zutrittskontrollmedien: Identifikation/Authentisierung durch Überwachungspersonal (persönlich oder mittels Überwachungskameras) oder durch automatische Identifikations- und Authentisierungssysteme wie Zugangscodes (Passwörter, PINs), Karten oder biometrische Verfahren

Die Einrichtung eines Empfangsdienstes (Portier, Front-Sekretariat etc.) hat weitreichende positive Auswirkungen gegen eine ganze Reihe von Gefährdungen.

Voraussetzung ist allerdings, dass bei der Umsetzung des Empfangsdienstes einige Grundprinzipien beachtet werden, die auch für scheinbar vertrauenswürdige Personen, wie z.B. ehemalige Mitarbeiter, Gültigkeit haben.

- Mitarbeiter am Empfang beobachten bzw. kontrollieren den Eingang zum Gebäude/Büro bzw. zum sicherheitsrelevanten Bereich.
- Unbekannte Personen haben sich beim Empfang zu legitimieren.
- Die Empfangsmitarbeiter halten vor Einlassgewährung eines Besuchers bei dem Besuchten Rückfrage.
- Der Besucher wird zum Besuchten begleitet oder am Eingang abgeholt.

6.1.3 Schließplan

Die Herstellung, Aufbewahrung, Verwaltung und Ausgabe von Schlüsseln ist zentral zu regeln. Reserveschlüssel sind gesichert aufzubewahren. Alle Maßnahmen und Informationen sollten in einem Schließplan dokumentiert werden.

Zu beachten ist u.a.:

- Ist eine Schließanlage vorhanden, so 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 und Schlüssel gegebenenfalls einzuziehen.

Das Gleiche gilt sinngemäß auch für alle anderen Zutrittskontrollmedien wie Magnetstreifen oder Chipkarten bzw. sogenannte Multifunktionschipkarten.

6.2 Geeignete Aufstellung und Aufbewahrung

Bei der Aufstellung eines IT-Systems sind verschiedene Voraussetzungen zu beachten, die die Sicherheit des Systems gewährleisten bzw. erhöhen sollen. Über diese Sicherheitsaspekte hinaus sollen durch eine geeignete Aufstellung auch die Lebensdauer und Zuverlässigkeit der Technik verbessert werden.

6.2.1 Geeignete Aufstellung eines Arbeitsplatz-IT-Systems

Unter Arbeitsplatz-IT-Systemen sind etwa PCs, Notebooks oder Terminals zu verstehen.

Bei der Aufstellung eines Arbeitsplatz-IT-Systems sollten zusätzlich zu den von den Herstellern festgeschriebenen Vorgaben und Hinweisen sowie ergonomischen Gesichtspunkten folgende Voraussetzungen beachtet werden:

- der Standort in der Nähe eines Fensters oder einer Tür erhöht die Gefahr des Beobachtetwerdens
- das System sollte nicht in unmittelbarer Nähe der Heizung aufgestellt werden (Vermeidung von Überhitzung, aber auch kompromittierender Abstrahlung)
- das System sollte, so weit möglich und erforderlich, physisch gesichert sein (Diebstahlschutz, versperrbare Diskettenlaufwerke ...)

6.2.2 Geeignete Aufstellung von Servern und anderen besonders schützenswerten IT-Komponenten

Neben Servern (Datenbank-, Programm- und Kommunikationsserver, aber auch TK-Anlagen) sind in diesem Zusammenhang auch Netzwerkkomponenten wie Router, Switches, Firewalls etc. zu schützen. Um Vertraulichkeit, Integrität und Verfügbarkeit im Betrieb von solchen besonders schützenswerten IT-Komponenten sicherzustellen, ist es zwingend erforderlich, diese in einer gesicherten Umgebung aufzustellen.

Diese kann realisiert werden als:

- **Serverraum:**
Raum zur Unterbringung von Servern, serverspezifischen Unterlagen, Datenträgern in kleinem Umfang sowie weiterer Hardware (etwa Drucker oder Netzwerkkomponenten). Im Serverraum ist im Allgemeinen kein ständig besetzter Arbeitsplatz eingerichtet, er wird nur sporadisch und zu kurzfristigen Arbeiten betreten. Ein Serverraum bietet grundsätzlich Schutz vor unbefugtem Betreten, spezielle Vorrichtungen wie z.B. Brandschutztüren können darüber hinaus im Fall eines Brandes die Sicherheit der Geräte und Daten erhöhen.
- **Serverschrank:**
Versperrbare Serverschränke (Racks) dienen zur Unterbringung von IT-Geräten und sollen den Inhalt gegen unbefugten Zugriff schützen. Der Schutz vor Schäden durch Feuer und Rauchgasen ist bei den meisten Serverschränken dagegen nicht gegeben.

Generell ist zu beachten:

- Der Zugang und Zugriff zu Servern und anderen schützenswerten Komponenten darf ausschließlich autorisierten Personen möglich sein.
- Eine Vertretungsregelung muss sicherstellen, dass der Zugriff auch im Vertretungsfall geregelt möglich ist und unautorisierte Zugriffe auch in Ausnahmesituationen nicht vorkommen können.
- In jedem Fall ist für die sichere Verwahrung der Zugangsschlüssel zu sorgen. Es muss außerdem darauf geachtet werden, dass die entsprechenden Räume bzw. Schränke

tatsächlich immer versperrt werden.

6.3 Brandschutz

Brandschutz stellt die Gesamtheit aller Maßnahmen dar, die die Entstehung und Ausbreitung von Bränden verhindern und die Bekämpfung von Bränden gewährleisten.

Der Einsatz von Brandschutztüren zur Bildung eines eigenen Brandabschnitts sowie Sicherheitstüren, die einen höheren Schutz gegen Einbruch bieten, ist bei systemkritischen Räumen (Serverräume, Verteilerräume) nach Möglichkeit vorzusehen.

Brandmeldeanlagen dienen zur Überwachung eines bestimmten, besonders gefährdeten Bereiches oder eines gesamten Gebäudes. Brandmelder dienen zur Früherkennung von Brandgefahren und werden in automatische und nichtautomatische Melder unterschieden, welche an einer Brandmeldeanlage hängen oder als Einzelmelder fungieren.

Bei Brandmeldern unterscheidet man:

- Ionisationsrauchmelder
- Streulichtmelder
- Wärmemelder (Maximal- oder Differentialmelder)
- Flammenmelder
- Druckknopfmelder (nicht automatisch)

Brandmeldeanlagen können mit einer TUS-Leitung direkt mit der Feuerwehr verbunden sein oder intern auf einer kompetenten, ständig besetzten Stelle auflaufen.

In Räumen mit IT oder Datenträgern (Serverraum, Datenträgerarchiv), 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. Die Einhaltung des Rauchverbotes ist zu kontrollieren.

Papier und andere leicht brennbare Materialien sollten unbedingt außerhalb der systemkritischen Räume (Serverraum, Verteilerraum) gelagert werden, um die Brandlast möglichst gering zu halten.

6.3.1 Einhaltung von Brandschutzvorschriften und Auflagen

Die gesetzlichen Brandschutzvorschriften und die Auflagen der zuständigen Baubehörde sowie der örtlichen Feuerwehr sind unbedingt einzuhalten.

Brandverhütungsstellen und/oder Brandschutzexperten können und sollen bei der Brandschutzplanung hinzugezogen werden. Regelmäßige Brandschutzbegehungen - angekündigt oder unangekündigt - sollten erfolgen, um Missestände im Brandschutzbereich aufzuzeigen.

6.3.2 Brandbekämpfung

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.

Handfeuerlöscher (Mittel der Ersten und Erweiterten Löschhilfe)

Eine Sofortbekämpfung ist nur möglich, wenn entsprechende Handfeuerlöscher in ausreichender Zahl und Größe im Gebäude - möglichst in räumlicher Nähe zu besonders schützenswerten Bereichen und Räumen - zur Verfügung stehen.

Pulverlöscher mit Eignung für Brandklasse E bis 1000 V sind für elektrisch betriebene Peripheriegeräte geeignet. Für elektronisch gesteuerte Geräte wie z.B. Computer müssen dagegen Kohlendioxid-Löschler (Brandklasse B) eingesetzt werden, um die Zerstörung empfindlicher Komponenten zu vermeiden.

Dabei ist zu beachten:

- Die Feuerlöscher müssen regelmäßig geprüft und gewartet werden.
- Die Feuerlöscher müssen so angebracht werden, dass sie im Brandfall leicht erreichbar sind.

- Die Beschäftigten müssen über die Standorte der nächsten Feuerlöscher informiert und in deren Handhabung unterwiesen sein.

Automatische Löschanlagen

Löschanlagen der verschiedensten Ausführungen sind meistens mit einer Brandmeldeanlage gekoppelt und werden im Bedarfsfall von dieser selbständig ausgelöst.

Automatische Löschanlagen werden meistens von der Behörde bei Vorlage einer erhöhten Brandgefährdung vorgeschrieben, um Entstehungsbrände effizient zu bekämpfen bzw. eine Ausbreitung zu unterbinden.

Rauchschutzvorkehrungen

Im Brandfall geht von der damit verbundenen Rauchentwicklung sowohl für Mensch als auch für IT-Geräte eine erhebliche Gefahr aus. Ein umfassender Rauchschutz ist daher vorzusehen.

In diesem Sinne ist zu gewährleisten, dass

- rauchdichte Brandschutztüren verwendet werden
- Rauchschutztüren verwendet werden, die ggf. bei Rauchentwicklung selbsttätig geschlossen werden und die Rauchausbreitung verhindern
- die Lüftungsanlage eine Ablüftung von Rauch vornehmen kann
- die Lüftungs- und Klimaanlage selbsttätig auf Rauchentwicklung reagieren

6.4 Stromversorgung, Maßnahmen gegen elektrische Risiken

6.4.1 Angepasste Aufteilung der Stromkreise

Die Dimensionierung, für die eine Elektroinstallation ausgelegt wurde, stimmt erfahrungsgemäß nach einiger Zeit nicht mehr mit den tatsächlichen Gegebenheiten überein. Es ist daher anzuraten, bei Änderungen der Raumnutzung und bei Änderungen und Ergänzungen der technischen Ausrüstung (IT, Klimaanlage, Beleuchtung etc.) die Elektroinstallation zu prüfen und gegebenenfalls anzupassen.

Eine unterdimensionierte Stromversorgung kann zu Computerabstürzen führen, die ihrerseits wieder die Gefahr von Datenverlust in sich bergen.

6.4.2 Lokale unterbrechungsfreie Stromversorgung

Mit einer unterbrechungsfreien Stromversorgung (USV) kann ein kurzzeitiger Stromausfall überbrückt werden oder die Stromversorgung solange aufrechterhalten werden, dass ein geordnetes Herunterfahren der angeschlossenen Rechner möglich ist.

USV-Anlagen (Unterbrechungsfreie Stromversorgung) können neben der Überbrückung von Totalausfällen der Stromversorgung und Unterspannungen auch dazu dienen, Überspannungen (z.B. durch Blitzschlag) zu glätten. Bei der Dimensionierung einer USV kann man in der Regel von einer üblichen Überbrückungszeit von ca. 10 bis 15 Minuten ausgehen, in der die angeschlossene IT ohne externe Stromquelle betrieben oder geordnet heruntergefahren werden kann. Die Überbrückung von Stromausfällen bzw. das geordnete Herunterfahren beugt Datenverlusten vor, die in Folge von plötzlichem "Ausschalten" (Stromverlust) entstehen können.

Dies ist insbesondere dann sinnvoll,

- wenn im Rechner umfangreiche Daten zwischengespeichert werden (z.B. im Cache-Speicher am Netzserver), bevor sie auf nichtflüchtige Speicher ausgelagert werden,
- beim Stromausfall ein großes Datenvolumen verlorengehen würde und nachträglich nochmals erfasst werden müsste,
- wenn die Stabilität der Stromversorgung nicht ausreichend gewährleistet ist.

6.4.3 Not-Aus-Schalter

Bei Räumen, in denen durch die darin betriebenen elektrischen Geräte erhöhtes Brandrisiko besteht, ist die Installation eines Not-Aus-Schalters vorzusehen. Mit Betätigung dieses 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.

Der Not-Aus-Schalter sollte innerhalb des Raumes neben der Eingangstür (eventuell mit Lagehinweis außen) oder außerhalb des Raumes neben der Tür angebracht und gegen versehentliches Betätigen geschützt werden.

6.4.4 Blitzschutzeinrichtungen, Überspannungsschutz

*Die direkten Auswirkungen eines Blitzeinschlages auf ein Gebäude (Beschädigung der Bausubstanz, Dachstuhlbrand u.ä.) lassen sich durch die Installation einer Blitzschutzanlage 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.*

Überspannungen durch Blitz haben hohes zerstörerisches Potenzial. Andere Überspannungen sind geringer, können aber trotzdem ausreichen, um Mikroelektronikgeräte zu stören oder zu zerstören. Der Überspannungsschutz wird in der Regel in drei voneinander abhängigen Stufen aufgebaut, und zwar in einen *Grobschutz*, mit dem Überspannungen bis 6000 V abgefangen werden können, in einen *Mittelschutz*, der die verbleibende Überspannung auf ca. 1500 V begrenzt und schließlich in einen *Feinschutz*, der die verbleibende Überspannung auch für empfindliche Bauteile absenkt.

Weiters ist zu beachten:

- Blitz- und Überspannungsschutzeinrichtungen sollten periodisch und nach bekannten Ereignissen geprüft und gegebenenfalls ersetzt werden.
- Potentialausgleich: Nur wenn alle Schutzeinrichtungen sich auf das gleiche Potential beziehen, ist ein optimaler Schutz möglich. Bei Nachinstallationen ist darauf zu achten, dass der Potentialausgleich mitgeführt wird.