IT-Sicherheitshandbuch

für die öffentliche

Verwaltung

Teil 2: IT-Sicherheitsmaßnahmen

B u n d e s m i n i s t e r i u m f ü r ö f f e n t l i c h e L e i s t u n g u n d S p o r t

IT-Sicherheitshandbuch

für die öffentliche Verwaltung

Teil 2:

IT-Sicherheitsmaßnahmen

Version 1.0

März 2000

Vorwort

Nach der Veröffentlichung des ersten Teiles ("IT-Sicherheitsmanagement") im Jahr 1999 liegt

Nach der Veröffentlichung des ersten Teiles ("IT-Sicherheitsmanagement") im Jahr 1999 liegt nunmehr der zweite Teil des "IT-Sicherheitshandbuches für die österreichischen Behörden" mit dem Titel "IT-Sicherheitsmaßnahmen" vor.

Das IT-Sicherheitshandbuch wurde auf Initiative und mit finanzieller Hilfe des Bundesministeriums für Inneres im Rahmen einer Arbeitsgruppe der ADV-Koordination im BKA entwickelt. Es soll Unterstüzung bei der Etablierung und Umsetzung von IT-Sicherheit bieten und insbesondere den einzelnen Ressorts ermöglichen,

* die für ihren Bereich relevanten IT-Sicherheitsziele und -strategien zu ermitteln,
* eine eigenständige, jedoch mit den anderen Ressorts kompatible IT-Sicherheitspolitik zu erstellen,
* geeignete Sicherheitsmaßnahmen auszuwählen und zu realisieren sowie
* IT-Sicherheit im laufenden Betrieb zu gewährleisten.

Der Teil 1 *"IT-Sicherheitsmanagement"* des Handbuches beinhaltet konkrete Anleitungen zur Etablierung eines umfassenden und kontinuierlichen IT-Sicherheitsprozesses innerhalb einer Behörde und deckt damit die ersten beiden oben angeführten Zielsetzungen ab.

Der nunmehr vorliegende zweite Teil *"IT-Grundschutzmaßnahmen"* beinhaltet die Beschreibung grundlegender organisatorischer, personeller, infrastruktureller und technischer Standardsicherheitsmaßnahmen. Ziel ist die Gewährleistung eines angemessenen und ausreichenden Sicherheitsniveaus für IT-Systeme mit *mittlerem Schutzbedarf* . Die Schwerpunkte liegen dabei auf der mittleren Datenverarbeitung und PCs, wobei versucht wird, eine möglichst umfassende und vollständige Sammlung von IT-Sicherheitsmaßnahmen für den gesamten System-Lifecycle zu geben, jedoch nicht auf systemspezifische Details eingegangen wird. Aus diesem Grund werden auch klassische RZ-Sicherheitsfragen nur am Rande behandelt, da sie im Allgemeinen systemspezifischer Lösungen bedürfen und oft über einen mittleren Schutzbedarf hinausgehen.

Einige generelle Anmerkungen:

* Das IT-Sicherheitshandbuch wurde für die Anwendung in der öffentlichen Verwaltung erstellt und ist auf die spezifischen Anforderungen in diesem Bereich abgestimmt. Aufgrund des generellen Ansatzes kann es aber auch durchaus für Anwender außerhalb dieses Bereiches von Nutzen sein.

* Das Handbuch konzentriert sich auf den Bereich "Sicherheit von Systemen der Informationstechnik" (kurz "IT-Sicherheit"). Dies umfasst Hardware, Software, Daten, aber

auch organisatorische, bauliche und personelle Fragen, soweit sie in direktem Zusammenhang mit der Sicherheit von IT-Systemen stehen. Abzugrenzen davon ist das Gebiet der "Informationssicherheit", das sich mit dem Schutz von Information generell, also etwa auch in schriftlicher Form, auf Mikrofilmen oder in gesprochener Form, befas Dies ist nicht Gegenstand dieses Handbuches.

*

* Das IT-Sicherheitshandbuch versteht sich als Sammlung von Leitlinien und Empfehlungen, die entsprechend den spezifischen Anforderungen und Bedürfnissen in einer Einsatzumgebung angepasst werden sollten. Es stellt eine Ergänzung zu den bestehenden Regelungen und Vorschriften (Datenschutzgesetz, Verschlusssachenvorschriften, Amtsgeheimnis,...) dar und soll diese nicht außer Kraft setzen oder zu ihnen im Widerspruch steh

*

* Seit einigen Jahren werden auf nationaler und internationaler Ebene verstärkt Anstrengen unternommen, einheitliche methodische Vorgehensweisen zur Etablierung von IT-Sicherheit sowie Standard-Maßnahmenkataloge zu erarbeiten. Die österreichische öffent-

liche Verwaltung unterstützt diese Bestrebungen und versucht, im vorliegenden Handbuch diesen internationalen Entwicklungen so weit wie möglich Rechnung zu tragen. Bei der Erstellung der Maßnahmenbeschreibungen wurde daher auch auf bewährte und etablierte Quellen zurückgegriffen, die im Einzelnen im Anhang B angeführt sind. Gedankt werden darf insbesondere dem Bundesamt für Sicherheit in der Informationstechnik, Bonn, für seine Zustimmung zur Verwendung des IT-Grundschutzhandbuches, das einen wichtigen Ausgangspunkt für das vorliegende Handbuch darstellt.

Um die Aktualität der beschriebenen Maßnahmen sicherzustellen, wird das IT-Sicherheitshandbuch regelmäßig überarbeitet und aktualisiert. Von besonderer Bedeutung ist dabei ein Feedback über die Erfahrungen mit der Anwendung des Handbuches in der Praxis. Alle Anwender des Handbuches werden daher eingeladen, diesbezügliche Anregungen und Erfahrungen den Verfassern mitzuteilen. Die nachstehend in alphabetischer Reihenfolge angeführten Mitglieder der Arbeitsgruppe stehen für Anregungen, Beiträge und Fragen gerne zur Verfügung:

Eduard Busch	BM für Inneres	eduard.busch@bmi.gv.at
DI Theodor Garaus	Bundeskanzleramt	theodor.garaus@bka.gv.at
Gerhard Herzog	BM für Landesverteidigung	gerhard.herzog@bmlv.gv.at
Helmar Heydebreck	Bundeskanzleramt	helmar.heydebreck@bka.gv.at
Peter Kelsch	BM für Inneres	peter.kelsch@bmi.gv.at
Ing. Roland Ledinger	Bundeskanzleramt	roland.ledinger@bka.gv.at
Ing. Johannes Pleskac	BM für Finanzen	johann.pleskac@bmf.gv.at
Dr. Ingrid Schaumüller-Bichl	externe Konsulentin	ingrid.schaumueller@telecom.at

---

Inhalt

IT-Sicherheitshandbuch für die öffentliche Verwaltung
Teil 2

1 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 Grundstücke, Gebäude oder Räume (Büros, Serverräume, Datenträgerarchiv, Räume für technische Infrastruktur, ...).

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 eingerichtet?
* Stärke und Schutz/Überwachung von Wänden, Türen, Fenstern, Lüftungsschächten etc.
* Infrastruktur (Wasser-, Stromversorgung, Kommunikationsverbindungen, Klimaanlage, USV,..)
* Welche Bereiche des Grundstückes bzw. des Gebäudes sind sicherheitsrelevant?

Im Folgenden werden eine Reihe von grundlegenden Sicherheitsmaßnahmen angeführt. Welche davon in einem konkreten Fall zum Einsatz kommen, ist abhängig von Größe und Schutzbedarf der Organisation. Nach Möglichkeit sollten bauliche und infrastrukturelle Maßnahmen bereits in der Planungs- bzw. Bauphase Berücksichtigung finden, ein nachträglicher Einbau ist meist teuer oder gar unmöglich.

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

Wo sinnvoll bzw. hilfreich werden in den nachfolgenden Maßnahmenbeschreibungen Normen beispielhaft herausgegriffen und angeführt. Dabei handelt es sich nicht um eine vollständige Aufzählung aller für einen Bereich relevanten Normen und auch nicht um verbindliche Einsatzempfehlungen, die angeführten Beispiele sollen lediglich einen Hinweis auf existierende, möglicherweise zur Anwendung kommende Normen geben und ein detailliertes Einarbeiten in die Materie erleichtern.

1.1 Bauliche Maßnahmen

INF 1.1 Geeignete Standortauswahl

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

* In Zusammenhang mit Schwächen in der Bausubstanz kann es durch Erschütterungen naher Verkehrswege (Straße, Eisenbahn, U-Bahn) zu Beeinträchtigungen der IT kommen. Gebäude, die direkt an Hauptverkehrstrassen (Autobahn, Bundesstraße, Bahn,...) liegen, können durch Unfälle beschädigt werden, für Gebäude in Einflugschneisen von Flughäfen besteht Gefahr durch einen eventuellen Flugzeugabsturz.
* Die Nähe zu optimalen Verkehrswegen wird in vielen Fällen als Vorteil angesehen werden, kann aber - da diese Verkehrswege auch potentielle Fluchtwege darstellen können - unter Umständen auch die Durchführung eines Anschlages erleichtern. Vor- und Nachteile sind entsprechend abzuwägen.
* In der Nähe von Sendeeinrichtungen kann es zu Störungen der IT kommen.
* Bei Überbauten von U-, S- oder Eisenbahnen kann es zu Störungen von Datenleitungen kommen.
* In der Nähe von Gewässern und in Niederungen ist mit Hochwasser zu rechnen.
* In der Nähe von Kraftwerken oder Fabriken kann durch Unfälle oder Betriebsstörungen (Explosion, Austritt schädlicher Stoffe) die Verfügbarkeit des Gebäudes (z.B. durch Evakuierung oder großräumige Absperrung) beeinträchtigt werden.

INF 1.2 Anordnung schützenswerter Gebäudeteile

Schützenswerte Räume oder Gebäudeteile sollten nicht in exponierten oder besonders gefährdeten Bereichen untergebracht sein. Insbesondere ist zu beachten:

* Kellerräume sind durch Wasser gefährdet.

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

Als Faustregel kann man sagen, dass schutzbedürftige Räume oder Bereiche im Zentrum eines Gebäudes besser untergebracht sind als in dessen Außenbereichen.
Optimal ist es, diese Aspekte schon in die Bauplanung für ein neues Gebäude oder in die Raumbelegungsplanung bei Einzug in ein bestehendes einzubeziehen.

Besteht die Möglichkeit, auch das Umfeld des Gebäudes in das Sicherheitskonzept einzubeziehen (etwa bei einer eigenen, ausschließlich der betreffenden Organisation gehörigen

---

Liegenschaft), so können zusätzliche bauliche und technische Sicherheitsmaßnahmen getroffen werden ("Perimeterschutz", "Freilandschutz"). Dazu zählen etwa:
* Zäune und Mauern
* Tore, Schranken und Fahrzeugsperren
* Kameraüberwachung und Bewegungsmelder

*

INF 1.3 Einbruchsschutz

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 nichtbenutzten Nebeneingängen,
* einbruchgesicherte Notausgänge,
* Verschluss von Personen- und Lastenaufzügen außerhalb der Dienstzeit.

Den Mitarbeitern ist durch Regelungen bekannt zu geben, welche Maßnahmen zum Einbruchsschutz beachtet werden müssen.

Beispielhaft gelten die in Anhang A angeführten ÖNORMEN zum Einbruchschutz.

INF 1.4 Zutrittskontrolle

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 die generellen Richtlinien für den Perimeter, Gebäude- u Geräteschutz fest. Dazu gehören:

* Festlegung der Sicherheitszonen:
  Zu schützende Bereiche können etwa Grundstücke, Gebäude, Rechnerräume, Räume mit Peripheriegeräten (Drucker,...), Archive, Kommunikationseinrichtungen und die Haustechnik sein. Die einzelnen Bereiche können unterschiedliche Sicherheitsstufen aufweisen.

* Generelle Festlegung der Zutrittskontrollpolitik:
  Hier wird grundsätzlich festgelegt, welche Personengruppen (etwa RZ-Mitarbeiter, Operator, Fachabteilungsmitarbeiter, Kunden, Angehörige von Lieferfirmen etc.) Zutritt

---

welchen Bereichen benötigen.
Um die Zahl der zutrittsberechtigten Personen zu einem Raum möglichst gering zu halten, sollte auch beim IT-Einsatz der Grundsatz der Funktionstrennung berücksichtigt werden. So verhindert beispielsweise eine getrennte Lagerung von Ersatzteilen für IT-Systeme u Datenträgern den unerlaubten Zugriff von Wartungstechnikern auf die Datenträger.

* Bestimmung eines Verantwortlichen für Zutrittskontrolle:
  Dieser vergibt die Zutrittsberechtigungen an die einzelnen Personen entsprechend den i der Sicherheitspolitik festgelegten Grundsätzen.

* Dokumentation der Vergabe und Rücknahme von Zutrittsberechtigungen

* Definition von Zeitabhängigkeiten:
  Es ist zu klären, ob zeitliche Beschränkungen der Zutrittsrechte erforderlich sind. So Zeitabhängigkeiten können etwa sein: Zutritt nur während der Arbeitszeit, Zutritt einm täglich oder befristeter Zutritt bis zu einem fixierten Datum.

* Festlegung der Zutrittskontrollmedien:
  Es ist festzulegen, ob die Identifikation bzw. die Authentisierung durch Überwachungs-personal (persönlich oder mittels Überwachungskameras) oder durch automatische Identifikations- und Authentisierungssysteme wie Zugangscodes (Passwörter, PINs), Karten oder biometrische Methoden erfolgen soll.

* Festlegung der Rechteprüfung
  Im Zutrittskontrollkonzept ist festzulegen, wo, zu welchen Zeiten und unter welchen Ra bedingungen eine Rechteprüfung erfolgen muss, sowie welche Aktionen bei versuchtem unerlaubten Zutritt zu setzen sind.

* Festlegung der Beweissicherung:
  Hier ist zu bestimmen, welche Daten bei Zutritt zu und Verlassen von einem geschützten Bereich protokolliert werden. Dabei bedarf es einer sorgfältigen Abwägung zwischen den Sicherheitsinteressen des Systembetreibers und den Schutzinteressen der Privatsphäre d Einzelnen.

* Behandlung von Ausnahmesituationen
  Es ist u.a. sicherzustellen, dass im Brandfall die Mitarbeiter schnellstmöglich die gefährdeten Zonen verlassen können.

Weiters sind folgende Fragen zu klären:

* Sind beim Betreten und/oder Verlassen eines geschützten Bereiches Vereinzelungs-mechanismen (Drehtüren, Schleusen, ...) notwendig?
* Welche Maßnahmen sind bei unautorisierten Zutrittsversuchen zu setzen?

Page 16

* Ist eine Nullsummenprüfung [1] erforderlich ?
* Ist das Auslösen eines "stillen Alarms" vorzusehen?
  Durch Eingabe einer vereinbarten Kennung, etwa einer zusätzlichen Ziffer zur üblichen PIN, wird ein Alarm an einer entfernten Überwachungsstelle (Portier, Polizei) ausgelöst. Eine solche Maßnahme bietet Schutz gegen jemanden, der den Zugang zu geschützten Bereichen gewaltsam erzwingen will.
* Sperrmöglichkeiten bei Verlust oder Duplizierung des Zutrittskontrollmediums (Schlüssel, Karte,...) und bei Austritt eines Mitarbeiters.
* Stehen die Kosten für die Installation, den laufenden Betrieb, die Wartung und die regelmäßige Revision des Zutrittskontrollsystems in vertretbarer Relation zum möglichen Sicherheitsrisiko?
* Ist die Kapazität des Zutrittskontrollsystems der Größe der Organisation angepasst? Insbesondere ist eine ausreichende Zahl von Kontrollstellen und eventuellen Vereinzelungsmechanismen vorzusehen, um Warteschlangen auch zu Stoßzeiten (Arbeitsbeginn,...) zu vermeiden.

Das Zutrittskontrollkonzept sollte bereits vor der Systemauswahl so detailliert wie möglich feststehen und weitgehend stabil bleiben. Überarbeitungen werden jedoch notwendig, bei

* Feststellung von Sicherheitsmängeln,
* schlechter Benutzerakzeptanz
  etwa auf Grund zu langer Wartezeiten oder psychologischer Faktoren (z.B. bei biometrischen Systemen) sowie
* Erweiterungen des sicherheitsrelevanten Bereiches.

INF 1.5 Portierdienst

Die Einrichtung eines Portierdienstes hat weit reichende positive Auswirkungen gegen eine ganze Reihe von Gefährdungen. Voraussetzung ist allerdings, dass bei der Durchführung des Portierdienstes einige Grundprinzipien beachtet werden.

* Der Portier beobachtet bzw. kontrolliert alle Personenbewegungen am Eingang zum Gebäude bzw. sicherheitsrelevanten Bereich.
* Unbekannte Personen haben sich beim Portier zu legitimieren.
* Der Portier hält vor Einlassgewährung eines Besuchers bei dem Besuchten Rückfrage.
* Der Besucher wird zu dem Besuchten begleitet oder am Eingang abgeholt.
* Dem Portier müssen die Mitarbeiter bekannt sein. Scheidet ein Mitarbeiter aus, ist auch der Portier zu unterrichten, ab wann diesem Mitarbeiter der Einlass zu verwehren ist.
* Abhängig von der Sensibilität des Bereiches sind die Führung eines Besucherbuches, in dem der Zutritt von Fremdpersonen zum Gebäude dokumentiert werden kann, sowie die Ausgabe von Besucherausweisen oder Besucherbegleitscheinen zu erwägen.

[1] Nullsummenprüfung: Feststellung der Anzahl der im geschützten Bereich befindlichen Personen durch Vergleich der Zu- und Ab
Voraussetzung für eine Nullsummenprüfung ist die Installation von Vereinzelungsmechanismen.

Page 17

Die Aufgabenbeschreibung muss verbindlich festschreiben, welche Aufgaben dem Portier im Zusammenspiel mit weiteren Schutzmaßnahmen zukommen (z.B. Gebäudesicherung nach Dienst- oder Geschäftsschluss, Scharfschaltung der Alarmanlage, Kontrolle der Außentüren und Fenster).

INF 1.6 Einrichtung einer Postübernahmestelle

Die Übernahme von Briefen und Paketen sollte durch eine zentrale Stelle unter Beachtung von für die betreffende Organisation adäquaten Sicherheitsregeln erfolgen. Solche Regeln können etwa sein:

* Pakete, die von einem Botendienst o.ä. gebracht werden, dürfen erst nach Rücksprache m dem namentlich angeführten Empfänger oder einem berechtigten Vertreter übernommen werden.
* Pakete, die ohne namentlich angeführten Empfänger an die Organisation adressiert sind und von einem Paket- oder Botendienst bzw. von einer Privatperson gebracht werden, sin nicht zu übernehmen.
* Wird außerhalb der Amts- bzw.- Bürostunden ein Brief oder ein Paket abgegeben, so ist vom Dienst habenden Mitarbeiter (z.B. Portier, Operator,...) beim Empfänger rückzufragen, ob eine Sendung erwartet wird. Ist dies nicht der Fall oder ist der Empfä nicht erreichbar, so ist die Sendung nicht anzunehmen.
* Für größere Organisationseinheiten ist die Beschaffung von Geräten zum Durchleuchten von Postsendungen zu erwägen.

1.2 Brandschutz

INF 2.1 Einhaltung von Brandschutzvorschriften und Auflagen

Die bestehenden gesetzlichen und internen Brandschutzvorschriften und die behördlichen Auflagen der örtlich zuständigen Feuerwehr sind für Gebäude unbedingt einzuhalten.

Die jeweiligen Brandverhütungsstellen der Bundesländer oder Brandschutzexperten können und sollen bei der Brandschutzplanung hinzugezogen werden.

In Anhang A sind eine Reihe von wichtigen Normen zum Thema Brandschutz angeführt.

Ebenso ist es notwendig, die allgemeinen und speziellen Bestimmungen des Arbeitnehmer-schutzes und die Arbeitsstättenverordnung bei der Errichtung und beim Betrieb zu beachtei

---

* Bundes-Bedienstetenschutzgesetz B-BSG, BGBl-Nr. 70/1999
* ArbeitnehmerInnenschutzgesetz, BGBL-Nr. 450/1994

und die dazu ergangenen Verordnungen.

Es ist empfehlenswert, weitere Hinweise zum Brandschutz zu beachten, wie sie zum Beispiel in den Publikationen des Verbands der Schadensversicherer (VdS) in Deutschland zu finden sind. (Adresse siehe Anhang D)

INF 2.2 Raumbelegung unter Berücksichtigung von Brandlasten

Eine Brandlast entsteht durch alle brennbaren Stoffe, die ins Gebäude eingebracht werden. Sie ist von der Menge und vom Heizwert der Stoffe abhängig. IT-Geräte und Leitungen stellen ebenso eine Brandlast dar wie Möbel, Fußbodenbeläge und Gardinen.

Bei der Unterbringung von IT-Geräten, Datenträgern etc. sollte eine vorherige Beachtung der vorhandenen Brandlasten im gleichen Raum und in den benachbarten Räumen erfolgen. So sollte etwa das Datenträgerarchiv nicht in der Nähe von oder über einem Papierlager untergebracht sein.

INF 2.3 Brandabschottung von Trassen

Bei Gebäuden mit mehreren Brandabschnitten lässt es sich kaum vermeiden, dass Trassen durch Brandwände und Decken führen. Die Durchbrüche sind nach Verlegung der Leitungen entsprechend dem Brandwiderstandswert der Wand bzw. Decke zu schotten. Um die Nachinstallation zu erleichtern, können geeignete Materialien (z.B. Brandschutzkissen) verwendet werden. Entsprechende Richtlinien und Normen (ÖNORM siehe angeführte Liste) sind zu beachten. Bei der Trassenplanung sollte der für den Brandschutz Zuständige hinzugezogen werden.

INF 2.4 Verwendung von Sicherheitstüren

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

* Sicherheitstüren (einbruchhemmende Türen) bieten auf Grund ihrer Stabilität einen höheren Schutz gegen Einbruch (z.B. bei Keller- und Lieferanteneingängen).
* Brandschutztüren verzögern die Ausbreitung eines Brandes.

Wichtige ÖNORMEN dazu werden in Anhang A angeführt.

Der Einsatz von Sicherheitstüren ist über den von der Feuerwehr vorgeschriebenen Bereich hinaus (vgl. *INF 2.1 Einhaltung von Brandschutzvorschriften*) bei Anlagen bei schutzbedürftigen Räumen wie Serverraum, Beleg- oder Datenträgerarchiv sinnvoll.

Es ist dafür zu sorgen, dass Brand- und Rauchschutztüren auch tatsächlich geschlossen und nicht (unzulässigerweise) z.B. durch Keile offen gehalten werden. Alternativ können Türen mit einem automatischen Schliessmechanismus, der im Alarmfall aktiviert wird, eingesetzt werden.

INF 2.5 Brandmeldeanlagen

Brandmeldeanlagen (BMA) dienen zur Überwachung eines bestimmten besonders gefährdeten Bereiches oder eines gesamten Gebäudes. Derartige Brandmeldeanlagen können mit einer TUS-Leitung[2] direkt mit der Feuerwehr verbunden sein oder intern auf einer kompetenten, ständig besetzten Stelle auflaufen.

Entsprechend den Anschlussbedingungen müssen künftig alle neuen Brandmeldeanlagen über

eine Interventionsschaltung verfügen, was bedeutet, dass nach dem ersten Brandalarm 3 bis Minuten Zeit verbleiben um die Meldung zu überprüfen. Wird diese Brandmeldung in der vorgesehenen Zeit nicht quittiert, bzw. gelangen während der Überprüfungszeit eine oder mehrere weitere Meldungen zur Brandmeldeanlage, werden diese sofort an die Feuerwehr weitergeleitet.

Bereits in Betrieb befindliche Brandmeldeanlagen müssen, je nach Grösse des Überwachungs- bereiches, bis spätestens 2010 umgebaut werden und eine Interventionsschaltung aufweisen

Siehe dazu TRVB S 123 Brandmeldeanlagen.

INF 2.6 Handfeuerlöscher

Die meisten Brände entstehen aus kleinen, anfangs noch gut beherrschbaren Brandherden. Besonders in Büros findet das Feuer reichlich Nahrung und kann sich sehr schnell ausbrei Der Sofortbekämpfung von Bränden kommt also ein sehr hoher Stellenwert zu.

Diese Sofortbekämpfung ist nur möglich, wenn Handfeuerlöscher in der jeweils geeigneten Brandklasse (ÖNORM EN2) in ausreichender Zahl und Größe im Gebäude zur Verfügung stehen. Dabei ist die räumliche Nähe zu schützenswerten Bereichen und Räumen wie Server- raum, Raum mit technischer Infrastruktur oder Belegarchiv anzustreben. Pulverlöscher mit

[2] Interessengemeinschaft Telekommunikation und Sicherheit (IG TUS)

Eignung für Brandklasse E bis 1000 V sind für elektrisch betriebene Peripheriegeräte geeignet, für elektronisch gesteuerte Geräte, z.B. Rechner, sollten Kohlendioxyd-Löscher (Brandklasse B) zur Verfügung stehen.

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 sollten sich die Standorte des nächsten Feuerlöschers einprägen.
* Die Standorte von Handfeuerlöschern sollten auch sichtbar (mit Piktogramm) markiert werden.
* Bei entsprechenden Brandschutzübungen sind die Mitarbeiter in die Benutzung der Handfeuerlöscher einzuweisen.

INF 2.7 Brandschutzbegehungen

Die Erfahrungen zeigen, dass im täglichen Betrieb die Vorschriften und Regelungen zum Brandschutz immer nachlässiger gehandhabt werden oft bis hin zur völligen Ignoranz. Einige Beispiele dazu:

* Fluchtwege werden blockiert, z.B. durch Möbel und Papiervorräte.
* Brandabschnittstüren werden durch Keile offen gehalten.
* Zulässige Brandlasten werden durch anwachsende Kabelmengen oder geänderte Nutzungen überschritten.
* Brandabschottungen werden bei Arbeiten beschädigt und nicht ordnungsgemäß wieder- hergerichtet.

Aus diesem Grund sollten ein- bis zweimal im Jahr Brandschutzbegehungen angekündigt

oder unangekündigt erfolgen. Vorgefundene Missstände müssen dazu Anlass geben, die Zustände und deren Ursachen unverzüglich zu beheben.

Im Wiederholungsfall oder bei besonders eklatanten Verstößen gegen die Brandschutzvorschriften sind auch entsprechende Sanktionen vorzusehen.

INF 2.8 Rauchverbot

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

1.3 Stromversorgung, Maßnahmen gegen elektrische und elektromagnetische Risiken

INF 3.1 Angepasste Aufteilung der Stromkreise

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

INF 3.2 Not-Aus-Schalter

Bei Räumen, in denen elektrische Geräte in der Weise betrieben werden, dass z.B. durch deren Abwärme, durch hohe Gerätedichte oder durch Vorhandensein zusätzlicher Brandlasten ein erhöhtes Brandrisiko besteht, ist die Installation eines Not-Aus-Schalters sinnvoll. Betätigung des Not-Aus-Schalters wird dem Brand eine wesentliche Energiequelle genommen, was bei kleinen Bränden zu deren Verlöschen führen kann. Zumindest ist aber die Gefahr durch elektrische Spannungen beim Löschen des Feuers beseitigt.

Zu beachten ist, dass lokale unterbrechungsfreie Stromversorgungen (USV) nach Ausschalter der externen Stromversorgung die Stromversorgung selbsttätig übernehmen und die angeschlossenen Geräte unter Spannung bleiben. Daher ist bei der Installation eines Not-Aus-Schalters zu beachten, dass auch die USV abgeschaltet und nicht nur von der externen Str versorgung getrennt wird.

Der Not-Aus-Schalter sollte innerhalb des Raumes neben der Eingangstür (evtl. mit Lagehinweis außen an der Tür) oder außerhalb des Raumes neben der Tür angebracht werden. Dabei ist allerdings zu bedenken, dass dieser Not-Aus-Schalter auch ohne Gefahr

versehentlich oder absichtlich betätigt werden kann.

INF 3.3 Zentrale Notstromversorgung

In Bereichen, in denen die Stromversorgung bei Ausfällen des öffentlichen Netzes über ein
längeren Zeitraum aufrechtzuerhalten ist - dies kann sowohl für die Versorgung von IT-
Anlagen als auch der Infrastruktur gelten - , ist eine zentrale Notstromversorgung vorzus
Diese wird in der Regel als Diesel-Notstrom-Aggregat realisiert.

INF 3.4 Lokale unterbrechungsfreie Stromversorgung

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

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

Zwei Arten der USV sind zu unterscheiden:

* Off-Line-USV: Hierbei werden die angeschlossenen Verbraucher im Normalfall direkt aus dem Stromversorgungsnetz gespeist. Erst wenn dieses ausfällt, schaltet sich die USV selbsttätig zu und übernimmt die Versorgung.
* On-Line-USV: Hier ist die USV ständig zwischen Netz und Verbraucher geschaltet. Die gesamte Stromversorgung läuft immer über die USV.

Beide USV-Arten können neben der Überbrückung von Totalausfällen der Stromversorgung
und Unterspannungen auch dazu dienen, Überspannungen zu glätten.

Bei der Dimensionierung einer USV kann man i. d. R. von einer üblichen Überbrückungszeit
von ca. 10 bis 15 Minuten ausgehen. Die Mehrzahl aller Stromausfälle ist innerhalb von 5
10 Minuten behoben, so dass nach Abwarten dieser Zeitspanne noch 5 Minuten übrig bleiben,
um die angeschlossene IT geordnet herunterfahren zu können, sollte der Stromausfall länge
andauern. Die meisten modernen USV-Geräte bieten Rechnerschnittstellen an, die nach einer
vorher festgelegten Zeit, entsprechend dem Zeitbedarf der IT und der Kapazität der USV, e
rechtzeitiges automatisches Herunterfahren (Shut-down) einleiten können. Für spezielle
Anwendungsfälle (z.B. TK-Anlagen) kann die erforderliche Überbrückungszeit auch mehrere
Stunden betragen.

Um die Schutzwirkung aufrechtzuerhalten, ist eine regelmäßige Wartung der USV
vorzusehen.

Falls die Möglichkeit besteht, die Stromversorgung unterbrechungsfrei aus einer anderen Quelle zu beziehen (z.B. durch Anschluss an eine zentrale USV), so stellt dies eine Alternative zur lokalen USV dar.

Weiters ist zu beachten:

* Die USV ist regelmäßig entsprechend den Angaben des Herstellers zu warten.
* Die Wirksamkeit der USV ist regelmäßig zu testen.
* Im Falle von Veränderungen ist zu überprüfen, ob die vorgehaltene Kapazität der USV noch ausreichend ist.

INF 3.5 Blitzschutzeinrichtungen (Äußerer Blitzschutz)

Die direkten Auswirkungen eines Blitzeinschlages auf ein Gebäude (Beschädigung der Bausubstanz, Dachstuhlbrand u.ä.) lassen sich durch die Installation einer Blitzschutzan verhindern. Über diesen "Äußeren Blitzschutz" hinaus ist fast zwingend der "Innere Blitzschutz", der Überspannungsschutz, erforderlich. Denn der äußere Blitzschutz schützt elektrischen Betriebsmittel in Gebäuden nicht. Dies ist nur durch einen Überspannungsschutz möglich (siehe dazu *INF 3.6 Überspannungsschutz (Innerer Blitzschutz)*, dessen hohe Kosten dem Schutzgut gegenüber gerechtfertigt sein müssen).

INF 3.6 Überspannungsschutz (Innerer Blitzschutz)

Je nach Qualität und Ausbau des Versorgungsnetzes des Energieversorgungsunternehmens und des eigenen Stromleitungsnetzes, abhängig vom Umfeld (andere Stromverbraucher) und von der geographischen Lage, können durch Induktion oder Blitzschlag Überspannungsspitzen im Stromversorgungsnetz entstehen. Überspannungen durch Blitz haben i.d.R. ein recht hohes zerstörerisches Potential, während Überspannungen anderer Ursachen geringer sind, aber trotzdem ausreichen können, um Mikroelektronikgeräte zu stören oder zu zerstören.

Der Überspannungsschutz wird in der Regel in drei voneinander abhängigen Stufen aufgebaut:

* Grobschutz:
  Geräte für den Grobschutz vermindern Überspannungen, wie sie durch direkten Blitzschla entstehen, und begrenzen sie auf ca. 6000V. Für die Auswahl des Grobschutzes ist es bedeutend, ob ein äußerer Blitzschutz vorhanden ist oder nicht.
* Mittelschutz:
  Der Mittelschutz begrenzt die verbleibende Überspannung auf ca. 1500 V und ist auf die Vorschaltung eines Grobschutzes angewiesen.

* Feinschutz:
  Geräte für den Feinschutz senken Überspannungen so weit herab, dass sie auch für empfindliche Bauteile mit Halbleiterbauelementen ungefährlich sind.

Weiters ist zu beachten:

* Blitz- und Überspannungsschutzeinrichtungen sollten periodisch und nach bekannten Ereignissen geprüft und ggf. 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.

INF 3.7 Schutz gegen elektromagnetische Einstrahlung

Die Funktion informationstechnischer Geräte kann durch die elektromagnetische Strahlung benachbarter Einrichtungen beeinträchtigt werden. Mögliche Ursachen für solche Störstrahlungen sind Radarstrahlung, Rundfunk- und Fernsehsender, Richtfunkanlagen, Hochspannungsleitungen, Maschinen, von denen elektromagnetische Störungen ausgehen können (Schweißgeräte, Anlagen mit starken Elektromotoren, usw.) oder atmosphärische Entladungen.

So weit möglich, sollten solche Störquellen bereits bei der Planung berücksichtigt bzw. ausgeschaltet werden. Als nachträgliche Maßnahmen bleiben etwa:

* die Verwendung von Schutzschränken mit speziellen Filtern und Türdichtungen oder
* die Abschirmung durch beschichtete Wände.

INF 3.8 Schutz gegen kompromittierende Abstrahlung

Überall dort, wo Information elektronisch übertragen, verarbeitet oder dargestellt wird, ist die Gefahr der kompromittierenden Abstrahlung gegeben. Bildschirme, Tastaturen, Drucker, Modems, Graphikkarten, LAN-Komponenten, Fax-Geräte und ähnliche Geräte geben elektromagnetische Wellen ab, die noch in einer Entfernung von mehreren Metern - bei Monitoren bis zu mehreren hundert Metern - aufgefangen und analysiert werden können. In der Nähe befindliche führende Leitungen (Heizkörper, Wasserleitungen,...) können diese Abstrahlung beträchtlich verstärken.

Abwehrmaßnahmen:

Möglichkeiten, den Verlust der Vertraulichkeit von Daten durch kompromittierende Abstrahlung zu verhindern, sind etwa:

* Auswahl des Standortes (innerhalb eines Gebäudes):
  Bereits eine geeignete Aufstellung von IT-Komponenten, die entsprechend vertrauliche Daten verarbeiten oder übertragen und bei denen die Gefahr einer kompromittierenden Abstrahlung besteht, kann das potentielle Risiko durch kompromittierende Abstrahlung in erheblichem Maße verringern.
  So sollten, so weit baulich, technisch und organisatorisch möglich, potentiell gefährdete Komponenten in Räumen untergebracht werden, die möglichst weit entfernt von Straßenfronten und Gebäuden mit Fremdfirmen sind. Weiters ist eine Aufstellung in der Nähe von

Fronten und Gebäuden mit Fremdfirmen sind. Weiters ist eine Aufstellung in der Nähe von führenden Leitungen (Heizungsrohre, Heizkörper, Wasserleitungen,...) zu vermeiden.

* Schirmung von Geräten:
Diese erfolgt durch die Verwendung spezieller Materialien. Solche abstrahlsichere Hardware-Komponenten werden in Anlehnung an den englischen Fachausdruck meist als "tempest-proof" oder "tempest-gehärtet" bezeichnet. Dabei steht TEMPEST für "Temporary Emission and Spurious Transmission" (befristete Ausstrahlung und unberechtigte Übermittlung).

* Schirmung von Räumen und Gebäuden:
Anstelle eines Schutzes auf Geräteebene ist - bei entsprechenden Gegebenheiten - auch ein Schutz auf Raum- oder Gebäudeebene möglich. Dabei werden Wände, Böden und Decken entsprechend abgeschirmt. Auch Spezialglas, das mit einem transparenten Metallfilm beschichtet ist, wird am Markt angeboten, da selbstverständlich Fenster in den Schutz miteinzubeziehen sind. Eine Raumschirmung schützt im Allgemeinen auch gegen Störstrahlung von außen.

* Überlagerung der kompromittierenden Abstrahlung:
Durch Senden von Störddaten in einer bestimmten Frequenzbreite können die Emissionen der DV-Geräte überlagert werden.

INF 3.9 Schutz gegen elektrostatische Aufladung

Elektrostatische Aufladungen können Schäden an Bauteilen, Programmstörungen oder Datenverluste verursachen. Aus diesem Grund wird für Komponenten, die in ungeschützter Umgebung eingesetzt werden, eine relativ hohe Widerstandsfähigkeit gegen elektrostatische Aufladung gefordert.

Zieht man allerdings in Betracht, dass abhängig von Bodenbeschaffenheit - hier stellen insbesondere Teppichböden eine Gefahrenquelle dar - und Schuhwerk die elektrostatische Aufladung von gehenden Personen 10 kV und mehr betragen kann, so zeigt sich die Notwendigkeit von Maßnahmen zur Vermeidung und Eliminierung elektrostatischer Aufladungen.

Solche Maßnahmen sind etwa:

* die Gewährleistung einer relativen Luftfeuchtigkeit von mindestens 50%,
* die Verwendung geeigneter Werkstoffe (Bodenbeläge,...),
* Erdungsmaßnahmen,
* der Einsatz von Antistatikmitteln.

1.4 Leitungsführung

INF 4.1 Lagepläne der Versorgungsleitungen

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

* genaue Führung der Leitungen (Einzeichnung in bemaßte Grundriss- und Lagepläne),
* genaue technische Daten (Typ und Abmessung),
* evtl. vorhandene Kennzeichnung,
* Nutzung der Leitungen (Nennung der daran angeschlossenen Netzteilnehmer, so weit

- möglich und zweckmäßig),
- Gefahrenpunkte und
- vorhandene und zu prüfende Schutzmaßnahmen.

Es muss möglich sein, sich anhand der Pläne einfach und schnell ein genaues Bild der Situation zu machen. Nur so kann das Risiko, dass Leitungen bei Arbeiten versehentlich beschädigt werden, auf ein Mindestmaß reduziert werden. Eine Schadstelle ist schneller zu lokalisieren, die Störung schneller zu beheben.

Weiters ist zu beachten:

- Alle Arbeiten an Leitungen sind rechtzeitig und vollständig zu dokumentieren.
- Die Pläne sind gesichert aufzubewahren, der Zugriff darauf ist zu regeln, da sie schützenswerte Informationen beinhalten.
- Die Verantwortlichkeiten für Aktualisierung und Aufbewahrung der Pläne sind festzulegen.

Vgl. dazu auch *ENT 2.4 Dokumentation und Kennzeichnung der Verkabelung*.

INF 4.2 Materielle Sicherung von Leitungen und Verteilern

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

- Verlegung der Leitungen unter Putz,
- Verlegung der Leitungen in Stahlpanzerrohr,

- Verlegung der Leitungen in mechanisch festen und abschließbaren Kanälen,
- Verschluss von Verteilern und
- bei Bedarf zusätzlich elektrische Überwachung von Verteilern und Kanälen.

Bei Verschluss sind Regelungen zu treffen, die die Zutrittsrechte, die Verteilung der Schlüssel und die Zugriffsmodalitäten festlegen.

Weiters sollte bei der Verlegung von Leitungen auch auf den Nagetierschutz Bedacht genommen werden.

INF 4.3 Entfernen oder Kurzschließen und Erden nicht benötigter Leitungen

Nicht mehr benötigte Leitungen sollten nach Möglichkeit entfernt werden. Ist dies auf Grund der damit verbundenen Beeinträchtigung des Dienstbetriebes (Öffnen von Decken, Fensterbank- und Fußbodenkanälen) nicht möglich, sind folgende Maßnahmen sinnvoll:

- Kennzeichnen der nicht benötigten Leitungen in der Revisionsdokumentation und Löschen der Eintragungen in der im Verteiler befindlichen Dokumentation,
- Auftrennen aller Rangierungen und Verbindungen der freien Leitungen in den Verteilern (so weit möglich),
- Kurzschließen der freien Leitungen an beiden Kabelenden und in allen berührten Verteilern,
- Auflegen der freien Leitungen auf Erde (Masse) an beiden Kabelenden und in allen berührten Verteilern; bei dadurch entstehenden Masse-Brumm-Schleifen ist nur einseitig zu erden,
- Gewährleisten, dass nicht mehr benötigte Leitungen bei ohnehin anstehenden Arbeiten im

* Gewährleisten, dass nicht mehr benötigte Leitungen bei ohnehin anstehenden Arbeiten im Netz entfernt werden.

INF 4.4 Auswahl geeigneter Kabeltypen

Bei der Auswahl von Kabeln ist neben der Berücksichtigung von übertragungstechnischen Anforderungen und Umfeldbedingungen auch die Frage nach den Sicherheitsanforderungen zu stellen.

Herkömmliche Kupferleitungen bieten ein potentielles Ziel für aktive und passive Angriffe. Abhilfe kann hier entweder die Verwendung mehrfach geschirmter Leitungen oder der Einsatz von Lichtwellenleitern bringen.

Lichtwellenleiter sind unempfindlich gegen elektrische und elektromagnetische Störungen und bieten Schutz gegen (aktives und passives) Wiretapping auf der Leitung. Ein potentielles

Angriffsziel stellen aber die Schnittstellen (etwa Verstärker) dar, hier sind bei Bedarf entsprechende Schutzvorkehrungen zu treffen.

INF 4.5 Schadensmindernde Kabelführung

Bei der Planung von Kabeltrassen ist darauf zu achten, dass erkennbare Gefahrenquellen umgangen werden. Grundsätzlich sollen Trassen nur in den Bereichen verlegt werden, die ausschließlich dem Benutzer zugänglich sind. Ein übersichtlicher Aufbau der Trassen erleichtert die Kontrolle. Trassen und einzelne Kabel sollen immer so verlegt werden, das vor direkten Beschädigungen durch Personen, Fahrzeuge und Maschinen geschützt sind.

Der Standort von Geräten sollte so gewählt werden, dass Kabel nicht im Lauf- oder Fahrbereich liegen. Ist dies nicht zu vermeiden, sind die Kabel den zu erwartenden Belastungen entsprechend durch geeignete Kanalsysteme zu schützen.

In Tiefgaragen ist darauf zu achten, dass nicht durch Trassen im Fahrbereich die zulässig Fahrzeughöhe unterschritten wird, und dass Fremdpersonen keinen unautorisierten Zugriff z den in der Regel in geringer Deckenhöhe verlaufenden Trassen erhalten.

Bei gemeinsam mit Dritten genutzten Gebäuden ist darauf zu achten, dass Kabel nicht in Fu bodenkanälen durch deren Bereiche führen. Fußboden- und Fensterbank-Kanalsysteme sind gegenüber den fremdgenutzten Bereichen mechanisch fest zu verschließen. Besser ist es, si an den Bereichsgrenzen enden zu lassen.

Bereiche mit hoher Brandgefahr sind zu meiden. Ist dies nicht möglich und ist der Betrieb erhalt aller auf der Trasse liegenden Kabel erforderlich, ist der entsprechende Trassenbe mit Brandabschottung zu versehen. Ist der Betriebserhalt nur für einzelne Kabel erforder ist dafür ein entsprechendes Kabel zu wählen.

In Produktionsbetrieben ist mit hohen induktiven Lasten und daraus resultierenden Störfel zu rechnen. Auch diese sind bei der Trassen- und Kabelverlegung zu berücksichtigen. Für d Schutz der Kabel gilt sinngemäß das Gleiche wie bei der Brandabschottung.

Bei Erdtrassen ist ca. 10 cm über der Trasse ein Warnband zu verlegen. Bei einzelnen Kabe

Bei Erdtrassen ist ca. 10 cm über der Trasse ein Warnband zu verlegen. Bei einzelnen Kab
(ohne Rohr) ist der Einbau von Kabelabdeckungen sinnvoll.

INF 4.6 Vermeidung von wasserführenden Leitungen

In Räumen oder Bereichen, in denen sich IT-Geräte mit zentralen Funktionen (z.B. Server)
befinden, sollten wasserführende Leitungen aller Art vermieden werden. Die einzigen wass

---

führenden Leitungen sollten, wenn unbedingt erforderlich, Kühlwasserleitungen, Löschwasserleitungen und Heizungsrohre sein. Zuleitungen zu Heizkörpern sollten mit Absperrventilen, möglichst außerhalb des Raumes/Bereiches, versehen werden. Außerhalb der Heizperiode sind diese Ventile zu schließen.

Sind Wasserleitungen unvermeidbar, kann als Minimalschutz eine Wasserauffangwanne oder -rinne unter der Leitung angebracht werden, deren Ablauf außerhalb des Raumes führt. Günstig ist es, dazu den Flur zu nutzen, da so ein eventueller Leitungsschaden früher ent wird.

Optional können Wassermelder mit automatisch arbeitenden Magnetventilen eingebaut werden. Diese Magnetventile sind außerhalb des Raumes/Bereiches einzubauen und müssen stromlos geschlossen sein.

Als zusätzliche oder alternative Maßnahme empfiehlt sich ggf. eine selbsttätige Entwässer
(*INF 6.8 Selbsttätige Entwässerung*).

1.5 Geeignete Aufstellung und Aufbewahrung

Bei der Aufstellung eines IT-Systems sind verschiedene Voraussetzungen zu beachten, die d Sicherheit des Systems gewährleisten bzw. erhöhen sollen. Über diese Sicherheitsaspekte, naturgemäß den Schwerpunkt des vorliegenden Handbuches bilden, hinaus sollen durch eine geeignete Aufstellung auch die Lebensdauer und Zuverlässigkeit der Technik sowie die Ergonomie des Systems verbessert werden.

Im Folgenden werden generelle Hinweise für die Aufstellung von IT-Systemen und Komponenten gegeben, wie sie für die mittlere Datenverarbeitung typisch sind. Dabei wird unterschieden zwischen:

* Arbeitsplatz-IT-Systemen (PCs, Notebooks, Telearbeitsplätze,..)
* Server (neben Datenbankservern, Kommunikationsservern, etc. sind davon auch Telekommunikationsanlagen umfasst)
* Netzwerkkomponenten (z.B. Modems, Router, Verteilerschränke,...)

Wie für das gesamte Handbuch zutreffend und bereits in der Einleitung ausgeführt, wird au hier nicht auf den Bereich des klassischen Rechenzentrums eingegangen, da hier im Allgemeinen sehr produkt- und herstellerspezifische Anforderungen bestehen und diese zudem über die Maßnahmen für den mittleren Schutzbedarf hinausgehen und damit den Rahmen der vorliegenden Arbeit sprengen würden.

Es ist festzuhalten, dass eine generelle Klassifikation aller IT-Komponenten in eine der genannten Gruppen nicht möglich ist. So kann ein Fax etwa als Stand-alone-Gerät betrachte

werden, oder aber als Teil eines Arbeitsplatz-IT-Systems, falls die Möglichkeit besteht, Fax direkt vom PC zu versenden.

Die unten angeführten Maßnahmen sind daher als allgemeine Hinweise zu verstehen, die auf die Bedürfnisse des speziellen Falles abzubilden sind.

INF 5.1 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 Her stellern festgeschriebenen Vorgaben und Hinweisen sowie ergonomischen Gesichtspunkten - unter anderem folgende Voraussetzungen beachtet werden:

* der Standort in der Nähe eines Fensters oder einer Tür erhöht die Gefahr des Beobachte von außerhalb,
* das System sollte nicht in unmittelbarer Nähe der Heizung aufgestellt werden (Vermeidung von Überhitzung, aber auch kompromittierender Abstrahlung, vgl. *INF 5.8 Schutz gegen kompromittierende Abstrahlung*),
* das System sollte so weit möglich und erforderlich, physisch gesichert sein (Diebstahlschutz, versperrbare Diskettenlaufwerke, ...).

INF 5.2 Geeignete Aufstellung eines Servers

Unter Servern sind in diesem Zusammenhang etwa Datenbank-, Programm- und Kommunikationsserver, aber auch TK-Anlagen zu verstehen.

Um Vertraulichkeit, Integrität und Verfügbarkeit im Betrieb von Servern sicherzustellen, es zwingend erforderlich, diese in einer gesicherten Umgebung aufzustellen.

Diese kann realisiert werden als:

* Serverraum (vgl. *INF 5.6 Serverräume*)
  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.

* Serverschrank, wenn kein separater Serverraum zur Verfügung steht (vgl. *INF 5.7 Beschaffung und Einsatz geeigneter Schutzschränke*).
  Serverschränke dienen zur Unterbringung von IT-Geräten und sollen den Inhalt sowohl

gegen unbefugten Zugriff als auch gegen die Einwirkung von Feuer oder schädigenden Stoffen (Staub, Gase,...) schützen.

Details zu den technischen und organisatorischen Sicherheitsmaßnahmen bei Serverräumen und Serverschränken finden sich in *INF 5.6 Serverräume* und *INF 5.7 Beschaffung und Einsatz geeigneter Schutzschränke*

Generell ist zu beachten:

* Der Zugang und Zugriff zu Servern darf ausschließlich autorisierten Personen möglich sein.
* Eine Vertretungsregelung muss sicherstellen, dass der Zugriff zum Server auch im Vertretungsfall geregelt möglich ist, und unautorisierte Zugriffe auch in Ausnahmesituati nicht vorkommen können.

INF 5.3 Geeignete Aufstellung aktiver Netzwerkkomponenten

Unter aktiven Netzwerkkomponenten sind beispielsweise Modems, Router und Verteilerschränke zu verstehen.

Um den Missbrauch von Netzwerkkomponenten zu verhindern, muss sichergestellt werden, dass nur Berechtigte physikalischen Zugriff darauf haben. So bedeutet etwa der Missbrauch eines Modems zum einem die Durchführung unbefugter Datenübertragungen, durch die Kosten verursacht, Viren eingeschleppt oder Interna nach außen transferiert werden können zum anderen das unbefugte Ändern oder Auslesen der Modem-Konfiguration, wodurch Sicherheitslücken entstehen können.

Steht ein Modem direkt an einem Arbeitsplatz-IT-System zur Verfügung, so ist der physikalische Zugriff darauf abzusichern (z.B. durch Versperren des Raumes, vgl. auch *INF 5.1 Geeignete Aufstellung eines Arbeitsplatz-IT-Systems*).

Wenn über ein Modem oder einen Modempool Zugänge zum internen Netz geschaffen werden, ist darauf zu achten, dass keine Umgehung einer bestehenden Firewall geschaffen wird. Sollen mit einem Modempool weitere externe Zugänge zu einem durch eine Firewall geschützten Netz geschaffen werden, muss dieser auf der unsicheren Seite der Firewall aufgestellt werden.

Netzwerkkomponenten sollten wie Server in einem gesicherten Serverraum oder einem Schutzschrank aufgestellt sein. Die entsprechenden Maßnahmen aus *INF 5.6 Serverräume* und *INF 5.7 Beschaffung und Einsatz geeigneter Schutzschränke* sind zu beachten.

Auch hier ist sicherzustellen:

* Der Zugang und Zugriff zu Netzwerkkomponenten darf ausschließlich autorisierten Personen möglich sein.
* Eine Vertretungsregelung muss sicherstellen, dass der Zugriff zu Netzwerkkomponenten auch im Vertretungsfall geregelt möglich ist und unautorisierte Zugriffe auch in Ausnahmesituationen nicht vorkommen können.

INF 5.4 Nutzung und Aufbewahrung mobiler IT-Geräte

Unter mobilen IT-Geräten sind alle für einen mobilen Einsatz geeigneten Geräte zu verstehen, so etwa Notebooks, Palmtops, Handhelds und Personal Assistants.

Da die Umfeldbedingungen bei mobilem Einsatz meist außerhalb der direkten Einflussnahme des Benutzers liegen, muss er versuchen, mobile IT-Geräte auch außer Haus sicher aufzubewahren. Hierfür können nur einige Hinweise gegeben werden, die bei der mobilen Nutzung zu beachten sind:

* Die Benutzer mobiler IT-Geräte sind über die potentiellen Gefahren bei Mitnahme und Nutzung eines solchen Gerätes außerhalb der geschützten Umgebung eingehend zu informieren und zu sensibilisieren. So weit möglich sollten solche Informationen in schriftlicher Form - etwa als Merkblätter - an die Mitarbeiter verteilt werden. Dabei ist auch auf die besonderen Gegebenheiten in verschiedenen Zielgebieten und in speziellen Situationen (etwa bei einer besonders eingehenden Zollkontrolle) hinzuweisen.
* Werden auf mobilen IT-Geräten vertrauliche, geheime und/oder sensible Daten (Definitionen s. Teil 1, Kapitel 2.2.4 dieses Handbuches ([KIT S01])) gespeichert und verarbeitet, so ist die Installation eines Zugriffsschutzes (über Passwort oder Chipkarte) sowie einer Festplatten- oder Dateiverschlüsselung dringend zu empfehlen (vgl. auch *SYS 5.5 Einsatz eines Verschlüsselungsproduktes für Arbeitsplatzsysteme*).
* So weit möglich, sollten auch Disketten und Streamerbänder ausschließlich chiffrierte Daten enthalten; werden in Ausnahmefällen unverschlüsselte Disketten oder Streamerbänder im mobilen Einsatz verwendet, so sollten diese keinesfalls unbeaufsichtigt (etwa im Hotel oder in einem Wagen) zurückgelassen werden.
* Nach Möglichkeit sollten die Zeiten, in denen das Gerät unbeaufsichtigt bleibt, minimiert werden.
* Werden mobile IT-Geräte in einem Kraftfahrzeug aufbewahrt, so sollte das Gerät von außen nicht sichtbar sein. Das Abdecken des Gerätes oder das Einschließen in den Kofferraum bieten Abhilfe.
* Wird ein mobiles IT-Gerät in fremden Büroräumen vor Ort benutzt, so ist dieser Raum nach Möglichkeit auch bei kurzzeitigem Verlassen zu verschließen. Wird der Raum für längere Zeit verlassen, sollte zusätzlich das Gerät ausgeschaltet werden, um über das Bootpasswort die unerlaubte Nutzung zu verhindern.
* In Hotelräumen sollte ein mobiles IT-Gerät nicht offen ausliegen. Das Verschließen des Gerätes in einem Schrank behindert Gelegenheitsdiebe.

---

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

INF 5.5 Sichere Aufbewahrung der Datenträger vor und nach Versand

Vor dem Versand eines Datenträgers ist zu gewährleisten, dass für den Zeitraum zwischen dem Speichern der Daten auf dem Datenträger und dem Transport ein ausreichender Zugriffsschutz besteht. Beschriebene Datenträger sollten bis zum Transport in entsprechenden Behältnissen (Schrank, Tresor) verschlossen aufbewahrt werden. Die für den Transport oder für die Zustellung Verantwortlichen (z.B. Poststelle) sind auf die sachgerechte und sichere Aufbewahrung und Handhabung von Datenträgern hinzuweisen.

Alternativ oder ergänzend kann auch eine verschlüsselte Speicherung der Daten vorgenommen werden.

Weitere Maßnahmen dazu finden sich in Kapitel 0.

INF 5.6 Serverräume

Ein Serverraum dient zur Unterbringung eines oder mehrerer Server sowie serverspezifischer Unterlagen. Darüber hinaus können dort auch Datenträger (in kleinerem Umfang) sowie zusätzliche Hardware, wie etwa Protokolldrucker oder Klimatechnik, vorhanden sein.

Im Serverraum ist kein ständig besetzter Arbeitsplatz eingerichtet, er wird nur sporadisch und zu kurzfristigen Arbeiten betreten. Zu beachten ist jedoch, dass im Serverraum auf Grund der Konzentration von IT-Geräten und Daten ein deutlich höherer Schaden eintreten kann als beispielsweise in einem Büroraum.

Für den Schutz von Serverräumen sind die entsprechenden baulichen und infrastrukturellen Maßnahmen, die im vorliegenden Kapitel 1 beschrieben werden, zur Anwendung zu bringen. Besondere Beachtung ist dabei folgenden Maßnahmen zu widmen:

* INF 1.4 Zutrittskontrolle
* INF 2.2 Raumbelegung unter Berücksichtigung von Brandlasten
* INF 2.6 Handfeuerlöscher
* INF 2.8 Rauchverbot
* INF 3.2 Not-Aus-Schalter
* INF 3.4 Lokale unterbrechungsfreie Stromversorgung
* INF 3.6 Überspannungsschutz (Innerer Blitzschutz)
* INF 4.6 Vermeidung von wasserführenden Leitung

---

* INF 6.4 Geschlossene Fenster und Türen
* INF 6.5 Alarmanlage
* INF 6.6 Fernanzeige von Störungen
* INF 6.7 Klimatisierung
* PER 2.3 Beaufsichtigung oder Begleitung von Fremdpersonen

INF 5.7 Beschaffung und Einsatz geeigneter Schutzschränke

Schutzschränke können ihren Inhalt gegen die Einwirkung von Feuer bzw. gegen unbefugten Zugriff schützen. Je nach angestrebter Schutzwirkung sind bei der Auswahl geeigneter Schutzschränke folgende Hinweise zu beachten:

* Schutz gegen Feuereinwirkung:
  Bei Schutzschränken unterscheidet man bezüglich Schutz gegen Feuereinwirkung die Güteklassen S60 und S120 nach ÖNORM EN 1047-1 . In diesen Güteklassen werden die Schutzschränke darauf geprüft, ob in ihnen bis zu einer Beflammungszeit von 60 bzw. 120 Minuten während eines normierten Testes für die geschützten Datenträger verträgliche Temperaturen erhalten bleiben. Durch Zusätze in der Klassifizierung werden die zu schützenden Datenträger bezeichnet. Die Kürzel bedeuten im Einzelnen:
  * P = Papier aller Art
  * D = Datenträger (z.B. Magnetbänder, Filme)
  * DIS = Disketten, Magnetbandkassetten einschließlich aller anderen Datenträger.
  * Die Unterschiede zwischen den Klassen liegen in der Isolationsleistung, die bei DIS-Schränken am höchsten ist.

  Für den IT-Grundschutz sollten bei Schutz gegen Feuer Schutzschränke der Güteklasse

* S60 ausreichend sein. Zu beachten bleibt, dass solche Schränke damit Schutz gegen Feuer für einen gewissen Zeitraum bieten, so dass Datenträger nicht zerstört werden, jedoch ist davon auszugehen, dass im Brandfall der Betrieb eines in einem Serverschrank untergebrachten Servers nicht aufrechterhalten werden kann.
* Bei Schutzschränken, die zum Schutz vor Feuer und Rauch dienen, sollte eine Vorrichtung zum automatischen Schließen der Türen im Brandfall vorgesehen werden. Die Schließung sollte lokal durch Rauchgasmelder und/oder extern durch ein Signal einer Brandmeldeanlage (soweit vorhanden) ausgelöst werden können.

* Schutz gegen unbefugten Zugriff:
Der Schutzwert gegen unbefugten Zugriff wird neben der mechanischen Festigkeit des Schutzschrankes entscheidend durch die Güte des Schlosses beeinflusst. Für den IT-Grundschutz sollten Wertschränke nach RAL-RG 627 [3] geeignet sein.
Sind Zugriffsschutz und Brandschutz in Kombination erforderlich, so können Datensicherungsschränke nach RAL-RG 626/9 verwendet werden.

Weitere relevante Normen und Informationen sind VDMA 24992 für Stahlschränke und RAL-RG 627 für Wertschränke. Hilfestellung bei der Bewertung des Widerstandswertes

3 RAL Deutsches Institut für Gütesicherung und Kennzeichnung e.V. Bonn

---

verschiedener Schutzschränke gibt das VDMA-Einheitsblatt 24990, in dem Sicherheitsmerkmale von Schutzschränken kurz beschrieben werden.

Bei der Auswahl von Schutzschränken ist auch die zulässige Deckenbelastung am Aufstellungsort zu berücksichtigen. Schutzschränke, die auf Grund ihrer geringen Größe relativ einfach weggetragen werden könnten, sollten in der Wand oder im Boden verankert werden.

Nach diesen Auswahlkriterien für den Schutzwert des Schutzschrankes ist als Nächstes die Ausstattung des Schrankes bedarfsgerecht festzulegen. Dazu sollte vor der Beschaffung ei Schutzschrankes festgelegt werden, welche Geräte bzw. welche Arten von Datenträgern in ihm aufbewahrt werden sollen. Die Innenausstattung des Schutzschrankes ist dieser Festlegung angemessen auszuwählen. Nachrüstungen sind in der Regel schwierig, da der Schutzwert des Schrankes und seine spezifische Zulassung beeinträchtigt werden können. Es sollte auch Raum für zukünftige Erweiterungen mit eingeplant werden.

Serverschränke:
Schutzschränke, in denen wichtige IT-Komponenten (also im Regelfall Server) untergebracht sind, werden auch als Serverschränke bezeichnet. In diesen sollte außer für den Server ur eine Tastatur auch Platz für einen Bildschirm und weitere Peripheriegeräte wie z.B. Bandlaufwerke vorgesehen werden, damit Administrationsarbeiten vor Ort durchgeführt werden können. Dazu ist zu beachten, dass die Ausstattung ergonomisch gewählt ist, damit Administrationsarbeiten am Server ungehindert durchgeführt werden können. So ist zum Beispiel ein ausziehbarer Boden für die Tastatur wünschenswert, der in einer Höhe angebra wird, dass der Administrator seine Arbeiten sitzend durchführen kann. Je nach Nutzung des Schrankes können auch eine Klimatisierung und/oder eine USV-Versorgung erforderlich sein. Die entsprechenden Geräte sollten dann im Schrank mit untergebracht werden. Andernfalls muss zumindest eine Lüftung vorhanden sein. Die Ausstattung des Schrankes mit einem lokal arbeitenden Brandfrüherkennungssystem, das im Brandfall die Stromzufuhr der Geräte unterbricht (auf der Eingangs- und Ausgangsseite der USV, sofern diese vorhanden ist), ist empfehlenswert.

Nicht im gleichen Schrank untergebracht werden sollten Backup-Datenträger und Protokolldrucker. Backup-Datenträger würden im Falle einer Beschädigung des Servers vermutlich

ebenfalls beschädigt. Die Protokollierung der Aktionen am Server dient auch zur Kontrolle des Administrators. Es ist also nicht sinnvoll, ihm, ggf. sogar als Einzigem, Zugriff auf Protokollausdrucke zu gewähren.

Verschluss von Schutzschränken:
Generell sind Schutzschränke bei Nichtbenutzung zu verschließen. Werden Arbeiten, die ein Öffnen des Schutzschrankes erfordern, unterbrochen, so ist auch bei kurzfristigem Verlass des Raumes der Schutzschrank zu verschließen.

Werden Schutzschränke mit mechanischen oder elektronischen Codeschlössern verwendet, so muss der Code für diese Schlösser geändert werden:

* nach der Beschaffung,
* bei Wechsel des Benutzers,
* nach Öffnung in Abwesenheit des Benutzers,
* wenn der Verdacht besteht, dass der Code einem Unbefugten bekannt wurde und
* mindestens einmal alle zwölf Monate.

Der Code darf nicht aus leicht zu ermittelnden Zahlen (z.B. persönliche Daten, arithmetis Reihen) bestehen.

Die jeweils gültigen Codes von Codeschlössern sind aufzuzeichnen und gesichert zu hinterlegen. Zu beachten ist, dass eine Hinterlegung im zugehörigen Schutzschrank sinnlos ist.

Wenn der Schutzschrank neben einem Codeschloss ein weiteres Schloss besitzt, so ist abzuwägen, ob Code und Schlüssel gemeinsam hinterlegt werden, was im Notfall einen schnelleren Zugriff erlauben würde, oder getrennt hinterlegt werden, so dass es für einen Angreifer schwieriger ist, sich Zugriff zu verschaffen.

1.6 Weitere Schutzmaßnahmen

INF 6.1 Einhaltung einschlägiger Normen und Vorschriften

Für nahezu alle Bereiche der Technik gibt es Normen bzw. Vorschriften, z.B. der ÖNORM und des ÖVE. Diese Regelwerke tragen dazu bei, dass technische Einrichtungen ein ausreichendes Maß an Schutz für den Benutzer und Sicherheit für den Betrieb gewährleisten. B der Planung und Errichtung von Gebäuden, bei deren Umbau, beim Einbau technischer Gebäudeausrüstungen (z.B. interne Versorgungsnetze wie Telefon- oder Datennetze) und bei Be schaffung und Betrieb von Geräten sind entsprechende Normen und Vorschriften unbedingt zu beachten.

In Anhang A werden einige dieser Normen beispielhaft angeführt.

INF 6.2 Regelungen für Zutritt zu Verteilern

Die Verteiler (z.B. für Energieversorgung, Datennetze, Telefon) sind nach Möglichkeit in Räumen für technische Infrastruktur unterzubringen. Die dort geforderten Maßnahmen sind

Räumen für technische Infrastruktur unterzubringen. Die dort geforderten Maßnahmen sind z
berücksichtigen.

Der Zutritt zu den Verteilern aller Versorgungseinrichtungen (Strom, Wasser, Gas, Telefo
Gefahrenmeldung, Rohrpost etc.) im Gebäude muss möglich und geordnet sein.

Mit möglich ist gemeint, dass

* Verteiler nicht bei Malerarbeiten mit Farbe oder Tapeten so verklebt werden, dass sie noch mit Werkzeug zu öffnen oder unauffindbar sind,
* Verteiler nicht mit Möbeln, Geräten, Paletten etc. zugestellt werden,
* für verschlossene Verteiler die Schlüssel verfügbar sind und die Schlösser funktionier

Mit geordnet ist gemeint, dass festgelegt ist, wer welchen Verteiler öffnen darf. Verteil
ten verschlossen sein und dürfen nur von den für die jeweilige Versorgungseinrichtung
zuständigen Personen geöffnet werden. Die Zugriffsmöglichkeiten können durch
unterschiedliche Schlüssel und entsprechende Schlüsselverwaltung geregelt werden (siehe
dazu *INF 1.4 Zutrittskontrolle*).

INF 6.3 Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile

Schützenswerte Gebäudeteile sind z.B. Rechenzentrum, Serverraum, Datenträgerarchiv,
Klimazentrale, Verteilungen der Stromversorgung, Schalträume, Ersatzteillager. Solche Be-
reiche sollten nach Möglichkeit keinen Hinweis auf ihre Nutzung tragen. Türschilder wie z
"Rechenzentrum" oder "EDV-Archiv" geben einem potentiellen Angreifer, der zum Gebäude
Zutritt hat, Hinweise, um seine Aktivitäten gezielter und damit erfolgversprechender vor-
bereiten zu können.

Ist es unvermeidbar, IT in Räumen oder Gebäudebereichen unterzubringen, die für Fremde
leicht von außen einsehbar sind (siehe auch *INF 1.2 Anordnung schützenswerter Gebäude-
teile*), so sind geeignete Maßnahmen zu treffen, um den Einblick zu verhindern oder so zu
gestalten, dass die Nutzung nicht offenbar wird. Dabei ist darauf zu achten, dass z.B. n
e i n Fenster einer ganzen Etage mit einem Sichtschutz versehen wird.

INF 6.4 Geschlossene Fenster und Türen

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

im Allgemeinen abgeschlossen werden. Dadurch wird verhindert, dass Unbefugte Zugriff auf darin befindliche Unterlagen und IT-Einrichtungen erlangen.

In manchen Fällen, z.B. in Großraumbüros, ist der Verschluss des Büros nicht möglich. In diesem Fall sollte alternativ jeder Mitarbeiter vor seiner Abwesenheit seine Unterlagen den persönlichen Arbeitsbereich verschließen: Schreibtisch, Schrank und PC (Schloss für Diskettenlaufwerk, Tastaturschloss), Telefon ("Clear Desk Policy").

Bei laufendem Rechner kann auf das Abschließen der Türen verzichtet werden, wenn eine Sicherungsmaßnahme installiert ist, mit der die Nutzung des Rechners nur unter Eingabe e Passwortes weitergeführt werden kann (passwortunterstützte Bildschirmschoner), der Bildschirm gelöscht wird und das Booten des Rechners die Eingabe eines Passwortes verlangt.

Bei ausgeschaltetem Rechner kann auf das Verschließen des Büros verzichtet werden, wenn die Inbetriebnahme des Gerätes die Eingabe eines Passwortes verlangt und sichergestellt dass keine schutzbedürftigen Gegenstände wie Unterlagen oder Datenträger offen ausliegen.

INF 6.5 Alarmanlage

Ist eine Alarmanlage für Einbruch oder Brand vorhanden und lässt sich diese mit vertretba Aufwand entsprechend erweitern, ist zu überlegen, ob zumindest die Kernbereiche der IT (Serverräume, Datenträgerarchive, Räume für technische Infrastruktur u. ä.) in die Überwachung durch diese Anlage mit eingebunden werden sollen. So lassen sich Gefährdungen wie Feuer, Einbruch, Diebstahl frühzeitig erkennen und Gegenmaßnahmen einleiten. Um die Schutzwirkung aufrechtzuerhalten, ist eine regelmäßige Wartung und Funktionsprüfung der Alarmanlage vorzusehen.

Ist keine Alarmanlage vorhanden oder lässt sich die vorhandene nicht nutzen, kommen als Minimallösung lokale Melder in Betracht. Diese arbeiten völlig selbstständig, ohne Anschl an eine Zentrale. Die Alarmierung erfolgt vor Ort oder mittels einer einfachen Zweidrahtleitung (evtl. Telefonleitung) an anderer Stelle.

Weiters ist zu beachten:

* Die Alarmanlage muss regelmäßig gewartet bzw. geprüft werden.
* Die zuständigen Personen sind über die im Alarmfall einzuleitenden Schritte zu unterrichten.

INF 6.6 Fernanzeige von Störungen

IT-Geräte und Supportgeräte, die keine oder nur seltene Bedienung durch eine Person erfo dern, werden oft in ge- und verschlossenen Räumen untergebracht (z.B. Serverraum). Das

führt dazu, dass Störungen, die sich in ihrem Frühstadium auf die IT noch nicht auswirker und einfach zu beheben sind, erst zu spät, meist durch ihre Auswirkungen auf die IT, entd werden. Feuer, Funktionsstörungen einer USV oder der Ausfall eines Klimagerätes seien als Beispiele für solche "schleichenden" Gefährdungen angeführt.

Durch eine Fernanzeige ist es möglich, solche Störungen früher zu erkennen. Viele Geräte, auf die man sich verlassen muss, ohne sie ständig prüfen oder beobachten zu können, haben heute einen Anschluss für Störungsfernanzeigen. Die technischen Möglichkeiten reichen dabei von einfachen Kontakten, über die eine Warnlampe eingeschaltet werden kann, bis zu Rechnerschnittstellen mit dazugehörigem Softwarepaket für die gängigen Betriebssysteme. Über die Schnittstellen ist es oft sogar möglich, jederzeit den aktuellen Betriebszustand angeschlossenen Geräte festzustellen und so Ausfällen rechtzeitig begegnen zu können.

INF 6.7 Klimatisierung

Um den zulässigen Betriebstemperaturbereich von IT-Geräten zu gewährleisten, reicht der normale Luft- und Wärmeaustausch eines Raumes manchmal nicht aus, so dass der Einbau einer Klimatisierung erforderlich wird. Deren Aufgabe ist es, die Raumtemperatur durch Kühlung unter dem von der IT vorgegebenen Höchstwert zu halten.

Werden darüber hinaus Forderungen an die Luftfeuchtigkeit gestellt, kann ein Klimagerät durch Be- und Entfeuchtung auch diese erfüllen. Dazu muss das Klimagerät allerdings an ei Wasserleitung angeschlossen werden. *INF 4.6 Vermeidung von wasserführenden Leitungen* ist zu beachten.

Darüber hinaus ist zu beachten, dass die Luftumwälzung durch eine Klimaanlage auch Emissionen aus der Umgebung in die Nähe von empfindlichen IT-Komponenten bringen kann. So ist etwa bei baulichen Maßnahmen, insbesondere bei Umbauarbeiten in bestehenden Räumen und Gebäuden, darauf zu achten, dass Kleber, Anstriche, etc. säurefrei sind, um ei Korrosion von IT-Bauteilen durch vorbeigeführte Luft aus der Klimaanlage zu vermeiden.

Um die Schutzwirkung aufrechtzuerhalten ist eine regelmäßige Wartung der Klimatisierungs- einrichtung vorzusehen.

INF 6.8 Selbsttätige Entwässerung

Alle Bereiche, in denen sich Wasser sammeln und stauen kann oder in denen fließendes oder stehendes Wasser nicht oder erst spät entdeckt wird und in denen das Wasser Schäden

---

verursachen kann, sollten mit einer selbsttätigen Entwässerung und ggf. mit Wassermelder ausgestattet sein. Zu diesen Bereichen gehören u. a. Keller, Lufträume unter Doppelböden, Lichtschächte und Heizungsanlagen.

---

2 Personelle Maßnahmen

Die Mitarbeiter stellen eine der wichtigsten Ressourcen einer Organisation dar. IT-Sicherheit kann auch bei besten technischen Maßnahmen nur funktionieren, wenn die Mitarbeiter ein ausgeprägtes Sicherheitsbewusstsein haben und bereit und fähig sind, die Vorgaben in der täglichen Praxis umzusetzen. Andererseits stellen Mitarbeiter auch potentielle Angriffs- oder Fehlerquellen dar.

Aus diesen Gründen ist der Schulung und Sensibilisierung für Fragen der IT-Sicherheit eine besondere Bedeutung zuzumessen. Darüber hinaus ist es auch notwendig, sich mit den Möglichkeiten und potentiellen Problemen von Mitarbeitern auseinander zu setzen ("Know your Employee").

Im Folgenden werden in Kapitel 2.1 Regelungen für eigene Mitarbeiter angeführt, die teilweise sinngemäß auch für Fremdpersonal gelten, Kapitel 2.2 gibt einige spezielle Regelungen für Fremdpersonal.

Kapitel 2.3 schließlich führt Maßnahmen zur Sensibilisierung und Schulung im Bereich IT-Sicherheit auf.

2.1 Regelungen für Mitarbeiter

PER 1.1 Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen

Bei der Einstellung von Mitarbeitern sind diese zur Einhaltung einschlägiger Gesetze (z.B. Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 DSG 2000, BGBl. I Nr. 165/1999) § 15 "Datengeheimnis", § 14 "Datensicherheitsmaßnahmen" und § 13 "Genehmigungspflichtige Übermittlung und Überlassung von Daten ins Ausland"), Vorschriften und interner Regelungen zu verpflichten. Damit sollen neue Mitarbeiter mit den bestehenden Vorschriften und Regelungen zur IT-Sicherheit bekannt gemacht und gleichzeitig zu deren Einhaltung motiviert werden. Dabei ist es sinnvoll, nicht nur die Verpflichtung durchzuführen, sondern auch die erforderlichen Exemplare der Vorschriften und Regelungen auszuhändigen und gegenzeichnen zu lassen bzw. für die Mitarbeiter an zentraler Stelle zur Einsichtnahme vorzuhalten.

Neben der Verpflichtung auf die Einhaltung von Gesetzen und Vorschriften empfiehlt es sich insbesondere, Regelungen zu folgenden Bereichen zu treffen, die dann auch in eine entsprechende Verpflichtungserklärung aufzunehmen sind:

---

* Clear Desk Policy, falls vorgesehen (vgl. *PER 1.7 Clear Desk Policy*)
* Einhaltung von PC-Benutzungsregeln (vgl. *SYS 5.1 Herausgabe einer PC-Richtlinie*)
* Einhaltung der Regeln für die Benutzung des Internet (s. Kap. 0 und Anhang C)

Im Anhang C dieses Handbuches finden sich Beispiele für folgende Verpflichtungserklärungen:

* Verpflichtungserklärung betreffend die Benutzung von IT-Systemen
* Verpflichtungserklärung für die Benutzung des Internet

PER 1.2 Aufnahme der sicherheitsrelevanten Aufgaben und Verantwortlichkeiten in die Stellenbeschreibung

Bei der Erstellung von Stellenbeschreibungen ist dafür Sorge zu tragen, dass alle sicherheitsrelevanten Aufgaben und Verantwortlichkeiten explizit in diese Beschreibungen aufgenommen werden. Anzuführen sind dabei sowohl die allgemein aus der organisationsweiten IT-Sicherheitspolitik abzuleitenden Verpflichtungen als auch spezielle Verantwortlichkeiten auf Grund der Tätigkeit. Dies gilt in besonderem Maße für Mitarbeiter mit speziellen Sicherheitsaufgaben (Mitglieder des IT-Sicherheitsmanagement-Teams, Datenschutz-/IT-Sicherheitsbeauftragte, Bereichs-IT-Sicherheitsbeauftragte, Applikations-/Projektverantwortliche).

PER 1.3 Vertretungsregelungen

Vertretungsregelungen haben den Sinn, für vorhersehbare (Urlaub, Dienstreise) und auch unvorhersehbare Fälle (Krankheit, Unfall, Kündigung) des Personenausfalls die Fortführung der Aufgabenwahrnehmung zu ermöglichen. Daher muss vor Eintritt eines solchen Falles geregelt sein, wer wen in welchen Angelegenheiten mit welchen Kompetenzen vertritt. Dies

ist besonders im Bereich der Informationsverarbeitung von Bedeutung, da dafür meist Spezialwissen erforderlich ist und eine zeitgerechte Einarbeitung unkundiger Mitarbeiter für den Vertretungsfall nicht möglich ist.

Für die Vertretungsregelungen sind folgende Randbedingungen einzuhalten:

* Die Übernahme von Aufgaben im Vertretungsfall setzt voraus, dass der Verfahrens- oder Projektstand hinreichend dokumentiert ist.
* Der Vertreter muss so geschult werden, dass er die Aufgaben jederzeit übernehmen kann. Stellt sich heraus, dass es Personen gibt, die auf Grund ihres Spezialwissens nicht kurzfristig ersetzbar sind, so bedeutet deren Ausfall eine gravierende Gefährdung des Normalbetriebes. Hier ist es von besonders großer Bedeutung, einen Vertreter zu schulen.
* Es muss festgelegt sein, welcher Aufgabenumfang im Vertretungsfall von wem wahrgenommen werden soll.

---

* Der Vertreter darf die erforderlichen Zugangs- und Zutrittsberechtigungen nur im Vertretungsfall erhalten.
* Ist es in Ausnahmefällen nicht möglich, für Personen einen kompetenten Vertreter zu benennen oder zu schulen, sollte frühzeitig überlegt werden, welche externen Kräfte für den Vertretungsfall eingesetzt werden können.

PER 1.4 Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern

Scheidet ein Mitarbeiter aus, so ist zu beachten:

* Vor dem Ausscheiden ist eine Einweisung des Nachfolgers durchzuführen.
* Von dem Ausscheidenden sind sämtliche Unterlagen, ausgehändigte Schlüssel, ausgeliehene IT-Geräte (z.B. tragbare Rechner, Speichermedien, Dokumentationen) zurückzufordern. Insbesondere sind die Behörden- bzw. Firmenausweise einzuziehen.
* Es sind sämtliche für den Ausscheidenden eingerichteten Zugangsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. Dies betrifft auch die externen Zugangsberechtigungen via Datenübertragungseinrichtungen. Wurde in Ausnahmefällen eine Zugangsberechtigung zu einem IT-System zwischen mehreren Personen geteilt (z.B. mittels eines gemeinsamen Passwortes), so ist nach Ausscheiden einer der Personen die Zugangsberechtigung zu ändern.
* Nach Möglichkeit sollte eine Neuvergabe der User-ID an einen anderen Mitarbeiter vermieden/ausgeschlossen werden.
* Ist die ausscheidende Person ein Funktionsträger in einem Notlaufplan, so ist der Notlaufplan zu aktualisieren.
* Sämtliche mit Sicherheitsaufgaben betrauten Personen, insbesondere der Portierdienst, sind über das Ausscheiden des Mitarbeiters zu unterrichten.
* Ausgeschiedenen Mitarbeitern ist der unkontrollierte Zutritt zum Behörden- oder Firmengelände, insbesondere zu Räumen mit IT-Systemen zu verwehren.
* Optional kann sogar für den Zeitraum zwischen Aussprechen der Kündigung und dem Ausscheiden der Entzug sämtlicher Zugangs- und Zugriffsrechte auf IT-Systeme sowie darüber hinaus auch das Verbot, schützenswerte Räume zu betreten, ausgesprochen werden.
* Als ein praktikables Hilfsmittel haben sich Laufzettel erwiesen, auf denen die einzelnen Aktivitäten des Ausscheidenden vorgezeichnet sind, die er vor Verlassen der Behörde bzw. des Unternehmens zu erledigen hat.

PER 1.5 Geregelte Verfahrensweise bei Versetzung eines Mitarbeiters

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.

PER 1.6 Gewährleistung eines positiven Betriebsklimas

Ein positives Betriebsklima motiviert die Mitarbeiter einerseits zur Einhaltung von IT-Si heitsmaßnahmen und bewirkt andererseits die Reduzierung von fahrlässigen oder vorsätzlichen Handlungen, die eine Störung des IT-Betriebs herbeiführen können. Daher sol auch unter IT-Sicherheitsaspekten versucht werden, ein positives Betriebsklima zu erreicl

Dazu gehört auch die ergonomische Gestaltung des Arbeitsplatzes. Hierzu bestehen eine Reihe von Regelungen und Normen, deren Nichtbeachtung u.a. eventuell zu Sicherheitsproblemen führen kann. Ergonomie ist nicht Gegenstand dieses Handbuches, die Wichtigkeit einer ergonomischen Gestaltung des Arbeitsplatzes sei aber hier nochmals bet

Weiters ist bei der Ausstattung von Arbeitsplätzen darauf zu achten, dass die Einhaltung IT-Sicherheitsmaßnahmen unterstützt wird. Dazu gehören etwa verschließbare Schreibtische oder Schränke, in denen Datenträger, Dokumentationen, Unterlagen und Zubehör verschlossen werden können.

Ursache für eine unzureichende Aufgabenerfüllung können oftmals persönliche Probleme eines Arbeitnehmers sein. Daher ist es für jede Organisation wichtig, ihre Mitarbeiter u eventuelle potentielle Probleme zu kennen ("Know your Employee"). In vielen Fällen kann e hilfreich sein, wenn eine Anlaufstelle zur Verfügung steht, die bei solchen Problemen konkrete Hilfe und Lösungsmöglichkeiten anbieten kann.

PER 1.7 Clear Desk Policy

Jeder Mitarbeiter sollte vor seiner Abwesenheit seine Unterlagen und den persönlichen Arbeitsbereich verschließen: Schreibtisch, Schrank, PC und Telefon. Dies gilt insbesonde für Großraumbüros, aber auch in den anderen Fällen ist dafür Sorge zu tragen, dass keine unberechtigten Personen (Besucher, Reinigungspersonal, unbefugte Mitarbeiter...) Zugriff Schriftstücken, Datenträgern und IT-Komponenten haben.

Ist eine Clear Desk Policy Regelung in einer Organisation vorgesehen, so sollte die Einh dieser Regelung in die Verpflichtungserklärung jedes Mitarbeiters (vgl. *PER 1.1*) *Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen* aufgenommen werden.

PER 1.8 Benennung eines vertrauenswürdigen Administrators und Vertreters

Administratoren von IT-Systemen und ihren Vertretern muss vom Betreiber großes Vertrauen entgegengebracht werden können. Sie haben - in Abhängigkeit vom eingesetzten System - weit gehende und oftmals alle Befugnisse. Administratoren und ihre Vertreter sind in der Lage, auf alle gespeicherten Daten zuzugreifen, sie ggf. zu verändern und Berechtigungen zu vergeben, dass erheblicher Missbrauch möglich wäre.

Das hierfür eingesetzte Personal muss sorgfältig ausgewählt werden. Es soll regelmäßig darüber belehrt werden, dass die Befugnisse nur für die erforderlichen Administrationsaufgaben verwendet werden dürfen.
Eine regelmäßige Kontrolle der Administratoren - etwa durch Auswertung von Protokollen durch Revisoren - ist vorzusehen.

Darüber hinaus sollte geprüft werden, wieweit durch technische Maßnahmen - etwa die Verschlüsselung von ausgewählten Daten oder Zugriffsbeschränkungen zu Protokollfiles - die Befugnisse von Administratoren eingeschränkt werden können, ohne deren Aufgabenerfüllung zu beeinträchtigen.

PER 1.9 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 einer Zugriffskontrolle nur dann erreicht werden, wenn jede Benutzer sich nach Aufgabenerfüllung bzw. bei Verlassen des Arbeitsplatzes am PC abmeldet. Ist es einem Dritten möglich, an einem PC unter der Identität eines anderen weiterzuarbeiten, so ist jegliche sinnvolle Zugriffskontrolle unmöglich. Daher sind alle Benutzer zu verpflichten, sich bei Verlassen des Arbeitsplatzes abzumelden.

Ist keine Zugriffskontrolle realisiert, so ist die Abmeldung des Benutzers aus Gesichtsp der Ordnungsmäßigkeit dennoch vorzuschreiben.

Ist absehbar, dass nur eine kurze Unterbrechung der Arbeit erforderlich ist, kann an Ste Abmeldens auch eine manuelle oder nach einer gewissen Zeit automatische Aktivierung der Bildschirmsperre erfolgen.

PER 1.10 Geregelte Verfahrensweise bei vermuteten Sicherheitsverletzungen

Die Vorgehensweise zur Untersuchung angeblicher (bewusster oder versehentlicher) Verletzungen von Sicherheitsvorgaben sowie potentielle Konsequenzen - im Falle interner

Mitarbeiter können dies beispielsweise disziplinäre Maßnahmen sein, im Falle externer Mitarbeiter etwa vertraglich abgeleitete Konsequenzen - sollen festgelegt, vom Management verabschiedet und allen Mitarbeitern bekannt sein.

Eine derartig geregelte Verfahrensweise kann einerseits infolge der abschreckenden Wirkung zur Prävention von Sicherheitsverletzungen dienen, und gewährleistet andererseits eine korrekte und faire Behandlung von Personen, denen Sicherheitsverletzungen angelastet werden.

2.2 Regelungen für den Einsatz von Fremdpersonal

PER 2.1 Regelungen für den kurzfristigen Einsatz von Fremdpersonal

Kurzfristig oder einmalig zum Einsatz kommendes Fremdpersonal ist wie Besucher zu behandeln, d.h. dass also etwa der Aufenthalt in sicherheitsrelevanten Bereichen nur in Begleitung von Mitarbeitern der Behörde bzw. des Unternehmens erlaubt ist etc. (vgl. dazu *INF 1.5 Portierdienst*)

PER 2.2 Verpflichtung externer Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen

Externe Mitarbeiter, die über einen längeren Zeitraum in einer oder für eine Organisation sind und ev. Zugang zu vertraulichen Unterlagen und Daten bekommen könnten, sind ebenfalls schriftlich auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen zu verpflichten.

In Anhang C werden Beispiele für die Formulierung derartiger Verpflichtungserklärungen gegeben:

* Verpflichtung zu Geheimhaltung und Datenschutz (Muster, entnommen aus AVB Wartung, vgl. Anhang C2)
* Verpflichtung zur Einhaltung des Datengeheimnisses gemäß §15 Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000, BGBl. I Nr. 165/1999) und zur Verschwiegenheit bezüglich sonstiger Dienst- und Amtsvorgänge (vgl. Anhänge C8 und C9)

PER 2.3 Beaufsichtigung oder Begleitung von Fremdpersonen

Fremde (Besucher, Handwerker, Wartungs- und Reinigungspersonal) sollten, außer in Räumen, die ausdrücklich dafür vorgesehen sind, nicht unbeaufsichtigt sein (siehe auch *INF 1.4 Zutrittskontrolle* und *INF 1.5 Portierdienst*). Wird es erforderlich, einen Fremden allein im Büro zurückzulassen, sollte man einen Kollegen ins Zimmer oder den Besucher zu einem Kollegen bitten.
Ist es nicht möglich, Fremdpersonen (z.B. Reinigungspersonal) ständig zu begleiten oder zu beaufsichtigen, sollte zumindest der persönliche Arbeitsbereich abgeschlossen werden: Schreibtisch, Schrank und PC (Schloss für Diskettenlaufwerk, Tastaturschloss). Siehe auch *PER 1.7 Clear Desk Policy*

Für den häuslichen Arbeitsplatz gilt, dass Familienmitglieder und Besucher sich nur dann alleine im Arbeitsbereich aufhalten dürfen, wenn alle Arbeitsunterlagen verschlossen aufbewahrt sind und die IT über einen aktivierten Zugangsschutz gesichert ist (vgl. Kap. 0).

Die Notwendigkeit dieser Maßnahmen ist den Mitarbeitern zu erläutern und ggf. in einer Dienstanweisung festzuhalten. Eine Dokumentation über den Aufenthalt von Fremdpersonen kann in einem Besucherbuch geführt werden.

PER 2.4 Information externer Mitarbeiter über die IT-Sicherheitspolitik

Externe Mitarbeiter sind so weit es zur Erfüllung ihrer Aufgaben und Verpflichtungen erforderlich ist über hausinterne Regelungen und Vorschriften zur IT-Sicherheit sowie die organisationsweite IT-Sicherheitspolitik zu unterrichten.

2.3 Sicherheitssensibilisierung und schulung

PER 3.1 Geregelte Einarbeitung/Einweisung neuer Mitarbeiter

Neuen Mitarbeitern müssen interne Regelungen, Gepflogenheiten und Verfahrensweisen im IT-Einsatz bekannt gegeben werden. Ohne eine entsprechende Einweisung kennen sie ihre Ansprechpartner bzgl. IT-Sicherheit nicht, sie wissen nicht, welche IT-Sicherheitsmaßnahmen durchzuführen sind und welche IT-Sicherheitspolitik die Behörde bzw. das Unternehmen betreibt. Daraus können Störungen und Schäden für den IT-Einsatz erwachsen. Daher kommt der geregelten Einarbeitung neuer Mitarbeiter eine entsprechend hohe Bedeutung zu.

Die Einarbeitung bzw. Einweisung sollte zumindest folgende Punkte umfassen:

* Planung der notwendigen Schulungen; arbeitsplatzbezogene Schulungsmaßnahmen (s. auch *PER 3.2 Schulung vor Programmnutzung* und *PER 3.3 Schulung zu IT-Sicherheitsmaßnahmen*),

---

* Vorstellung aller Ansprechpartner, insbesondere zu IT-Sicherheitsfragen,
* Erläuterung der hausinternen Regelungen und Vorschriften zur IT-Sicherheit und der
* organisationsweiten IT-Sicherheitspolitik.

PER 3.2 Schulung vor Programmnutzung

Durch unsachgemäßen Umgang mit IT-Anwendungen hervorgerufene Schäden können vermieden werden, wenn die Benutzer eingehend in die IT-Anwendungen eingewiesen werden. Daher ist es unabdingbar, dass die Benutzer vor der Übernahme IT-gestützter Aufgaben ausreichend geschult werden. Dies betrifft sowohl die Nutzung von Standardprogrammpaketen als auch von speziell entwickelten IT-Anwendungen. Darüber hinaus müssen auch bei umfangreichen Änderungen in einer IT-Anwendung Schulungsmaßnahmen durchgeführt werden.

Stehen leicht verständliche Handbücher zu IT-Anwendungen bereit, so kann an Stelle der Schulung auch die Aufforderung stehen, sich selbstständig einzuarbeiten. Eine wesentliche Voraussetzung dazu ist allerdings die Bereitstellung ausreichender Einarbeitungszeit.

PER 3.3 Schulung zu IT-Sicherheitsmaßnahmen

Die überwiegende Zahl von Schäden im IT-Bereich entsteht durch Nachlässigkeit. Um dies zu verhindern, ist jeder Einzelne zum sorgfältigen Umgang mit der IT zu motivieren. Zusätzlich sind Verhaltensregeln zu vermitteln, die Verständnis für die IT-Sicherheitsmaßnahmen wecken.

Insbesondere sollen folgende Themen in der Schulung zu IT-Sicherheitsmaßnahmen vermittelt werden:

* *Sensibilisierung für IT-Sicherheit*
  Jeder Mitarbeiter ist auf die Notwendigkeit der IT-Sicherheit hinzuweisen. Das Aufzeigen der Abhängigkeit der Organisation und damit der Arbeitsplätze von dem reibungslosen Funktionieren der IT-Systeme ist ein geeigneter Einstieg in die Sensibilisierung. Darüber hinaus ist der Wert von Informationen herauszuarbeiten, insbesondere unter den Gesichtspunkten Vertraulichkeit, Integrität und Verfügbarkeit. Diese Sensibilisierungsmaßnahmen sind in regelmäßigen Zeitabständen zu wiederholen, evtl. auch durch praktische Hinweise z.B. in hausinternen Publikationen oder im Intranet.
* *Die mitarbeiterbezogenen IT-Sicherheitsmaßnahmen*
  Zu diesem Thema sollen die IT-Sicherheitsmaßnahmen vermittelt werden, die in einem IT-Sicherheitskonzept erarbeitet wurden und von den einzelnen Mitarbeitern umzusetzen sind. Dieser Teil der Schulungsmaßnahmen hat große Bedeutung, da viele IT-Sicherheitsmaßnahmen erst nach einer entsprechenden Schulung und Motivation effektiv umgesetzt werden können.

---

* *Die produktbezogenen IT-Sicherheitsmaßnahmen*
  Zu diesem Thema sollen die IT-Sicherheitsmaßnahmen vermittelt werden, die inhärent mit einem Softwareprodukt verbunden sind und bereits im Lieferumfang enthalten sind. Dies können neben Passwörtern zur Anmeldung, der Pausenschaltung durch Bildschirmschoner auch Möglichkeiten der Verschlüsselung von Dokumenten oder Datenfeldern sein.
  Hinweise und Empfehlungen über die Strukturierung und Organisation von Dateien, die Bewegungsdaten enthalten, können die Vergabe von Zugriffsrechten erleichtern und den Aufwand für die Datensicherung deutlich reduzieren.
* *Das Verhalten bei Auftreten eines Virus auf einem PC*
  Hier soll den Mitarbeitern vermittelt werden, wie mit Viren umzugehen ist. Mögliche Inhalte dieser Schulung sind (siehe Kap. 0):
  * Wirkungsweise und Arten von Viren
  * Vorbeugende Maßnahmen
  * Erkennen des Virusbefalls
  * Sofortmaßnahmen im Verdachtsfall
  * Maßnahmen zur Eliminierung des Virus
* *Der richtige Einsatz von Zugangscodes und Zugangskontrollmedien*
  Hierbei sollen die Bedeutung von Zugangscodes (Passwörtern, PINs, Zugangscodes für Voicemail, etc.) und Zugangskontrollmedien (Karten, Token,...) für die IT-Sicherheit erläutert werden. Ebenso sind die Randbedingungen, die einen wirksamen Einsatz von Zugangscodes und Zugangskontrollmedien erst ermöglichen, herauszuarbeiten (vgl. auch *SYS 1.5 Regelungen des Passwortgebrauches*, *SYS 1.6 Regelungen des Gebrauchs von Chipkarten*)
* *Die Bedeutung der Datensicherung und deren Durchführung*
  Die regelmäßige Datensicherung ist eine der wichtigsten IT-Sicherheitsmaßnahmen in jedem IT-System. Vermittelt werden sollen das Datensicherungskonzept (s. Kap. 0 *Disaster Recovery und Business Continuity Planung*) der Organisation und die von jedem Einzelnen durchzuführenden Datensicherungsaufgaben. Besonders bedeutend ist dies für

den PC-Bereich, in dem jeder Benutzer selbst die Datensicherung verantwortlich durchführen muss.

* *Der 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.
* *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 Akten) arbeiten müssen, sind für die gesetzlich erforderlichen Sicherheitsmaßnahmen zu schulen. Dies betrifft etwa Meldepflichten, den Umgang mit den Rechten von Betroffenen (Auskunft, Richtigstellung, Löschung, Widerspruch,...), Datensicherheitsmaßnahmen sowie Übermittlung und Überlassung von Daten.

---

* *Die Einweisung in Notfallmaßnahmen*
  Sämtliche Mitarbeiter (auch nicht unmittelbar mit IT befasste Personen wie Portier oder Wachpersonal) sind in bestehende Notfallmaßnahmen einzuweisen. Dazu gehören die Erläuterung der Fluchtwege, die Verhaltensweisen bei Feuer, der Umgang mit Feuerlöschern, das Notfall-Meldesystem (wer als Erstes wie zu benachrichtigen ist) und der Umgang mit dem Disaster Recovery Handbuch.
* *Vorbeugung gegen Social Engineering*
  Die Mitarbeiter sollen auf die Gefahren des Social Engineering hingewiesen werden. Die typischen Muster solcher Versuche, über gezieltes Aushorchen an vertrauliche Informationen zu gelangen, ebenso wie die Methoden, sich dagegen zu schützen, sollten bekannt gegeben werden. Da Social Engineering oft mit der Vorspiegelung einer falschen Identität einhergeht, sollten Mitarbeiter regelmäßig darauf hingewiesen werden, die Identität von Gesprächspartnern zu überprüfen und insbesondere am Telefon keine vertraulichen Informationen weiterzugeben.

PER 3.4 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 Behörden bzw. 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. Die Einrichtung eines Helpdesk kann sich insbesondere bei einer hohen Zahl dezentraler Systeme wie PCs als vorteilhaft erweisen.

Es muss für jeden Benutzer klar ersichtlich sein, an wen er sich in Problemfällen zu wenden hat.

PER 3.5 Aktionen bei Auftreten von Sicherheitsproblemen (Incident Handling Pläne)

Die Aufgaben und Verantwortlichkeiten aller Mitarbeiter bei Auftreten von sicherheitsrelevanten Ereignissen sollten im Rahmen der organisationsweiten IT-Sicherheitspolitik (High-Level-Beschreibung) sowie spezieller "Incident Handling Pläne" (IHPs) sowohl für einzelne Bereiche als auch für die gesamte Organisation festgelegt werden (vgl. dazu auch Teil 1, Kap. 6.3 dieses Handbuches).

Unter sicherheitsrelevanten Ereignissen sind dabei zu verstehen:
* Angriffe und (vermutete) Angriffsversuche gegen ein IT-System
* (vermutete) Sicherheitsschwächen
* Funktionsstörungen von Systemen (etwa durch maliziöse Software)

Incident Handling Pläne sollen in schriftlicher Form und 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.

PER 3.6 Schulung des Wartungs- und Administrationspersonals

Das Wartungs- und Administrationspersonal sollte mindestens so weit geschult werden, dass
* alltägliche Administrationsarbeiten selbst durchgeführt,
* einfache Fehler selbst erkannt und behoben,
* Datensicherungen selbsttätig durchgeführt,
* die Eingriffe von externem Wartungspersonal nachvollzogen und
* Manipulationsversuche oder unbefugte Zugriffe auf die Systeme erkannt

werden können.

PER 3.7 Sensibilisierung der Mitarbeiter für mögliche TK-Gefährdungen

Die Mitarbeiter müssen über die mit dem Benutzen einer digitalen TK-Anlage verbundenen Gefährdungen informiert werden. Dies könnte z.B. durch eine kurze Unterweisung oder mit Hilfe von Merkblättern geschehen. Es ist darauf hinzuweisen, dass ein abnormes Verhalten der TK-Anlage gemeldet werden soll. Bei Manipulationen an der TK-Anlage sollte eine unabhängige Kontrollinstanz wie das IT-Sicherheitsmanagement-Team oder der Datenschutz-/IT-Sicherheitsbeauftragte informiert werden.

Ebenso sind die Mitarbeiter auf die potentiellen Gefahren bei der Benutzung von Mobiltelefonen hinzuweisen. Dabei sind nicht nur die technischen Möglichkeiten des Abhörens vo Gesprächen zu berücksichtigen, sondern auch die Tatsache, dass bei Benutzung von Mobiltelefonen in öffentlichen Räumen Umstehende von vertraulichen Informationen Kenntnis erlangen könnten. Gespräche mit vertraulichem oder geheimem Charakter über Mobiltelefone

sollten daher grundsätzlich verboten sein. Ist dies nicht möglich oder erwünscht, können Verschlüsselungssysteme Schutz der Information auf dem Übertragungsweg bieten. Nach wie vor hat der Benutzer aber darauf zu achten, dass sein Gespräch nicht von anderen Anwesenden unbefugt mitgehört wird.

Da sich erfahrungsgemäß viele Mitarbeiter dieser Problematik nicht bewusst sind, ist eingehend und wiederholt darauf hinzuweisen.

PER 3.8 Einweisung in die Regelungen der Handhabung von Kommunikationsmedien

Der Einsatz neuer Medien und Geräte - dazu zählen Fax und Modems genauso wie etwa Anrufbeantworter und Voice Mail - erleichtert die Kommunikation, bringt aber auch neue potentielle Gefährdungen der Vertraulichkeit und Integrität von Informationen mit sich. A Mitarbeiter sind daher auf die Besonderheiten der Handhabung von solchen Geräten hinzu- weisen und für potentielle Gefahren zu sensibilisieren.

Verständliche Bedienungsanleitungen, Sicherheitshinweise und ggf. auch Dienstanweisungen sind den Mitarbeitern zur Kenntnis zu bringen und verfügbar zu halten.

Im Folgenden werden einige Beispiele angeführt, was solche Regelungen umfassen sollten. Sie sind den jeweiligen technischen Anforderungen und Möglichkeiten anzupassen.

Fax (Stand-alone-Gerät):

* Festlegung eines Fax-Verantwortlichen, der für die Verteilung eingehender Fax-Sendungen zuständig ist und als Ansprechpartner in Fax-Problemfällen fungiert,
* Festlegung, wer das Faxgerät benutzen darf,
* Verbot des Versendens von vertraulichen Informationen per Fax (oder besondere technische und organistorische Vorkehrungen für diesen Fall, wie etwa telefonische Ankündigung eines derartigen Fax),
* Verwendung einheitlicher Fax-Deckblätter,
* ggf. Kontrolle von Einzelsendenachweisen.

Modem:

* Information über mögliche Gefährdungen, einzuhaltende Sicherheitsmaßnahmen und Regelungen beim Betrieb eines Modems,
* Auswirkungen verschiedener Konfigurationen auf die Betriebssicherheit des Modems.

Anrufbeantworter:

* Regelung über den Einsatz von Sicherungscodes für die Fernabfrage
* Vermeidung schutzbedürftiger Informationen auf Anrufbeantwortern,
* Regelmäßiges Abhören und Löschen aufgezeichneter Gespräche,
* Abschalten nicht benötigter Leistungsmerkmale.

PER 3.9 Einweisung in die Bedienung von Schutzschränken

Nach der Beschaffung eines Schutzschrankes (Serverschrank oder Datensicherungsschrank) sind die Benutzer in die korrekte Bedienung einzuweisen. Dies sollte auch bei Neuübertragung einer Aufgabe erfolgen, die die Nutzung eines Schutzschrankes umfasst.

Beispiele für zu vermittelnde Punkte sind:

* Korrekter Umgang mit dem Schloss des Schutzschrankes:
  Dabei ist auf typische Fehler hinzuweisen, wie zum Beispiel das Nichtverwerfen von Codeschlössern. Die Regelungen zur Schlüsselverwaltung, Schlüsselhinterlegung und Vertretungsregelung sind aufzuzeigen. Insbesondere ist einzufordern, dass der Schutzschrank bei auch nur kurzfristiger Nichtbenutzung verschlossen wird.
* Im Falle eines Serverschrankes ist darauf hinzuweisen, dass unnötige brennbare Materialien (Ausdrucke, überzählige Handbücher, Druckerpapier) nicht im Serverschrank aufbewahrt werden sollen.
* Datensicherungsträger des Servers sollten in einem anderen Brandabschnitt bzw. bei Bedarf disloziert gelagert werden. Eine Aufbewahrung im Serverschrank ist daher ungeeignet und nur dann zulässig, wenn eine Kopie der Datensicherungsbestände in einem anderen Brandabschnitt bzw. disloziert ausgelagert ist.
* Wird ein klimatisierter Serverschrank eingesetzt, sollten dessen Öffnungszeiten minimi werden. Gegebenenfalls ist sporadisch zu kontrollieren, ob im Serverschrank Wasser kondensiert ist.

3 IT-Sicherheitsmanagement

Diese in diesem Kapitel angeführten Maßnahmen aus dem Bereich IT-Sicherheitsmanagement sollen einen angemessenen, umfassenden und konsistenten Grad an IT-Sicherheit für die gesamte Organisation gewährleisten.

gesamte Organisation gewährleisten.

SMG 1.1 Etablierung eines IT-Sicherheitsmanagementprozesses

Methodisches Sicherheitsmanagement ist zur Gewährleistung umfassender und angemessener IT-Sicherheit unerlässlich. Dabei handelt es sich um einen kontinuierlichen Prozess, der die Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit, Authentizität und Zuverlässigkeit von IT-Systemen gewährleisten soll. Dieser Prozess ist zumindest auf Ebene der Gesamtorganisation zu etablieren, über eine Durchführung auf der Ebene einzelner Organisationseinheiten ist im Einzelfall zu entscheiden.

Zu den Aufgaben des IT-Sicherheitsmanagements gehören:

* Festlegung der IT-Sicherheitsziele, -strategien und -politiken der Organisation,
* Festlegung der IT-Sicherheitsanforderungen,
* Ermittlung und Analyse von Bedrohungen und Risiken,
* Festlegung geeigneter Sicherheitsmaßnahmen,
* Überwachung der Implementierung und des laufenden Betriebes der ausgewählten Maßnahmen,
* Förderung des Sicherheitsbewusstseins innerhalb der Organisation sowie
* Entdecken von und Reaktion auf sicherheitsrelevante Ereignisse.

Die folgende Graphik zeigt die wichtigsten Aktivitäten im Rahmen des IT-Sicherheitsmanagements und die eventuell erforderlichen Rückkopplungen zwischen den einzelnen Stufen. In Teil 1 des vorliegenden Handbuches ([KIT S01] werden die zur Etablierung eines umfassenden IT-Sicherheitsmanagementprozesses erforderlichen Schritte detailliert beschrieben.

Entwicklung einer organisationsweiten IT-Sicherheitspolitik

Risikoanalyse

Detaillierte Risikoanalyse | Grundschutz-Ansatz | Kombinierter Ansatz

Erstellung eines IT-Sicherheitskonzeptes

Auswahl von Maßnahmen

Risikoakzeptanz

Entwicklung

IT-Systemsicherheitspolitiken

IT-Sicherheitsplan

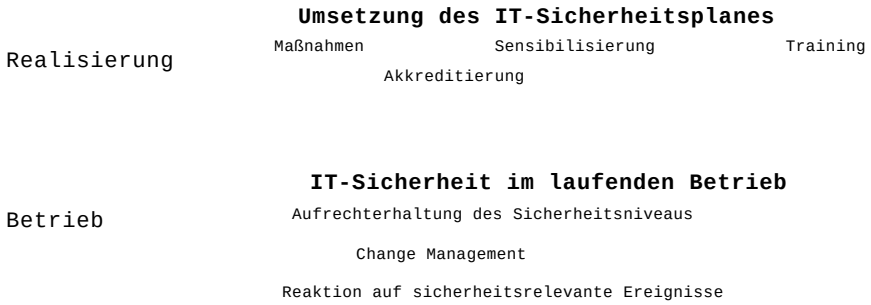

Abbildung 3 IT-Sicherheitsmanagement.1: Aktivitäten im Rahmen des IT-Sicherheitsmanagements

SMG 1.2 Erarbeitung einer organisationsweiten IT-Sicherheitspolitik

Als organisationsweite IT-Sicherheitspolitik bezeichnet man die Leitlinien und Vorgaben innerhalb einer Organisation, die unter Berücksichtigung gegebener Randbedingungen grundlegende Ziele, Strategien, Verantwortlichkeiten und Methoden für die Gewährleistung der IT-Sicherheit festlegen.

Jede Organisation sollte eine in schriftlicher Form vorliegende IT-Sicherheitspolitik erarbeiten, die als langfristig gültiges Dokument zu betrachten ist.

Die organisationsweite IT-Sicherheitspolitik soll allgemeine Festlegungen treffen, die fü Einsatzbereiche der Informationstechnologie innerhalb einer Organisation zur Anwendung kommen und folgende Inhalte umfassen:

* Grundsätzliche Ziele und Strategien
* Organisation und Verantwortlichkeiten für IT-Sicherheit
* Risikoanalysestrategien, akzeptables Restrisiko und Risikoakzptanz
* Klassifikation von Daten
* Organisationsweite Richtlinien zu Sicherheitsmaßnahmen
* Disaster Recovery Planung
* Nachfolgeaktivitäten zur Überprüfung und Aufrechterhaltung der Sicherheit

Details und Anleitungen zur Erstellung einer organisationsweiten IT-Sicherheitspolitik fi sich in Teil 1, Kapitel 2 des vorliegenden Handbuches.

SMG 1.3 Erarbeitung von IT-Systemsicherheitspolitiken

Für jedes IT-System sollte eine IT-Systemsicherheitspolitik erarbeitet werden, die
* die grundlegenden Vorgaben und Leitlinien zur Sicherheit in diesem System definiert,
* Details über die ausgewählten Sicherheitsmaßnahmen beschreibt und
* die Gründe für die Auswahl der Sicherheitsmaßnahmen dargelegt.

Die IT-Systemsicherheitspolitik sollte Aussagen zu folgenden Bereichen treffen:

* Definition und Abgrenzung des Systems, Beschreibung der wichtigsten Komponenten
* Definition der wichtigsten Ziele und Funktionalitäten des Systems
* Festlegung der IT-Sicherheitsziele des Systems
* Abhängigkeit der Organisation vom betrachteten IT-System
* Investitionen in das System
* Risikoanalysestrategie
* Werte, Bedrohungen und Schwachstellen lt. Risikoanalyse
* Sicherheitsrisiken
* Beschreibung der bestehenden und der noch zu realisierenden Sicherheitsmaßnahmen
* Gründe für die Auswahl der Maßnahmen
* Kostenschätzungen für die Realisierung und Wartung (Aufrechterhaltung) der Sicherheitsmaßnahmen
* Verantwortlichkeiten

Details und Anleitungen zur Erstellung von IT-Systemsicherheitspolitiken finden sich in T
1, Kapitel 4.3 des vorliegenden Handbuches.

SMG 1.4 Festlegung von Verantwortlichkeiten

Um eine Berücksichtigung aller wichtigen Sicherheitsaspekte und eine effiziente Erledigu
sämtlicher anfallender Aufgaben zu gewährleisten, ist es erforderlich, die Rollen aller
IT-Sicherheitsprozess involvierten Personen klar zu definieren.

Diese Festlegung erfolgt zweckmäßig im Rahmen der organisationsweiten IT-SicherheitspolitiSMG 1.2 Erarbeitung einer organisationsweiten IT-Sicherheitspolitik
und Teil 1, Kapitel 2.2.2).

Es empfiehlt sich, darüber hinaus detaillierte Regelungen zu folgenden Bereichen zu tref
* Datensicherung,
* Datenarchivierung,
* Datenübertragung,
* Dokumentation von IT-Verfahren, Software, IT-Konfiguration,
* Zutritts-, Zugangs- und Zugriffsberechtigungen,
* Datenträger- und Betriebsmittelverwaltung,
* Anwendungsentwicklung,
* Kauf und Leasing von Hardware und Software,
* Abnahme und Freigabe von Software,
* Wartungs- und Reparaturarbeiten,
* Datenschutz,
* Schutz gegen maliziöse Software (Viren, Würmer, trojanische Pferde,...)
* Revision,
* Notfallvorsorge und
* Vorgehensweise bei Verletzung der Sicherheitspolitik.

Nähere Erläuterungen dazu finden sich in den nachfolgenden Maßnahmenbeschreibungen.

Weiters ist zu beachten:
* Die Regelungen sind den betroffenen Mitarbeitern in geeigneter Weise bekannt zu geben.
* Sämtliche Regelungen sind in der aktuellen Form an einer Stelle vorzuhalten und bei berechtigtem Interesse zugänglich zu machen.
* Es empfiehlt sich, die Bekanntgabe zu dokumentieren.
* Die getroffenen Regelungen sind regelmäßig zu aktualisieren, um Missverständnisse

Die getroffenen Regelungen sind regelmäßig zu aktualisieren, um Missverständnisse, ungeklärte Zuständigkeiten und Widersprüche zu verhindern.

SMG 1.5 Funktionstrennung

Im Rahmen der Zuordnung von Aufgaben und Verantwortlichkeiten ist auch festzulegen, welche Funktionen nicht miteinander vereinbar sind, also auch nicht von einer Person gleichzeitig wahrgenommen werden dürfen ("Funktionstrennung").

Vorgaben hierfür können aus den Aufgaben selbst oder aus gesetzlichen Bestimmungen resultieren. Beispiele dafür sind:

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

Insbesondere wird deutlich, dass meistens operative Funktionen nicht mit kontrollierenden Funktionen vereinbar sind.

Nach der Festlegung der einzuhaltenden Funktionstrennung kann die Zuordnung der Funktionen zu Personen erfolgen. Die dabei getroffenen Festlegungen sind zu dokumentieren und bei Veränderungen im IT-Einsatz zu aktualisieren. Sollte bei dieser Zuordnung eine Person miteinander unvereinbare Funktionen wahrnehmen müssen, so ist dies in einer entsprechenden Dokumentation über die Funktionsverteilung besonders hervorzuheben.

SMG 1.6 Einrichtung von Standardarbeitsplätzen

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

IT-Sicherheit:

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

IT-Management:

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

IT-Nutzer:

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

Systemadministration bei Installation und Wartung:
* Eine gewissenhaft geplante und getestete Installation kann fehlerfrei und mit geringem Arbeitsaufwand installiert werden.
* Die einheitliche Arbeitsumgebung erleichtert Wartung und Support.

Schulung:
* Die Teilnehmer werden in dem Umfeld geschult, das sie am Arbeitsplatz vorfinden.

SMG 1.7 Akkreditierung von IT-Systemen

Für jedes IT-System ist sicherzustellen, dass es den Anforderungen der IT-Systemsicherhei politik genügt. Dabei ist insbesondere darauf zu achten, dass die Sicherheit des Systems
* in einer bestimmten Betriebsumgebung,
* unter bestimmten Einsatzbedingungen und
* für eine bestimmte vorgegebene Zeitspanne

gewährleistet ist.

Erst nach erfolgter Akkreditierung kann das System - oder gegebenenfalls eine spezifische Anwendung - in Echtbetrieb gehen.

Techniken zur Akkreditierung sind:

* Prüfung der Maßnahmen auf Übereinstimmung mit der IT-Sicherheitspolitik (Security Compliance Checking), vgl. auch Kap. 0
* Tests
* Evaluation und Zertifizierung von Systemen

Änderungen der eingesetzten Sicherheitsmaßnahmen oder der Betriebsumgebung können eine neuerliche Akkreditierung des Systems erforderlich machen. Die Kriterien, wann eine Neu- akkreditierung durchzuführen ist, sollten in der IT-Systemsicherheitspolitik festgelegt w

4 Sicherheit in der Systementwicklung

Die Anforderungen an die Sicherheit eines IT-Systems sollten bereits zu Beginn der Entwicklung ermittelt und abgestimmt werden. Eine nachträgliche Implementierung von Sicherheitsmaßnahmen ist bedeutend teurer und bietet im Allgemeinen weniger Schutz als Sicherheit, die von Beginn an in den Systementwicklungsprozess oder in den Auswahlprozess für ein Produkt integriert wurde.

Sicherheit sollte daher integrierter Bestandteil des gesamten Lebenszyklus eines IT-Systems bzw. eines Produktes sein.

Die in Kapitel_0 angeführten Maßnahmen orientieren sich am "Vorgehensmodell für die Entwicklung von IT-Systemen des Bundes" ([IT-BVM]) sowie teilweise an den Vorgaben der "Information Technology Security Evaluation Criteria" ([ITSEC]).

Im Gegensatz zu den ITSEC, die zwischen "IT-Systemen" und "IT-Produkten" unterscheiden, wobei der gemeinsame Oberbegriff "Evaluierungsgegenstand" (EVG) lautet, wird in den folgenden Maßnahmenbeschreibungen der besseren Lesbarkeit halber, wenn nicht explizit angeführt, stets von "IT-Systemen" oder einfach "Systemen" gesprochen, auch wenn es sich im Einzelfall um ein Produkt (etwa Standardsoftware) oder eine Einzelkomponente handelt.

4.1 Sicherheit im gesamten Lebenszyklus eines IT-Systems

In den [IT-BVM] wird ein an die Bedürfnisse der österreichischen Bundesverwaltung angepaßtes Vorgehensmodell (V-Modell) für die Entwicklung von IT-Systemen vorgestellt, das im folgenden kurz beschrieben wird.

Das österreichische Vorgehensmodell wurde in Anlehnung an das international anerkannte deutsche Vorgehensmodell [4] entwickelt. Es teilt sich in vier Bereiche auf:

[4] Dieses wird seit sieben Jahren in vielen europäischen Ländern angewendet und wird laufend von der Bundesrepublik Deutschland gewartet und verbessert.

IT-Sicherheitshandbuch für die öffentliche Verwaltung
Teil 2

PM
Projektmanagement

QS		KM
Qualitäts-sicherung	**SE** System-erstellung	Konfigurations-management

Abbildung 4 Sicherheit in der Systementwicklung.2: Die vier Bereiche (Submodelle) des IT-BVM

SE Systemerstellung
In diesem Bereich werden die Tätigkeiten beschrieben, die zur eigentlichen Erstellung des EDV-Systems notwendig sind. Weiters beschreibt es die Abhängigkeiten der Tätigkeiten untereinander und deren erzeugte Ergebnisse.

PM Projektmanagement
Hier werden alle Tätigkeiten zusammengefaßt, die das Projekt steuern (wie z.B. Kosten-steuerung, Terminsteuerung usw.).

QS Qualitätssicherung
Tätigkeiten, um eine hohe Qualität der EDV-Anwendung sicherzustellen, werden in der QS zusammengefaßt.

KM Konfigurationsmanagement
Dieser Bereich beinhaltet Tätigkeiten, die Änderungen leichter nachvollziehbar bzw. überhaupt erst möglich machen (z.B. die Ablage der Entwicklungsdokumente und des Programmcodes).

Alle diese Bereiche sind eng miteinander verzahnt.

Systemerstellung (SE)

Der Bereich SE gliedert sich in sechs Phasen (Vierecke im Hintergrund). Jede Phase teilt in weitere Elementarphasen (Blöcke im Vordergrund) und diese wiederum in Aktivitäten (nicht abgebildet). Es folgt eine kurze Beschreibung der Elementarphasen:

Abbildung 4 Sicherheit in der Systementwicklung.3: Gliederung des Vorgehensmodells

* SE 1 System-Anforderungsanalyse
  Hier werden die Anforderungen an das Gesamtsystem erhoben. Unter dem Gesamtsystem versteht man nicht nur das IT-System, sondern auch das fachliche Umfeld, selbst wenn Teile davon später nicht mittels EDV abgedeckt werden.

* SE 2 System-Entwurf
  Der Grobentwurf des Gesamtsystems wird ermittelt und festgehalten
*
* SE 3 SW-/HW-Anforderungsanalyse
  In dieser Elementarphase konzentriert man sich bereits auf die Anforderungen der Softw bzw. der Hardware. Bereiche, die nicht von der späteren IT-Anwendung betroffen sind, werden hier nicht weiter untersucht.
*
* SE 4 SW-Grobentwurf
  Die Software wird grob gegliedert und beschrieben.
*

---

* SE 5 SW-Feinentwurf
  Die zuvor gebildete grobe SW-Struktur wird weiter verfeinert und beschrieben.

*
* SE 6 SW-Implementierung
  Die Softwarevorgaben werden in Programme bzw. Datenbanken umgesetzt. Erste Über-
  prüfungen gegenüber dem SW-Feinentwurf werden durchgeführt.

*
* SE 7 SW-Integration
  Die einzelnen Softwareteile werden zu größeren Softwareeinheiten zusammengefügt und
  getestet.

*
*

</d