Österreichisches Informationssicherheitshandbuch

Teil 1: Informationssicherheitsmanagement
Teil 2: Informationssicherheitsmaßnahmen

Version 2.3
April 2007

BUNDESKANZLERAMT ÖSTERREICH

books@ocg.at
BAND 226

Wissenschaftliches Redaktionskomitee der OCG

o.Univ.Prof.Dr.G.Chroust
o.Univ.Prof.Dr.G.Haring
o.Univ.Prof.Dr.G.Kotsis
Dr. N. Rozsenich
Univ.Doz.Dr.V.Risak
o.Univ.Prof.Dr.P.Zinterhof

Österreichisches Informationssicherheitshandbuch

Teil 1: Informationssicherheitsmanagement
Teil 2: Informationssicherheitsmaßnahmen

Version 2.3
April 2007

© Österreichische Computer Gesellschaft 2007

Bibliographische Information Der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet über http://dnb.ddb.de abrufbar.

Erstellt und herausgegeben vom Bundeskanzleramt, Informationssicherheitsbüro, in Zusammenarbeit mit A-SIT (Zentrum für sichere Informationstechnologie – Austria) und der OCG (Österreichische Computer Gesellschaft)

© Österreichische Computer Gesellschaft
Komitee für Öffentlichkeitsarbeit
www.ocg.at

Druck: Druckerei Ferdinand Berger & Söhne
Pulverturmgasse 3
1090 Wien
http://www.berger.at

ISBN 978-3-85403-226-9 Neubearb. und erw. Aufl.
(ISBN 3-85403-181-5 Erstausgabe)

Das österreichische Informationssicherheitshandbuch

Vorwort Staatssekretärin Heidrun Silhavy

In unserer Gesellschaft ist das wirtschaftliche und gesellschaftliche Leben zunehmend digitalisiert - Arbeits- und Geschäftsprozesse basieren immer stärker auf IT-Lösungen. Durch die wachsende Abhängigkeit von der IT-Infrastruktur besteht ein starkes volkswirtschaftliches und staatliches Interesse an einer funktionierenden und sicheren Informationsverarbeitung. Sicherheit und Zuverlässigkeit der Informationstechnik entscheiden darüber, ob zentrale gesellschaftliche Bereiche funktionieren.

Dabei genügt es nicht, sich auf die Technik zu verlassen. Zur Zielerreichung müssen verschiedene Teilaspekte integriert betrachtet werden, denn Sicherheit können wir nur ganzheitlich erhöhen. Das Informationssicherheitshandbuch umfasst daher auch den Begriff der Informationssicherheit mit dem Ziel die Verarbeitung, Speicherung und Kommunikation von Informationen so zu gestalten, dass die Vertraulichkeit, Verfügbarkeit und Integrität der Informationen und Systeme in ausreichendem Maß sichergestellt wird. Dabei gilt es die Systeme vor Gefahren bzw. Bedrohungen zu schützen, Schaden zu vermeiden und Risiken zu minimieren, wobei wir auch die Sicherheit von nicht elektronisch verarbeiteten Informationen beachten müssen.

Um eine umfassende Informationssicherheit zu gewährleisten, müssen wir die Problematik verstehen, die aufgezeigten Maßnahmen konsequent umsetzen und mit den eingesetzten Hilfsmitteln richtig umgehen. Zugleich müssen wir mit der Entwicklung ständig Schritt halten.

Das vorliegende „österreichische Informationssicherheitshandbuch“ soll dazu ein probates Hilfsmittel sein und wurde im Auftrag des Bundeskanzleramtes (BKA) aufgrund der aktuellen internationalen Entwicklung neu überarbeitet. Es beschreibt umfassende Strategien und Maßnahmen, mit denen Informationssicherheit effektiv etabliert und aufrechterhalten werden kann, orientiert sich an internationalen Standards unter Berücksichtigung österreichischer Vorschriften und trägt zur Umsetzung einer einheitlichen Vorgehensweise im Bereich des Informationssicherheitsmanagements bei. Die dargestellten Inhalte beschränken sich dabei nicht nur auf die öffentliche Verwaltung, sondern eignen sich auch für die Anwendung durch Wirtschaft und interessierte Bürger und Bürgerinnen.

Österreich besitzt mit dem "Österreichischen Informationssicherheitshandbuch" ein international anerkanntes Standardwerk zur Informationssicherheit und trägt damit dem jüngsten Schwerpunkt zur „Sicherheit für Gesellschaft, Wirtschaft und Wissenschaft“ auf europäischer Ebene Rechnung.

Ich bin daher überzeugt, dass die Anwendung dieses Werkes dazu beitragen wird, das bereits anerkannt hohe Niveau der Informationssicherheit in Österreich weiter anzuheben.

INHALT

Teil 1: Informationssicherheitsmanagement

Vorwort (Management Summary)

1 Informationssicherheitsmanagement in der Praxis ... 14
1.1 Ziele und Aufgaben des Informationssicherheitsmanagements ... 14
1.2 Zielsetzungen des Handbuches ... 15
2 Der Informationssicherheitsmanagement-Prozess ... 17
3 Entwicklung einer organisationsweiten Informationssicherheitspolitik ... 21
3.1 Aufgaben und Ziele einer Informationssicherheitspolitik ... 21
3.2 Die Inhalte der Informationssicherheitspolitik ... 22
3.2.1 Informationssicherheitsziele und -strategien ... 22
3.2.2 Management Commitment ... 23
3.2.3 Organisation und Verantwortlichkeiten für Informationssicherheit ... 24
3.2.4 Risikoanalysestrategien, akzeptables Restrisiko und Akzeptanz von außergewöhnlichen Restrisiken ... 27
3.2.5 Klassifizierung von Informationen ... 29
3.2.6 Klassifizierung von IT-Anwendungen und IT-Systemen, Grundzüge der Business Continuity Planung ... 31
3.2.7 Überprüfung und Aufrechterhaltung der Sicherheit ... 32
3.2.8 Dokumente zur Informationssicherheit ... 33
3.3 Life Cycle der Informationssicherheitspolitik ... 33
3.3.1 Erstellung ... 33
3.3.2 Offizielle Inkraftsetzung ... 33
3.3.3 Regelmäßige Überarbeitung ... 34
4 Risikoanalyse ... 35
4.1 Risikoanalysestrategien ... 35
4.2 Detaillierte Risikoanalyse ... 36
4.2.1 Abgrenzung des Analysebereiches ... 38
4.2.2 Identifikation der bedrohten Objekte (Werte, assets) ... 38
4.2.3 Wertanalyse (Impact Analyse) ... 38
4.2.4 Bedrohungsanalyse ... 40
4.2.5 Schwachstellenanalyse ... 42
4.2.6 Identifikation bestehender Sicherheitsmaßnahmen ... 43
4.2.7 Risikobewertung ... 44
4.2.8 Auswertung und Aufbereitung der Ergebnisse ... 44
4.3 Grundschutzansatz ... 45
4.3.1 Die Idee des IT-Grundschutzes ... 45
4.3.2 Grundschutzanalyse und Auswahl von Maßnahmen ... 46
4.4 Kombinierter Ansatz ... 48
4.4.1 Festlegung von Schutzbedarfskategorien ... 49
4.4.2 Schutzbedarfsfeststellung ... 52
4.4.3 Durchführung von Grundschutzanalysen und detaillierten Risikoanalysen ... 53
4.5 Akzeptables Restrisiko ... 54
4.6 Akzeptanz von außergewöhnlichen Restrisiken ... 54
5 Erstellung von Sicherheitskonzepten ... 55
5.1 Auswahl von Maßnahmen ... 55
5.1.1 Klassifikation von Sicherheitsmaßnahmen ... 55

5.1.2 Ausgangsbasis für die Auswahl von Maßnahmen 57
5.1.3 Auswahl von Maßnahmen auf Basis einer detaillierten Risikoanalyse 57
5.1.4 Auswahl von Maßnahmen im Falle eines Grundschutzansatzes 58
5.1.5 Auswahl von Maßnahmen im Falle eines kombinierten Risikoanalyseansatzes 59
5.1.6 Bewertung von Maßnahmen 59
5.1.7 Rahmenbedingungen 59
5.2 Risikoakzeptanz 60
5.3 Sicherheitsrichtlinien 61
5.3.1 Aufgaben und Ziele 61
5.3.2 Inhalte 61
5.3.3 Fortschreibung der Sicherheitsrichtlinien 62
5.3.4 Verantwortlichkeiten 62
5.4 Informationssicherheitsplan 62
5.5 Fortschreibung des Sicherheitskonzeptes 63
6 Umsetzung des Informationssicherheitsplanes 64
6.1 Implementierung von Maßnahmen 64
6.2 Sensibilisierung (Security Awareness) 66
6.3 Schulung 67
6.4 Akkreditierung 68
7 Informationssicherheit im laufenden Betrieb 69
7.1 Aufrechterhaltung des erreichten Sicherheitsniveaus 69
7.1.1 Wartung und administrativer Support von Sicherheitseinrichtungen 69
7.1.2 Überprüfung von Maßnahmen auf Übereinstimmung mit der Informationssicherheitspolitik (Security Compliance Checking) 70
7.1.3 Fortlaufende Überwachung der IT-Systeme (Monitoring) 71
7.2 Change Management 72
7.3 Reaktion auf sicherheitsrelevante Ereignisse (Incident Handling) 72
8 Industrielle Sicherheit 74
8.1 Beschreibung der generellen Anforderungen 74
8.2 Rechtlicher Hintergrund 75
8.3 Ausstellung einer Sicherheitsunbedenklichkeitsbescheinigung 77
8.3.1 Ablauf 77
8.3.2 Verantwortlichkeiten und Kontakte 78
Anhang A: 80
A.1 Literatur 80
A.2 Gesetzestexte 81
A.3 Glossar 83

Teil 2: Informationssicherheitsmaßnahmen

1 Bauliche und infrastrukturelle Maßnahmen ... 89
1.1 Bauliche Maßnahmen ... 89
1.2 Brandschutz ... 95
1.3 Stromversorgung, Maßnahmen gegen elektrische und elektromagnetische Risiken ... 101
1.4 Leitungsführung ... 107
1.5 Geeignete Aufstellung und Aufbewahrung ... 110
1.6 Weitere Schutzmaßnahmen ... 116
2 Personelle Maßnahmen ... 121
2.1 Regelungen für Mitarbeiter/innen ... 121
2.2 Regelungen für den Einsatz von Fremdpersonal ... 126
2.3 Sicherheitssensibilisierung und -schulung ... 127
3 IT-Sicherheitsmanagement ... 133
3.1 IT-Sicherheitsmanagement ... 133
4 Sicherheit in der Systementwicklung ... 140
4.1 Sicherheit im gesamten Lebenszyklus eines IT-Systems ... 140
4.2 Dokumentation ... 156
4.3 Evaluierung und Zertifizierung ... 161
5 Systemsicherheit ... 163
5.1 Berechtigungssysteme, Schlüssel- und Passwortverwaltung ... 163
5.2 Betriebsmittel und Datenträger ... 171
5.3 Einsatz von Software ... 175
5.4 Virenschutz ... 179
5.5 Arbeitsplatz-IT-Systeme ... 188
5.6 System-/Netzwerkadministration ... 194
5.7 Remote Access ... 208
5.8 Gesicherte Anbindung an Fremdnetze (Internet-Sicherheit) ... 220
5.9 Telearbeit ... 252
5.10 Protokollierung ... 261
5.11 Kryptographische Maßnahmen ... 269
6 Aufrechterhaltung der Sicherheit im laufenden Betrieb ... 283
6.1 Wartung ... 283
6.2 Security Compliance Checking und Monitoring ... 288
6.3 Change Management ... 293
6.4 Reaktion auf sicherheitsrelevante Ereignisse (Incident Handling) ... 297
7 Disaster Recovery und Business Continuity Planung ... 299
7.1 Datensicherung ... 299
7.2 Strategie und Planung ... 307
7.3 Umsetzung und Test ... 317
Anhang A: Wichtige Normen ... 319
A 1 Brandschutz ... 319
A 2 Sicherheitstüren und einbruchhemmende Türen ... 321
A 3 Wertbehältnisse ... 321
A 4 Vernichtung von Akten und Daten ... 321
A 5 Informationssicherheit und IT-Sicherheit ... 322

Anhang B: Referenzdokumente **324**
Anhang C: Muster für Verträge, Verpflichtungserklärungen und Inhaltsverzeichnisse **327**
Anhang D: Wichtige Adressen **346**
Anhang E: Referenzierte IKT-Board Beschlüsse und Gesetze **348**
E.1 IKT-Board Beschlüsse 348
E.2 Gesetzestexte 350

Vorwort (Management Summary)

Mehr denn je ist uns bewusst: Informationen sind Werte. Wir besitzen sie aus unterschiedlichen Gründen - weil wir für ihre Verwahrung oder Verarbeitung Verantwortung tragen, weil wir aus ihnen einen Vorteil ziehen, weil ihre Kenntnis uns vor Schaden bewahrt und noch viel mehr. Gehen sie uns verloren, werden sie gestohlen, sind sie falsch oder einfach nicht auffindbar, wenn wir sie benötigen, dann erleiden wir Schaden - die Palette reicht von geringfügig bis existenzbedrohend.

Das ist zwar nichts Neues, dennoch ist es der zentrale und immer wichtiger werdende Aspekt der Informationssicherheit. Niemand bestreitet das, aber wie viel sind wir bereit, in den Schutz unserer Informationen zu investieren und was ist im speziellen Fall die optimale Lösung? Hier wird es schon differenzierter, das zeigen entsprechende Umfragen immer wieder.

Aus der Fülle möglicher Bedrohungen und der Fülle möglicher Gegenmaßnahmen methodisch diejenigen identifizieren zu helfen, welche für ein spezielles Szenario beachtet werden sollen bzw. müssen, war von Beginn an die Zielsetzung dieses Handbuches. Ausgehend von seiner ersten Version („IT-Sicherheitshandbuch für die öffentliche Verwaltung“), die sich am Sicherheitsbedürfnis öffentlicher Einrichtungen orientiert hat, wurde beim „Österreichischen IT-Sicherheitshandbuch“ dem steigenden Interesse aus der Wirtschaft Rechnung getragen, um in der vorliegenden Version „Österreichisches Informationssicherheitshandbuch“ auf die umfassende Bedeutung von Information - unabhängig von ihrer Gestalt - einzugehen.

Selbstverständlich betreffen solche Weiterentwicklungen vor allem die Inhalte: Ist es doch die rasante Entwicklung im Bereich der Informationstechnologie (IT), welche sowohl in der öffentlichen Verwaltung als auch in der Privatwirtschaft zu bemerkenswerten Innovationsschüben führt, sowohl für die rechtmäßigen Besitzer/innen der Information wie auch für die potentiell unrechtmäßigen. Es gibt nicht nur immer wieder neue Technologien, sondern auch völlig neue Anwendungsgebiete wie z.B. E-Government. Die steigende Vernetzung führt dazu, dass Information „ortslos“ wird - es ist unerheblich wo diese bzw. ihr/e Nutzer/in sich gerade physisch befinden.

Gleichzeitig steigt das Risikopotential. Am Beispiel der Spam-E-Mails kann man erkennen, wie schnell ein zunächst harmlos erscheinendes Phänomen zu einem massiven Problem wurde. Und schließlich ist es immer noch die Person, der besonderes Augenmerk zu schenken ist - sie entwickelt sich nicht so rasant weiter wie die Technik; auf „typische“ Verhaltensmuster ist Verlass - sonst wären E-Mail-Würmer oder die jüngsten Phishing-Angriffe nicht so problematisch.

Ein Sicherheitshandbuch kann somit seinen Zweck nur dann erfüllen, wenn es regelmäßig der aktuellen Entwicklung Rechnung trägt und daher immer wieder überarbeitet, ergänzt und ggf. neu ausgerichtet wird. Das war die Motivation, die vorliegende Version herauszugeben.

Schwerpunktmäßig soll damit Unterstützung geboten werden, um:

- relevante Sicherheitsziele und -strategien zu ermitteln
- eine organisationsspezifischen Informationssicherheitspolitik zu erstellen
- spezifisch geeignete Sicherheitsmaßnahmen auszuwählen und zu realisieren
- Informationssicherheit im laufenden Betrieb zu gewährleisten
- Kenntnis international üblicher Good-Practices im Bereich der Informationssicherheit zu erlangen.

Das Informationssicherheitshandbuch besteht aus zwei Teilen:

Der erste Teil "Informationssicherheitsmanagement" beschreibt den grundlegenden Vorgang, Informationssicherheit in einer Behörde, Organisation bzw. einem Unternehmen zu etablieren und bietet eine konkrete Anleitung, den umfassenden und kontinuierlichen Sicherheitsprozess zu entwickeln.

Der zweite Teil mit dem Titel "Informationssicherheitsmaßnahmen" beschreibt die konkreten Einzelmaßnahmen auf organisatorischer, personeller, infrastruktureller und technischer Ebene, sodass den spezifischen Bedrohungen angemessene Standardsicherheitsmaßnahmen für IT-Systeme und Informationen entgegengesetzt werden können. Dabei wird besonders auf die spezifisch österreichischen Anforderungen, Regelungen und Rahmenbedingungen, aber auch auf die durchgängige Einbeziehung des gesamten Lebenszyklus der jeweiligen Systeme, von der Entwicklung bis zur Beendigung des Betriebs, eingegangen. Ein eigenes Kapitel wurde der "Industriellen Sicherheit" gewidmet, das Unterstützung für die Erstellung einer Sicherheits-unbedenklichkeitsbescheinigung und eine Übersicht aller für industrielle Sicherheit relevanten Vorgabedokumente aus dem nationalen, EU- und NATO-Bereich gibt. Als komfortable Erleichterung bietet die elektronische Version des Handbuchs die Möglichkeit, automatisiert die für spezielle Szenarien notwendigen bzw. maßgeblichen Kapitel auswählen zu lassen, indem zuvor organisationsbedingte Parameter vorgegeben werden.

Neuerungen in der Version 2.3

Das frühere IT-Sicherheitshandbuch wurde zum Informationssicherheitshandbuch weiterentwickelt. Das primäre Thema ist daher die Sicherheit der Information unter Verwendung sicherer Technologien, welche auch über die reine Informationstechnologie hinausgehen. Informationssicherheit bedeutet auch Umgang mit klassifizierten Informationen (nach nationalen, EU- und NATO-Vorgaben). Hievon sind vor allem Behörden und solche Unternehmen betroffen, welche bei Ausschreibungen mit klassifizierten Informationen zu tun haben. Die industrielle Sicherheit wird in einem eigenen Kapitel des Informationssicherheitshandbuches behandelt.

Die Bedürfnisse der Wirtschaft bzw. Industrie werden in allen Teilen berücksichtigt: so wurde die elektronische Form so umgestaltet, dass eine einfache Anpassung und Adaptierung an die Anforderungen von Unternehmen möglich ist. Die Maßnahmen für Checklisten können nun auf drei Detaillierungsebenen ausgewählt werden. Die elektronische Version kann nun noch einfacher lokal auf einem Anwender-PC oder in einem Behörden- oder Firmennetzwerk installiert werden. Mit der Einarbeitung der aktuellen IKT-Board Beschlüsse ist nun auch der Teil 2 wieder auf dem aktuellsten Stand für den Einsatz in der Verwaltung.

Anwendungsbereich

Das Informationssicherheitshandbuch versteht sich als Sammlung von Leitlinien und Empfehlungen, die entsprechend den spezifischen Anforderungen und Bedürfnissen in einer Einsatzumgebung angepasst werden müssen. Es stellt eine Ergänzung zu den bestehenden Regelungen und Vorschriften (Datenschutzgesetz, Informationssicherheitsgesetz, Verschlusssachenvorschriften, Amtsgeheimnis, ...) dar und setzt diese weder außer Kraft noch steht es zu ihnen im Widerspruch.

Durch die Aktualisierung und Erweiterung auf Informationssicherheit stellt das Informationssicherheitshandbuch nun für eine noch breitere Zielgruppe das ideale Informationssicherheits-Werkzeug dar.

Kompatibilität mit internationalen Aktivitäten

Seit einigen Jahren werden auf nationaler und internationaler Ebene verstärkt Anstrengungen unternommen, einheitliche methodische Vorgehensweisen zur Etablierung von Informationssicherheit sowie Standard-Maßnahmenkataloge zu erarbeiten. Im Informationssicherheitshandbuch wird versucht, diesen internationalen Entwicklungen so weit wie möglich Rechnung zu tragen. Bei der Erstellung der Vorgehensweisen und Maßnahmenbeschreibungen wurde daher auch auf bewährte und etablierte Quellen zurückgegriffen, die im Einzelnen im Anhang des Handbuches angeführt sind. Insbesondere darf dem deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) für dessen Zustimmung zur Nutzung des Grundschutzhandbuches gedankt werden, das eine wichtige Basis für das vorliegende Handbuch darstellt. Im Bereich der Informationssicherheit bzw. für die industrielle Sicherheit sind die Vorgabedokumente der EU und NATO maßgeblich.

Sicherstellung der Aktualität

Um die Aktualität der beschriebenen Maßnahmen sicherzustellen, wird das Österreichische Informationssicherheitshandbuch regelmäßig überarbeitet und aktualisiert. Von besonderer Bedeutung ist dabei ein Feedback über die Erfahrungen mit der Anwendung des Handbuches in der Praxis. Alle Personen, die das Handbuch anwenden, werden daher eingeladen, diesbezügliche Anregungen und Erfahrungen jenen, die das Handbuch verfasst haben, mitzuteilen.

1 Informationssicherheitsmanagement in der Praxis

Information stellt heute sowohl für die öffentliche Verwaltung als auch für Organisationen der Privatwirtschaft einen wichtigen Wert dar. Die Erfüllung der Geschäftsprozesse ist ohne die Korrektheit, Vertraulichkeit und Verfügbarkeit der Informationen oft nicht mehr möglich. Information kann dabei in unterschiedlicher Form existieren – elektronisch gespeichert oder übertragen, geschrieben, als Bild oder in gesprochener Form. Die Tatsache, dass weite Bereiche des täglichen Lebens ohne den Einsatz von informationstechnischen Systemen heute nicht mehr funktionsfähig sind, rückt die Frage nach der Sicherheit der Informationen und der Informationstechnologie zunehmend in den Brennpunkt des Interesses.

Dabei darf sich Sicherheit nicht auf einzelne Teilaspekte, wie die Verschlüsselung vertraulicher Daten oder die Installation von Firewalls beschränken, sondern muss integraler Bestandteil eines modernen IKT-(Informations- und Kommunikationstechnologie-)Konzeptes sein. Methodisches Sicherheitsmanagement ist zur Gewährleistung umfassender und angemessener Informationssicherheit unerlässlich.

Das gegenständliche Handbuch beschreibt die Vorgehensweise zur Etablierung eines umfassenden Informationssicherheitsmanagementsystems (ISMS). Dabei wird Information unabhängig von ihrer Darstellungsform betrachtet, also elektronisch gespeicherte und verarbeitete Information genauso wie Information in schriftlicher oder gesprochener Form.

Die hier dargestellte Vorgehensweise wird für die österreichische Bundesverwaltung sowie für andere Bereiche der öffentlichen Verwaltung bzw. für die Privatwirtschaft zur Anwendung empfohlen.

1.1 Ziele und Aufgaben des Informationssicherheitsmanagements

Informationssicherheitsmanagement ist ein kontinuierlicher Prozess, der die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen in einer Organisation gewährleisten soll. Dies soll durch die Etablierung eines Informationssicherheitsmanagementsystems (ISMS) erreicht werden.

Zu den Aufgaben des Informationssicherheitsmanagements gehören:

- Festlegung der Sicherheitsziele und -strategien der Organisation,
- Ermittlung und Bewertung der Informationssicherheitsrisiken (information security risk assessment),
- 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 (information security incident handling).

Informationssicherheit ist immer eine Management-Aufgabe. Nur wenn die Leitung einer Organisation voll hinter den Sicherheitszielen und den damit verbundenen Aktivitäten steht, kann diese Aufgabe erfolgreich wahrgenommen werden.

1.2 Zielsetzungen des Handbuches

Das vorliegende Informationssicherheitshandbuch soll es Sicherheitsverantwortlichen und Führungskräften ermöglichen, die für ihren Bereich relevanten Informationssicherheitsziele und -strategien zu ermitteln, eine organisationsweite Informationssicherheitspolitik zu erstellen, geeignete und angemessene Sicherheitsmaßnahmen auszuwählen und zu realisieren sowie Informationssicherheit im laufenden Betrieb zu gewährleisten. Darüber hinaus soll das Handbuch dazu beitragen, eine einheitliche Vorgehensweise und Sprachregelung im Bereich der Informationssicherheit zu entwickeln, wobei aber größtmögliche Flexibilität zur Umsetzung der unterschiedlichen Sicherheitsanforderungen der einzelnen Organisationen bzw. Organisationseinheiten (OEs) gewahrt bleiben soll.

Ziel ist es, Informationssicherheit zu einem integralen Bestandteil der Geschäftsprozesse einer Organisation zu machen.

Einige generelle Anmerkungen:

Abgrenzung IT-Sicherheit und Informationssicherheit:

Die Frage der Definition dieser beiden Begriffe und ihrer Abgrenzung voneinander war in den vergangenen Jahren oft Gegenstand lebhafter Diskussionen. Dabei ist auch ein gewisser Bedeutungswandel bei diesen Begriffen festzustellen: Verstand man von einigen Jahren unter “IT-Sicherheit” im Wesentlichen den Schutz von IT-Systemen (und damit den auf ihnen verarbeiteten Informationen) und unter “Informationssicherheit” den Schutz von Informationen unabhängig von ihrer Darstellungsform (also elektronisch, schriftlich, bildhaft oder gesprochen), so sind diese beiden Begriffe mittlerweile fast synonym zu sehen: auch in der IT-Sicherheit sind Fragen zu behandeln, wie Information an sich geschützt werden kann (etwa wie mit Papierausdrucken von vertraulichen Informationen umzugehen ist), während umgekehrt die Sicherheit von elektronisch gespeicherten und verarbeiteten Informationen ohne die technische Sicherung der zugrunde liegenden IKT-(Informations- und Kommunikationstechnologie-)Systeme nicht zu erreichen ist. Die Grenzen sind also fließend. International hat sich in den letzten Jahren eher der Begriff “Informationssicherheit” als der umfassendere etabliert. Dieser Entwicklung Rechnung tragend wird das bisherige “Österreichische IT-Sicherheitshandbuch” mit der vorliegenden Version in “Österreichisches Informationssicherheitshandbuch” umbenannt.

Scope:

Inhaltlich behandelt das vorliegende Handbuch den gesamten Bereich der Informationssicherheit. Information wird dabei wie oben diskutiert umfassend gesehen: in elektronisch gespeicherter oder übertragener Form, sowie auch schriftliche, gesprochene oder bildhaft dargestellte Information. Betrachtet werden dabei auch die Sicherheit von Hardware und Software, die zur Speicherung, Verarbeitung und Übertragung von Informationen dient, sowie organisatorische, bauliche und personelle Fragen, soweit sie in direktem Zusammenhang mit der Sicherheit von IKT-Systemen und den von ihnen verarbeiteten Informationen stehen. Die Abgrenzung zu verwandten Gebieten, wie Brandschutz, Objektsicherheit, Sicherheit von kritischen Infrastrukturen oder Datenschutz ist nicht immer eindeutig, oft gibt es Überschneidungen zwischen den einzelnen Themen. Das vorliegende Handbuch geht hier einen pragmatischen Weg und versucht, Lösungen und Anleitung für die in der Praxis auftretenden Probleme zu geben.

Neu gegenüber den Vorgängerversionen ist ein spezielles Kapitel zum Thema “industrielle Sicherheit”, das die Anforderungen an Firmen, die sich um Aufträge bewerben, in denen EU-klassifizierte Informationen verarbeitet werden, darstellt.

2 Der Informationssicherheitsmanagement-Prozess

Informationen und die sie verarbeitenden Prozesse, Systeme und Netzwerke sind wichtige Werte jeder Organisation, sowohl in der öffentlichen Verwaltung als auch in der Privatwirtschaft. Informationssicherheitsmanagement (ISM) soll die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen und der sie verarbeitenden Systeme gewährleisten. Fallweise können auch weitere Anforderungen wie Zurechenbarkeit, Authentizität und Zuverlässigkeit bestehen.

Informationssicherheitsmanagement ist ein kontinuierlicher Prozess, dessen Strategien und Konzepte ständig auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf fortzuschreiben sind.

Zentrale Aktivitäten im Rahmen des ISM sind:

- die Entwicklung einer organisationsweiten Informationssicherheitspolitik
- die Durchführung einer Risikoanalyse
- die Erstellung eines Sicherheitskonzeptes
- die Umsetzung der Sicherheitsmaßnahmen
- die Gewährleistung der Informationssicherheit im laufenden Betrieb
- die kontinuierliche Überwachung und Verbesserung des ISMS

Der nachfolgend dargestellte Prozess basiert auf internationalen Standards und Leitlinien zum Informationssicherheitsmanagement, insbesondere den “Guidelines on the Management of IT Security (GMITS)” ISO/IEC TR 13335 sowie ISO/IEC 27001. Er kann sowohl auf eine gesamte Organisation als auch auf Teilbereiche Anwendung finden.

Über die Anwendung auf Ebene einzelner Behörden, Abteilungen oder anderer Organisationseinheiten ist dann im spezifischen Zusammenhang - abhängig vom IT-Konzept und den bestehenden Sicherheitsanforderungen - zu entscheiden.

Die nachfolgende Graphik zeigt die wichtigsten Aktivitäten im Rahmen des Informationssicherheitsmanagements und die eventuell erforderlichen Rückkopplungen zwischen den einzelnen Stufen.

Im Folgenden wird, wenn nicht ausdrücklich anders angeführt, allgemein der Begriff “Organisation” (oder synonym dazu “Institution”) verwendet, wobei aber zu beachten ist, dass damit beliebige Organisationseinheiten gemeint sein können.

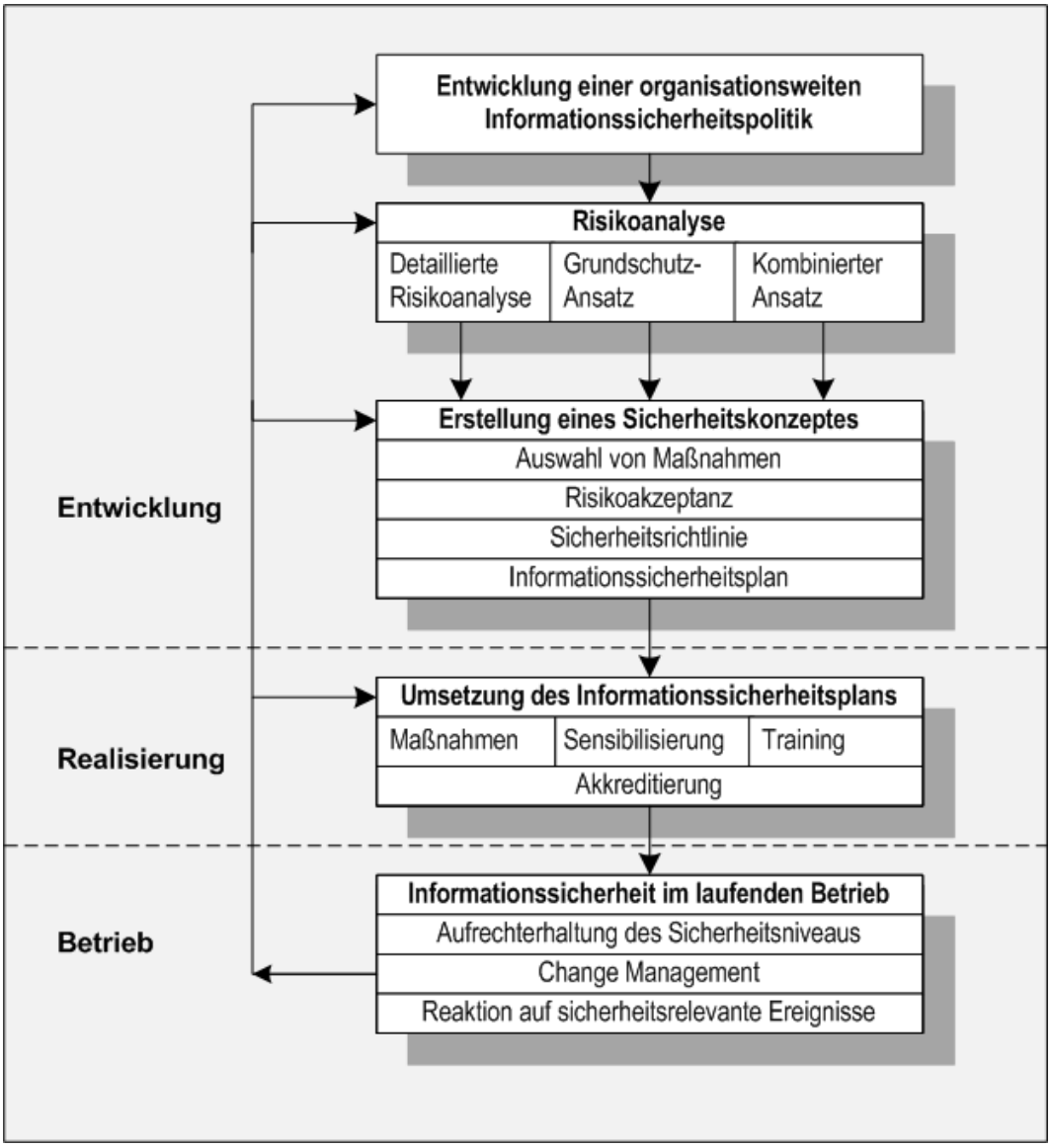

Abbildung 1: Aktivitäten im Rahmen des Informationssicherheitsmanagements

Informationssicherheitsmanagement umfasst damit folgende Schritte:

Entwicklung einer organisationsweiten Informationssicherheitspolitik

Als organisationsweite Informationssicherheitspolitik (Corporate Information Security Policy) bezeichnet man die Leitlinien und Vorgaben innerhalb einer Organisation, die unter Berücksichtigung gegebener Randbedingungen grundlegende Ziele, Strategien, Verantwortlichkeiten und Methoden für die Gewährleistung der Informationssicherheit festlegen.

Die organisationsweite Informationssicherheitspolitik (im Folgenden der Einfachheit halber als "Informationssicherheitspolitik" bezeichnet) stellt ein langfristig orientiertes Grundlagendokument dar, auf dessen Basis die Informationssicherheit einer Organisation aufgebaut wird. Details zu Sicherheitsmaßnahmen und deren Umsetzung sind nicht Bestandteil der organisationsweiten Informationssicherheitspolitik, sondern sind im Rahmen einzelner systemspezifischer Sicherheitsrichtlinien zu behandeln.

Die Informationssicherheitspolitik ist eingebettet in eine Hierarchie von Regelungen und Leitlinien. Abhängig vom IT-Konzept und den Sicherheitsanforderungen kann es auch notwendig werden, eine Hierarchie von Informationssicherheitspolitiken für verschiedene Organisationseinheiten (etwa Abteilungen, nachgeordnete Dienststellen, ...) zu erstellen.

Risikoanalyse

Eine wesentliche Aufgabe des Informationssicherheitsmanagements ist das Erkennen und Einschätzen von Sicherheitsrisiken und deren Reduktion auf ein tragbares Maß. Dieses "Informationsrisikomanagement" oder auch "Informationssicherheitsrisikomanagement" sollte Teil des generellen Risikomanagements einer Organisation und mit der dort gewählten Vorgehensweise kompatibel sein. Aus Gründen der besseren Lesbarkeit wird im Folgenden, wenn nicht explizit anders erwähnt, der Begriff "Risiko" stets im Sinne von "Informationssicherheitsrisiko" verwendet, ebenso Risikoanalyse und Risikomanagement im Sinne von Informationssicherheitsrisikoanalyse und –management. Im Rahmen des vorliegenden Handbuches werden drei Risikoanalysestrategien behandelt (s. Kapitel 4 „Risikoanalyse"): Detaillierte Risikoanalyse, Grundschutzansatz und Kombinierter Ansatz. Die Festlegung einer geeigneten Risikoanalysestrategie sollte im Rahmen der Informationssicherheitspolitik erfolgen, um ein organisationsweit einheitliches Vorgehen zu gewährleisten.

Erstellung eines Sicherheitskonzeptes

Abhängig von den Ergebnissen der Risikoanalyse werden in einem nächsten Schritt Maßnahmen ausgewählt, die die Risiken auf ein definiertes und beherrschbares Maß reduzieren sollen. Im Anschluss daran ist das verbleibende Restrisiko zu ermitteln und zu prüfen, ob dieses für die Organisation tragbar ist oder weitere Maßnahmen zur Risikoreduktion erforderlich sind.

Für wichtige IT-Systeme und Anwendungen wird die Erstellung eigener Sicherheitsrichtlinien (auch als "IT-Systemsicherheitspolitiken" bezeichnet) empfohlen. Diese sollen die grundlegenden Leitlinien zur Sicherheit eines konkreten IT-Systems bzw. einer Anwendung vorgeben sowie konkrete Sicherheitsmaßnahmen und ihre Umsetzung beschreiben. Die Sicherheitsrichtlinien müssen mit der organisationsweiten Informationssicherheitspolitik kompatibel sein.

In einem Informationssicherheitsplan werden alle kurz-, mittel- und langfristigen Aktionen festgehalten, die zur Umsetzung der ausgewählten Maßnahmen erforderlich sind.

Die Erstellung von Sicherheitskonzepten wird in Kapitel 5 „Erstellung von Sicherheitskonzepten" behandelt.

Umsetzung des Informationssicherheitsplans

Bei der Implementierung der ausgewählten Sicherheitsmaßnahmen ist zu beachten, dass die meisten technischen Sicherheitsmaßnahmen ein geeignetes organisatorisches Umfeld brauchen, um vollständig wirksam zu sein. Unabdingbare Voraussetzung für eine erfolgreiche Umsetzung des Informationssicherheitsplanes in der Praxis sind auch entsprechende Sensibilisierungs- und Schulungsmaßnahmen. Weiters ist festzulegen, wie die Effizienz und Effektivität der ausgewählten Sicherheitsmaßnahmen beurteilt werden kann. Dies erfolgt durch die Definition geeigneter Kennzahlen.

Kapitel 6 „Umsetzung des Informationssicherheitsplanes" des vorliegenden Handbuches behandelt diese Umsetzungsfragen.

Informationssicherheit im laufenden Betrieb

Umfassendes Informationssicherheitsmanagement beinhaltet nicht zuletzt auch die Aufgabe, die Sicherheit im laufenden Betrieb aufrechtzuerhalten und gegebenenfalls veränderten Bedingungen anzupassen.

Zu den erforderlichen Follow-Up-Aktivitäten zählen (s. Kapitel 7 „Informationssicherheit im laufenden Betrieb“):

- Die Aufrechterhaltung des erreichten Sicherheitsniveaus
  Dies umfasst:
  - Wartung und administrativen Support von Sicherheitseinrichtungen,
  - die Messung der Effektivität der ausgewählten Sicherheitsmaßnahmen anhand definierter Kennzahlen (Information Security Measurement),
  - die Überprüfung von Maßnahmen auf Übereinstimmung mit der Informations-Sicherheitspolitik (Security Compliance Checking) sowie
  - die fortlaufende Überwachung der IT-Systeme (Monitoring)
- umfassendes Change Management
- eine angemessene Reaktion auf sicherheitsrelevante Ereignisse (Incident Handling)

3 Entwicklung einer organisationsweiten Informationssicherheitspolitik

Die Informationssicherheitspolitik bildet die Basis für die Entwicklung und die Umsetzung eines risikogerechten und wirtschaftlich angemessenen Informationssicherheitskonzeptes. Sie stellt ein Grundlagendokument dar, das die sicherheitsbezogenen Ziele, Strategien, Verantwortlichkeiten und Methoden langfristig und verbindlich festlegt.

Die organisationsweite Informationssicherheitspolitik soll allgemeine Festlegungen treffen, die den Schutz der Informationen und der IT-Systeme innerhalb einer Organisation gewährleisten. Diese Richtlinien werden in den nachgeordneten Sicherheitsrichtlinien, etwa der E-Mail-Sicherheitsrichtlinie oder der Netzwerksicherheitsrichtlinie, konkret umgesetzt.

Ziel dieses Abschnittes ist es, die Erarbeitung einer Informationssicherheitspolitik zu unterstützen.

Das folgende Kapitel gibt eine Anleitung zur Erstellung einer derartigen Politik und legt die wesentlichen Inhalte fest. Diese sind:

- Informationssicherheitsziele und -strategien
- Erklärung der Leitungsebene über die Unterstützung der Ziele des Informationssicherheits-managements (Management Commitment)
- Organisation und Verantwortlichkeiten für Informationssicherheit
- Risikoanalysestrategien, akzeptables Restrisiko und Risikoakzeptanz
- Klassifizierung von Daten
- Klassifizierung von IT-Anwendungen und IT-Systemen, Grundzüge der Business Continuity Planung
- Aktivitäten zur Überprüfung und Aufrechterhaltung der Sicherheit
- Verweise auf weitere Dokumente zum Thema Informationssicherheit, wie etwa Sicherheitsrichtlinien

3.1 Aufgaben und Ziele einer Informationssicherheitspolitik

Eine organisationsweite Informationssicherheitspolitik hat die Aufgabe, die Vertraulichkeit, Integrität und Verfügbarkeit der Information in einer Organisation sicherzustellen.

Dabei gilt:

- Die Informationssicherheitspolitik wird als schriftliches Dokument erstellt und bildet die Grundlage des Informationssicherheitsmanagements.
- Die Informationssicherheitspolitik legt Leitlinien fest, schreibt aber keine Implementierung vor.
- Das Management unterstützt und fördert die Aktivitäten zum Informationssicherheits-management. Die Informationssicherheitspolitik enthält ein explizites Statement des Managements über die Unterstützung der Informationssicherheitsziele (Management Commitment).
- Die Informationssicherheitspolitik wird offiziell verabschiedet und in Kraft gesetzt.
- Jede/r Mitarbeiter/in muss Kenntnis über die wichtigsten Inhalte der Informationssicherheitspolitik haben. Die direkt mit Informationssicherheit beschäftigten Mitarbeiter/innen müssen im Besitz einer aktuellen Version der Informationssicherheitspolitik sein.

Geltungsbereich

Im Bereich der öffentlichen Verwaltung ist zumindest auf Ressortebene eine eigene, ressortspezifische Informationssicherheitspolitik zu erstellen. Bei Bedarf können aus dieser weitere Informationssicherheitspolitiken, etwa auf Behörden- oder Abteilungsebene, abgeleitet werden.

Im Bereich der Privatwirtschaft wird die Erarbeitung einer organisationsweiten Informationssicherheitspolitik zumindest für große bis mittlere Unternehmen empfohlen. Abhängig von der Unternehmensstruktur und den strategischen Zielen kann die Erstellung einer Informationssicherheitspolitik auch für kleinere Unternehmen empfehlenswert sein.

3.2 Die Inhalte der Informationssicherheitspolitik

Der folgende Abschnitt beschreibt, welche Themenbereiche im Rahmen der Informationssicherheitspolitik in jedem Fall angesprochen werden sollten, und gibt Anleitungen zur Erstellung dieses Dokumentes. Über die angeführten Themenbereiche hinaus können organisationsspezifisch weitere wichtige Sicherheitsthemen in die Informationssicherheitspolitik aufgenommen werden.

3.2.1 Informationssicherheitsziele und -strategien

Schritt 1: Festlegung der wesentlichen Informationssicherheitsziele

Im Rahmen der Erstellung der Informationssicherheitspolitik sind zunächst die spezifischen Sicherheitsziele der Organisation zu erarbeiten, die mit dieser Politik erreicht werden sollen.

Beispiele für solche Ziele sind:

- Gewährleistung der aus gesetzlichen Vorgaben resultierenden Anforderungen
- Gewährleistung des Vertrauens der Öffentlichkeit in die betroffene Organisation bzw. die öffentliche Verwaltung im Allgemeinen
- Hohe Verlässlichkeit des Handelns, insbesondere in Bezug auf Vertraulichkeit, Richtigkeit und Rechtzeitigkeit.

Dies erfordert:

- Vertraulichkeit der verarbeiteten Informationen
- Einhaltung aller Gesetze, Verträge und Regelungen (etwa des Datenschutzgesetzes, des Informationssicherheitsgesetzes, von SLAs und Normen)
- Korrektheit, Vollständigkeit und Authentizität der Informationen (Integrität der IT)
- Rechtzeitigkeit (Verfügbarkeit der Daten und Services)
- Sicherung der investierten Werte
- Sicherstellung der Kontinuität der Arbeitsabläufe
- Reduzierung der im Schadensfall entstehenden Kosten (Schadensvermeidung und Schadensbegrenzung)
- Gewährleistung des besonderen Prestiges

Neben diesen eher allgemein gültigen Zielen sind die organisationsspezifischen Sicherheitsziele - bezugnehmend auf die spezifischen Aufgaben und Projekte - zu formulieren.

Zur Präzisierung dieser Ziele können folgende Fragen hilfreich sein:

- Welche Informationen sind besonders schützenswert?
- Welche Auswirkungen hätte eine gravierende Verletzung der Sicherheit dieser Informationen (Verlust von Vertraulichkeit, Integrität und/oder Verfügbarkeit)?
- Welche wesentlichen Entscheidungen hängen von der Genauigkeit, Integrität oder Verfügbarkeit dieser Informationen ab?
- Welche essentiellen Aufgaben der betreffenden Organisation können bei Kompromittierung dieser Informationen nicht mehr durchgeführt werden?
- Welche essentiellen Aufgaben der betreffenden Organisation können ohne IT-Unterstützung nicht mehr durchgeführt werden?

Schritt 2: Festlegung des angestrebten Sicherheitsniveaus

In diesem Schritt ist festzulegen, welches Sicherheitsniveau in Bezug auf

- Vertraulichkeit,
- Integrität und
- Verfügbarkeit

angestrebt werden soll.

Schritt 3: Ausarbeitung von Strategien für das Informationssicherheitsmanagement

Die Sicherheitsstrategie legt fest, wie die definierten Sicherheitsziele erreicht werden können.

Eine organisationsweite Informationssicherheitspolitik kann und soll lediglich eine High-Level-Beschreibung der gewählten Strategien beinhalten, Detailbeschreibungen sind Aufgabe der nachgeordneten Sicherheitsrichtlinien.

Beispiele für Strategien für das Informationssicherheitsmanagement sind:

- eine klare Zuordnung aller Verantwortlichkeiten im Informationssicherheitsprozess,
- die Einführung eines QM-Systems,
- die Entwicklung von Sicherheitsrichtlinien für die wichtigsten Systeme, Services und Anwendungen
- die Etablierung eines organisationsweiten Incident Handling Plans,
- Orientierung an internationalen Richtlinien und Standards,
- Informationssicherheit als integraler Bestandteil des gesamten Lebenszyklus eines IT-Systems,
- die Förderung des Sicherheitsbewusstseins aller Mitarbeiter/innen.

3.2.2 Management Commitment

Die Leitungsebene soll im Rahmen der Informationssicherheitspolitik ein klares Bekenntnis zur Bedeutung der Informationssicherheit für die Institution abgeben. Dazu zählen insbesondere die Unterstützung der Ziele und Prinzipien der Informationssicherheit und die Erklärung ihrer Übereinstimmung mit den Geschäftszielen und -strategien.

3.2.3 Organisation und Verantwortlichkeiten für Informationssicherheit

Um eine Berücksichtigung aller wichtigen Aspekte und eine effiziente Erledigung sämtlicher anfallender Aufgaben zu gewährleisten, ist es erforderlich, die Rollen und Verantwortlichkeiten aller in den Informationssicherheitsprozess involvierten Personen klar zu definieren.

Die Organisation des ISM ist für jede Institution - entsprechend ihrer Größe, Struktur und Aufgaben - spezifisch festzulegen und in der Informationssicherheitspolitik festzuschreiben.

Zentrale Aufgaben im Informationssicherheitsmanagement-Prozess übernehmen dabei

- das Informationssicherheitsmanagement-Team,
- die IT-Sicherheitsbeauftragten (zur Wahl der Bezeichnung s. unten),
- die Bereichs-IT-Sicherheitsbeauftragten und
- die Applikations-/Projektverantwortlichen.

Auf der Ebene der Bundesverwaltung ist zusätzlich in jedem Ressort die Person einer/eines Informationssicherheitsbeauftragten gemäß Informationssicherheitsgesetz InfoSiG BGBl. I Nr. 23/2002 i.d.g.F., § 7 einzurichten. Weiters werden für diesen Bereich durch das IKT-Board verbindliche Regelungen zur IKT-Sicherheit vorgegeben.

Es ist zu betonen, dass es sich bei diesen Funktionen bzw. Gremien, die im Folgenden näher beschrieben werden, um Rollen handelt, die - abhängig von der Größe und den Sicherheitsanforderungen einer Organisation - durchaus auch von mehreren Personen wahrgenommen werden können. In diesem Fall ist auf eine genaue Trennung der Kompetenzen und Verantwortlichkeiten Bedacht zu nehmen. Genauso ist es möglich, dass eine Person eine dieser Rollen zusätzlich zu anderen Aufgaben übernimmt. So könnte beispielsweise ein Systemadministrator als Bereichs-IT-Sicherheitsbeauftragte/r für dieses System agieren. Dabei ist aber unbedingt darauf zu achten, dass ausreichend Zeit für die sicherheitsrelevanten Tätigkeiten zur Verfügung steht und es zu keinen Kollisionen von Verantwortlichkeiten oder Interessen kommt.

Nachfolgend werden die wichtigsten typischen Aufgaben und Verantwortlichkeiten dieser Funktionen bzw. Gremien kurz beschrieben. Eine detaillierte, auf die speziellen Aufgaben und Anforderungen der betreffenden Organisation abgestimmte Beschreibung ist im Rahmen der organisationsweiten Informationssicherheitspolitik zu geben.

Die/der IT-Sicherheitsbeauftragte

Die/der IT-Sicherheitsbeauftragte ist die zentrale Ansprechperson für alle Informations- und IT-Sicherheitsfragen innerhalb einer Organisation und trägt die fachliche Verantwortung für diesen Bereich.

Anmerkung: Die Bezeichnung “IT-Sicherheitsbeauftragte/r” für die Person einer/eines zentralen Sicherheitsverantwortlichen wurde zum einen gewählt, weil es sich um einen in vielen Institutionen sowohl des Behörden- als auch des Privatwirtschaftsbereiches eingeführten Begriff handelt, zum anderen, um diese Rolle gegenüber der Rolle der/des Informationssicherheitsbeauftragten gemäß InfoSiG abzugrenzen, der/dem ganz spezifische Aufgaben lt. Gesetz zukommen.

Zu den Pflichten der/des IT-Sicherheitsbeauftragten gehören:

- die verantwortliche Mitwirkung an der Erstellung des Informationssicherheitskonzeptes,
- die Gesamtverantwortung für die Realisierung der ausgewählten Sicherheitsmaßnahmen,
- die Planung und Koordination von Schulungs- und Sensibilisierungsveranstaltungen,
- die Gewährleistung der Informationssicherheit im laufenden Betrieb sowie
- die Verwaltung der für Informationssicherheit zur Verfügung stehenden Ressourcen.

Die/der IT-Sicherheitsbeauftragte kann einzelne Aufgaben delegieren, die Gesamtverantwortung für die Informationssicherheit verbleibt aber bei dieser Person.

Der Funktion der/des IT-Sicherheitsbeauftragten kommt eine zentrale Bedeutung zu. Daher sollte diese Rolle in jedem Fall - also auch bei kleinen Organisationen - definiert und klar einer Person, eventuell zusätzlich zu anderen Aufgaben, zugeordnet sein.

Das Informationssicherheitsmanagement-Team

Das Informationssicherheitsmanagement-Team ist verantwortlich für die Regelung der organisationsweiten Informationssicherheitsbelange sowie für die Erarbeitung von Plänen, Vorgaben und Richtlinien zur Informationssicherheit.

Zu den Aufgaben des Teams zählen typischerweise:

- die Festlegung der Informationssicherheitsziele der Organisation,
- die Entwicklung einer organisationsweiten Informationssicherheitspolitik,
- Unterstützung und Beratung bei der Erstellung des Informationssicherheitskonzeptes,
- die Überprüfung des Konzeptes auf Erreichung der Informationssicherheitsziele,
- die Förderung des Sicherheitsbewusstseins in der gesamten Organisation sowie
- die Festlegung der personellen und finanziellen Ressourcen für Informationssicherheit.

Zusammensetzung des Teams:

Die genaue Festlegung der Zusammensetzung sowie der Aufgaben und Verantwortlichkeiten des Informationssicherheitsmanagement-Teams haben im Rahmen der Informationssicherheitspolitik zu erfolgen.

Generell ist zu empfehlen, dass die/der IT-Sicherheitsbeauftragte sowie ein/e Vertreter/in der IT-Anwender/innen dem Informationssicherheitsmanagement-Teams angehören.

Die Bereichs-IT-Sicherheitsbeauftragten

Die Komplexität moderner IT-Systeme erfordert zur Gewährleistung eines angemessenen Sicherheitsniveaus tief gehende Systemkenntnisse. Wenn mehrere unterschiedliche Systemplattformen zum Einsatz kommen, können diese von einer einzelnen Person oft nicht mehr abgedeckt werden. Daher wird es in vielen Fällen empfehlenswert sein, Bereichs-IT-Sicherheitsbeauftragte zu definieren. Diese haben die fachliche Verantwortung für alle IT-Sicherheitsbelange in einem bestimmten Bereich. Ein Bereich kann beispielsweise ein IT-System oder eine Betriebssystemplattform sein, auch eine Zuordnung nach Abteilungen oder Betriebsstandorten ist denkbar.

Zu den Aufgaben einer/s Bereichs-IT-Sicherheitsverantwortlichen zählen

- die Mitwirkung bei den ihren/seinen Bereich betreffenden Teilen des Informationssicherheitskonzeptes,
- die Erarbeitung eines detaillierten Planes zur Realisierung der ausgewählten Sicherheitsmaßnahmen,
- die Umsetzung dieses Planes,
- die regelmäßige Prüfung der Wirksamkeit und Einhaltung der eingesetzten Sicherheitsmaßnahmen im laufenden Betrieb,
- Information der/des IT-Sicherheitsbeauftragten über bereichsspezifischen Schulungsbedarf sowie
- Meldungen an die/den IT-Sicherheitsbeauftragte/n bei sicherheitsrelevanten Ereignissen.

Applikations-/Projektverantwortliche

Für jede IT-Anwendung und jedes IT-Projekt ist die fachliche Gesamtverantwortung und damit auch die Verantwortung für deren Sicherheit klar festzulegen.

Zu den Aufgaben einer/s Applikations- oder Projektverantwortlichen zählen insbesondere

- die Festlegung der Sicherheits- und Qualitätsanforderungen der Applikation bzw. des Projektes,
- die Klassifizierung der verarbeiteten Daten,
- die Vergabe von Zugriffsrechten sowie
- organisatorische und administrative Maßnahmen zur Gewährleistung der IT-Sicherheit in der Projektentwicklung und im laufenden Betrieb.

Neben den oben beschriebenen Rollen gibt es im Bereich der Bundesverwaltung eine spezielle, per Gesetz festgelegte Rolle – die/den Informationssicherheitsbeauftragte/n.

Die/der Informationssicherheitsbeauftragte

Auf Ressortebene sind gemäß Informationssicherheitsgesetz InfoSiG BGBl. I Nr. 23/2002 Informationssicherheitsbeauftragte zu bestellen.

Aufgaben der/des Informationssicherheitsbeauftragten sind:

- die Überwachung der Einhaltung der Bestimmungen des Informationssicherheitsgesetzes InfoSiG BGBl. I Nr. 23/2002, der Informationssicherheitsverordnung InfoSiV BGBl. I Nr. 548/2003 i.d.g.F. und der sonstigen Informationssicherheitsvorschriften,
- die periodische Überprüfung der Sicherheitsvorkehrungen für den Schutz von (lt. InfoSiG BGBl. I Nr. 23/2002) klassifizierten Informationen,
- die Berichterstattung darüber an die Informationssicherheitskommission,
- Behebung von erkannten Mängeln,
- Sicherheitsüberprüfung von betroffenen Personen gemäß §3 Abs. 1 Z1 und 2 InfoSiG BGBl. I Nr. 23/2002,
- Information der Bundesministerin bzw. des Bundesministers des jeweiligen Ministeriums in Angelegenheiten der Informationssicherheit sowie
- Erstattung von Verbesserungsvorschlägen, falls erforderlich.

Die/der Informationssicherheitsbeauftragte ist Mitglied der Informationssicherheitskommission.

Weitere Pflichten und Verantwortungen im Bereich Informationssicherheit

Sicherheit ist nicht ausschließlich Angelegenheit der damit per Definition betrauten Personen. Jede/r Mitarbeiter/in, auch wenn sie/er nicht direkt in den Bereich Informationssicherheit involviert ist, muss ihre/seine spezifischen Pflichten und Verantwortlichkeiten im Rahmen der Informationssicherheit kennen und erfüllen. Ebenso sind die Rechte und Pflichten von externen Personen, Lieferanten und Vertragspartnern festzulegen.

Im Rahmen der organisationsweiten Informationssicherheitspolitik sind daher auch die Aufgaben und Verantwortlichkeiten folgender Personenkreise zu definieren:

- Management/Behördenleitung (”Sicherheit als Managementaufgabe”)
- DV-Entwicklung und technischer Support
- Dienstnehmer
- Leasingpersonal, externe Mitarbeiter/innen
- Lieferanten und Vertragspartner

Informationssicherheit und Datenschutz

Auch wenn die Einrichtung einer/s Datenschutzbeauftragten gesetzlich nicht gefordert ist (vgl. Datenschutzgesetz DSG 2000 BGBl. I Nr. 165/1999), ist es sinnvoll, in Organisationen, in denen personenbezogene Daten lt. DSG 2000 verarbeiten werden, die datenschutzbezogenen Aufgaben zu konzentrieren und die erforderlichen Tätigkeiten zuzuordnen. Es ist aber zu betonen, dass die Gesamtverantwortung für die Datenschutzbelange bei der Geschäftsführung verbleibt und nicht delegiert werden kann.

3.2.4 Risikoanalysestrategien, akzeptables Restrisiko und Akzeptanz von außergewöhnlichen Restrisiken

Methodisches Risikomanagement ist zur Erarbeitung eines vollständigen und organisationsweiten Informationssicherheitskonzeptes unerlässlich. Um Risiken zu beherrschen, ist es zunächst erforderlich, sie zu kennen und zu bewerten. Dazu wird in einer Risikoanalyse das Gesamtrisiko ermittelt. Ziel ist es, dieses Risiko so weit zu reduzieren, dass das verbleibende Restrisiko quantifizierbar und akzeptierbar wird.

In der Informationssicherheitspolitik sollen die Risikoanalysestrategie der Organisation sowie das akzeptable Restrisiko festgelegt werden. Weiters ist die Vorgehensweise bei der Akzeptanz von außergewöhnlichen Restrisiken zu definieren.

Im folgenden Abschnitt werden die wichtigsten Punkte, die im Rahmen der Informationssicherheitspolitik zum Thema Risikoanalyse festgelegt werden sollten, aufgeführt. Details zur Risikoanalyse sind in Kapitel 4 „Risikoanalyse“ enthalten.

Schritt 1: Festlegung der anzuwendenden Risikoanalysestrategie

Die heute gängige Praxis unterscheidet drei Varianten zur Risikoanalysestrategie einer Organisation:

- Grundschutzansatz:
  Unabhängig von den tatsächlichen Sicherheitsanforderungen werden für alle IT-Systeme Standardsicherheitsmaßnahmen (”Grundschutzmaßnahmen”) eingesetzt. Diese Vorgehensweise spart Ressourcen und führt schnell zu einem relativ hohen Niveau an Sicherheit. Der Nachteil liegt darin, dass der Grundschutzlevel für die vorhandenen Geschäftsprozesse und IT-Systeme möglicherweise nicht angemessen sein könnte.
- Detaillierte Risikoanalyse:
  Für alle Geschäftsprozesse und die sie unterstützenden IT-Systeme wird eine detaillierte Risikoanalyse durchgeführt. Diese Methode gewährleistet die Auswahl von effektiven und angemessenen Sicherheitsmaßnahmen, benötigt jedoch viel Zeit und Aufwand.
- Kombinierter Ansatz:
  In einem ersten Schritt wird in einer Schutzbedarfsfeststellung (High Level Risk Analysis) ausgehend von den Geschäftsprozessen der Schutzbedarf für die einzelnen Prozesse, die sie unterstützenden Systeme und die verarbeiteten Informationen ermittelt. Bei normalem Schutzbedarf wird von einer pauschalisierten Gefährdungslage ausgegangen, so dass auf eine detaillierte Risikoanalyse verzichtet und eine Grundschutzanalyse (s. o.) durchgeführt werden kann. Dies erlaubt eine schnelle und effektive Auswahl von grundlegenden Sicherheitsmaßnahmen bei gleichzeitiger Gewährleistung eines angemessenen Schutzniveaus. Bei hohem Schutzbedarf können wahlweise Grundschutzmaßnahmen eingesetzt oder eine detaillierte Risikoanalyse durchgeführt werden. Besteht sehr hoher Schutzbedarf, so sind die betroffenen Geschäftsprozesse und IT-Systeme einer detaillierten Risikoanalyse zu unterziehen, auf deren Basis individuelle Sicherheitsmaßnahmen ausgewählt werden.

Diese Option kombiniert die Vorteile des Grundschutzansatzes mit denen einer detaillierten Risikoanalyse und stellt heute die allgemein empfohlene Vorgehensweise dar.

Schritt 2: Festlegung des akzeptablen Restrisikos

Nach Durchführung aller ausgewählten Sicherheitsmaßnahmen verbleibt im Allgemeinen ein Restrisiko, dessen Abdeckung wirtschaftlich nicht mehr vertretbar wäre. In der Informationssicherheitspolitik sind diese akzeptablen Restrisiken so exakt wie möglich zu quantifizieren.

Schritt 3: Festlegung der Vorgehensweise zur Akzeptanz von außergewöhnlichen Restrisiken

Verbleibt nach Durchführung aller im Sicherheitsplan vorgesehenen Maßnahmen ein Restrisiko, das höher ist als das generell akzeptable und dessen weitere Reduktion technisch nicht möglich oder unwirtschaftlich wäre, so besteht in begründeten Ausnahmefällen die Möglichkeit einer bewussten Akzeptanz des erhöhten Restrisikos.

In der Sicherheitspolitik sind

- das Vorgehen bei Risiken, die in Abweichung von der generellen Sicherheitspolitik in Kauf genommen werden sollen, sowie
- die Verantwortlichkeiten dafür

festzulegen.

3.2.5 Klassifizierung von Informationen

Die Klassifizierung der verarbeiteten, gespeicherten und übertragenen Informationen in Bezug auf ihre Vertraulichkeit und Datenschutzanforderungen ist wesentliche Voraussetzung für die spätere Auswahl adäquater Sicherheitsmaßnahmen.

Daher sind in der Informationssicherheitspolitik entsprechende Sicherheitsklassen zu definieren und weiters die Verantwortlichkeiten für die Durchführung der Klassifizierung festzulegen.

3.2.5.1 Definition der Sicherheitsklassen

A) Festlegung von Klassifizierungsstufen bzgl. Vertraulichkeit (Vertraulichkeitsklassen)

Die Vertraulichkeitsklassen können als Maß dafür gesehen werden, welche Auswirkungen ein Missbrauch der Information auf die Institution haben kann.

Im Bereich der Bundesverwaltung sind die unten angeführten hierarchischen Klassen definiert. Diese Klassen sind lt. Informationssicherheitsgesetz InfoSiG BGBl. I Nr. 23/2002 gesetzlich festgelegt für "klassifizierte Informationen, die Österreich im Einklang mit völkerrechtlichen Regelungen erhalten hat".

HINWEIS: Im Sinne der Kompatibilität und Einheitlichkeit erscheint diese Klassifizierung auch für andere Daten im Bereich der Bundesverwaltung sinnvoll. Zum Zeitpunkt der Erstellung dieser Version des Sicherheitshandbuches ist jedoch eine neue „Geheimschutzverordnung" zu national klassifizierten Informationen in Arbeit. Dieser soll nicht vorgegriffen werden, weshalb hier keine Vorgaben gemacht werden.

- EINGESCHRÄNKT:
  Die unbefugte Weitergabe der Informationen würde den in Art. 20, Abs. 3 B-VG genannten Interessen zuwiderlaufen. [Anmerkung: Alle mit Aufgaben der Bundes-, Landes- und Gemeindeverwaltung betrauten Organe sowie die Organe anderer Körperschaften des öffentlichen Rechts sind, soweit gesetzlich nicht anderes bestimmt ist, zur Verschwiegenheit über alle ihnen ausschließlich aus ihrer amtlichen Tätigkeit bekannt gewordenen Tatsachen verpflichtet, deren Geheimhaltung im Interesse der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit, der umfassenden Landesverteidigung, der auswärtigen Beziehungen, im wirtschaftlichen Interesse einer Körperschaft des öffentlichen Rechts, zur Vorbereitung einer Entscheidung oder im überwiegenden Interesse der Parteien geboten ist (Amtsverschwiegenheit). ...]
- VERTRAULICH:
  Die Informationen stehen nach anderen Bundesgesetzen unter strafrechtlichem Geheimhaltungsschutz und ihre Geheimhaltung ist im öffentlichen Interesse gelegen.
- GEHEIM:
  Die Informationen sind vertraulich und ihre Preisgabe würde zudem die Gefahr einer erheblichen Schädigung der in Art. 20, Abs. 3 B-VG genannten Interessen schaffen.
- STRENG GEHEIM:
  Die Informationen sind geheim und ihr Bekannt werden würde überdies eine schwere Schädigung der in Art. 20, Abs. 3 B-VG genannten Interessen wahrscheinlich machen.

Nicht-klassifizierte Informationen werden nachfolgend auch als "OFFEN" bezeichnet.

In den übrigen Verwaltungsbereichen und in der Privatwirtschaft ist es jeder Organisation überlassen, in ihrer Informationssicherheitspolitik eine für ihre Zwecke adäquate Definition von Vertraulichkeitsklassen vorzunehmen, sofern es nicht bereits diesbezügliche Regelungen gibt. Aus Gründen der Kompatibilität wird die Anwendung des genannten Schemas in denjenigen Bereichen, in denen nicht zwingende Gründe für ein anderes Klassifizierungsschema bestehen, empfohlen. Allerdings werden Organisationen der Privatwirtschaft, sofern sie nicht besonders strenge Sicherheitsanforderungen haben, im Allgemeinen mit weniger Klassen (meist 3 oder 4) das Auslangen finden.

Im Rahmen der Informationssicherheitspolitik sollte darauf hingewiesen werden, dass die Klassifizierung der Daten sehr sorgfältig vorzunehmen ist. Nicht nur die Einstufung in eine zu niedrige Vertraulichkeitsklasse ist mit potentiellen Gefahren verbunden, auch die leichtfertige Einstufung in eine zu hohe Vertraulichkeitsklasse ist zu vermeiden, da etwa die Behandlung von geheimen Daten durchwegs mit erheblichem Aufwand verbunden ist.

B) Klassifizierung von Daten in Bezug auf Datenschutz

Werden personenbezogene Daten verarbeitet, so sind die Daten auch dahingehend zu klassifizieren. Die nachfolgende Klassifizierung gemäß Datenschutzgesetz DSG 2000 BGBl. I Nr. 165/1999 gilt sowohl für den Behörden- als auch für den privatwirtschaftlichen Bereich.

- NUR INDIREKT PERSONENBEZOGEN:
  Der Personenbezug der Daten kann mit rechtlich zulässigen Mitteln nicht bestimmt werden.
- PERSONENBEZOGEN:
  Angaben über Betroffene [Anmerkung – Betroffene: Jede vom Auftraggeber verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet werden.], deren Identität bestimmt oder bestimmbar ist.
- SENSIBEL:
  Daten über rassische und ethnische Herkunft, politische Meinungen, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugungen, Gesundheit oder Sexualleben von natürlichen Personen.

3.2.5.2 Festlegung der Verantwortlichkeiten und der Vorgehensweise

Im Rahmen der Informationssicherheitspolitik ist generell festzulegen, wer die Klassifizierung der Daten vorzunehmen hat. Dies kann in den einzelnen Organisationen unterschiedlich sein und auch von IT-System zu IT-System differieren.

Als allgemeine Richtlinie kann gelten, dass die Klassifizierung einer Information von jener Person vorzunehmen ist, von der diese Information stammt, oder, wenn diese keine eindeutigen Vorgaben gemacht hat, von jener Person in der Organisation, die diese Information von außen erhält.

Weiters ist festzulegen, in welcher Form die Klassifizierung bzw. Deklassifizierung erfolgt und wie klassifizierte Information gekennzeichnet wird.

Die/der für die Information verantwortliche Mitarbeiter/in wird oft als “Dateneigner” oder “Data Owner” bezeichnet.

3.2.5.3 Erarbeitung von Regelungen zum Umgang mit klassifizierten Informationen

In diesem Schritt ist festzulegen, wie die Information in Abhängigkeit von den Sicherheitsklassen zu behandeln ist.

Werden in einer Organisation häufig klassifizierte Informationen verarbeitet und gespeichert, so empfiehlt sich die Erarbeitung eines eigenständigen Dokumentes, in dem u.a. folgende Fragen behandelt werden:

- Kennzeichnung klassifizierter Information (sowohl elektronischer als auch nicht-elektronischer)
- Verwahrung klassifizierter Information (Zugriffsberechtigungen, etwaige Vorschriften zur Verschlüsselung)
- Übermittlung klassifizierter Information (mündliche Weitergabe, persönliche Weitergabe, Versendung durch Post oder Kurier, elektronische Übertragung, über welche Verbindungen, Vorschriften zur Verschlüsselung)
- Registrierung klassifizierter Information
- Ausdruck klassifizierter Information (auf welchen Drucker, durch wen)
- Backup (Klartext, chiffriert, Schutz der Backup-Medien)
- Aufbewahrung / Wiederverwendung / Vernichtung von Datenträgern mit klassifizierter Information
- Weitergabe klassifizierter Information (an wen, durch wen, unter welchen Bedingungen)
- Deklassifizierung klassifizierter Information (wann, durch wen)

Näheres zum Umgang mit klassifizierten Informationen siehe Kapitel 8.

3.2.6 Klassifizierung von IT-Anwendungen und IT-Systemen, Grundzüge der Business Continuity Planung

Ziel der Business Continuity Planung ist es, die Verfügbarkeit der wichtigsten Applikationen und Systeme innerhalb eines definierten Zeitraumes zu gewährleisten sowie Vorkehrungen zur Schadensbegrenzung im Katastrophenfall zu treffen ("Gewährleistung eines kontinuierlichen Geschäftsbetriebes").

Dabei wird unterschieden zwischen der Aufrechterhaltung der Betriebsverfügbarkeit im Fall von Störungen oder Bedienungsfehlern (im Folgenden auch als Business Contingency Planung bezeichnet) sowie der Gewährleistung eines Notbetriebes und des geordneten Wiederanlaufs im Katastrophenfall (Katastrophenvorsorge, K-Planung).

Im Rahmen der Informationssicherheitspolitik sind die Verfügbarkeitsklassen für IT-Anwendungen und die diesen Anwendungen zugrunde liegenden IT-Systeme sowie der darauf verarbeiteten oder gespeicherten Informationen zu definieren. Die Business Continuity Planung selbst ist nicht Bestandteil der Informationssicherheitspolitik, sondern muss in den entsprechenden weiteren Aktivitäten erfolgen.

Nachfolgend ein Beispiel für ein solches Klassifizierungsschema – basierend auf den Katastrophenvorsorge- und Ausfallssicherheitsüberlegungen im IT-Bereich des Bundeskanzleramtes [K-Fall]:

- Betriebsverfügbarkeitskategorie 1 – Keine Vorsorge (unkritisch):
  Für die IT-Anwendung werden keine besonderen Vorkehrungen getroffen. Es ist ein Datenverlust bzw. Ausfall der IT-Anwendung unbestimmter Dauer denkbar. Eine Behinderung in der Wahrnehmung der Aufgaben der betroffenen Verwaltungsstelle entsteht durch den Ausfall bzw. Datenverlust nicht.
- Betriebsverfügbarkeitskategorie 2 – Offline Sicherung:
  Es sind die gängigen Sicherungsmaßnahmen für die IT-Anwendung vorgesehen, ein Datenverlust ist auszuschließen. Die IT-Anwendung kann bei technischen Problemen erst nach deren Behebung am ursprünglichen Produktivsystem in Betrieb genommen werden. Die Sicherung wird an einen externen Ort ausgelagert.
- Betriebsverfügbarkeitskategorie 3 – Redundante Infrastruktur:
  Die Infrastruktur für die IT-Anwendung ist derart ausgelegt, dass bei Ausfall einer IT-Komponente der Betrieb durch redundante Auslegung ohne Unterbrechung fortgesetzt werden kann.
- Betriebsverfügbarkeitskategorie 4 – Redundante Standorte:
  Die IT-Infrastruktur sowie die darauf aufsetzende IT-Anwendung ist auf zwei Standorte verteilt, so dass bei Betriebsunterbrechung des einen Standortes die IT-Anwendung uneingeschränkt am zweiten Standort weiter betrieben werden kann.

Zusätzlich zu den vier genannten Kategorien ist noch die Zusatzqualität „K-Fall sicher“ definiert, welche auch die Anforderungen in Katastrophenfällen berücksichtigt:

- K-Fall sicher (K2 bis K4):
  Die IT-Anwendung ist derart konzipiert, dass zumindest ein Notbetrieb in einer Zero-Risk-Umgebung möglich ist. Dazu werden die Daten je nach Aktualisierungsgrad laufend in die Zero-Risk-Umgebung transferiert und der Betrieb der IT-Anwendung derart gestaltet, dass ein Wiederaufsetzen eines definierten Notbetriebes in der Zero-Risk-Umgebung umgehend möglich ist.

In Summe ergibt eine derartige Einstufung die Verfügbarkeitsklassen 1 bis 4 und K2 bis K4. Die Zusatzoption „K-Fall sicher“ in Verbindung mit Betriebsverfügbarkeitskategorie 1 ist nicht sinnvoll.

Für nähere Informationen und für Klassifizierungsbeispiele siehe Abschnitt 7.2 im 2. Teil des vorliegenden Handbuches.

3.2.7 Überprüfung und Aufrechterhaltung der Sicherheit

Informationssicherheit ist kein durch einmalige Anstrengungen erreichbarer und dann unveränderbarer Zustand. Umfassendes Informationssicherheitsmanagement beinhaltet vielmehr auch die Aufgabe, Informationssicherheit im laufenden Betrieb kontinuierlich zu überprüfen und aufrechtzuerhalten.

Die Informationssicherheitspolitik muss daher Leitlinien und Kennzahlen zur Bewertung der Sicherheit hinsichtlich Angemessenheit, Wirksamkeit und Ordnungsmäßigkeit der eingesetzten Maßnahmen sowie deren Übereinstimmung mit der Informationssicherheitspolitik und dem Informationssicherheitskonzept vorgeben.

3.2.8 Dokumente zur Informationssicherheit

Abschließend sollte ein Verweis auf die wichtigsten Dokumente zum Informationssicherheitsmanagement (Sicherheitsrichtlinien, Informationen über spezielle Sicherheitsmaßnahmen oder -systeme, organisatorische Regelungen …) gegeben werden.

3.3 Life Cycle der Informationssicherheitspolitik

3.3.1 Erstellung

Die Informationssicherheitspolitik soll von allen Mitarbeitern/innen getragen werden. Es ist daher wichtig, dass bei ihrer Erstellung alle wesentlichen Kräfte der Organisation beteiligt werden und das Dokument mit Vertretern/innen aller Beteiligten bzw. Betroffenen abgestimmt wird.

Zunächst ist eine verantwortliche Person für die Erstellung der Informationssicherheitspolitik zu nominieren. Im Allgemeinen wird dies, soweit bereits definiert, die/der IT-Sicherheitsbeauftragte sein.

Weiters sollen Vertreter/innen folgender Bereiche an der Erstellung der organisationsweiten Informationssicherheitspolitik mitarbeiten bzw. in den Abstimmungsprozess miteinbezogen werden:

- IT-Abteilung
- Anwender/innen
- Bereichs-IT-Sicherheitsbeauftragte
- Personalabteilung
- Gebäudeverwaltung und Infrastruktur
- Revision
- Budgetabteilung

Die wesentlichen Inhalte der Informationssicherheitspolitik müssen allen Betroffenen und Beteiligten, also allen Mitarbeitern/innen der Organisation, aber auch etwa externen Mitarbeitern/innen und Lieferanten, bekannt sein.

Dazu sollten in der Folge die für die einzelnen Personengruppen wichtigsten Richtlinien und Vorgaben der Informationssicherheitspolitik zusammengefasst und jeder/m Betroffenen in schriftlicher Form zur Kenntnis gebracht werden. Wo nötig, sind das Einverständnis mit diesen Vorgaben und die Kenntnis der daraus erwachsenden Verpflichtungen auch durch eine Unterschrift bestätigen zu lassen (etwa Verpflichtung auf das Datengeheimnis, Ergänzungen zu Dienstverträgen, Geheimhaltungsverpflichtungen von externen Personen, ...)

3.3.2 Offizielle Inkraftsetzung

Die Informationssicherheitspolitik wird von der Leitung der Organisation offiziell verabschiedet und in Kraft gesetzt.

Wesentliche Voraussetzung für eine erfolgreiche Implementierung und Umsetzung der Informationssicherheitspolitik ist, dass sie die volle und für jede/n Beteiligte/n sichtbare Unterstützung durch das Management erhält.

3.3.3 Regelmäßige Überarbeitung

Zwar stellt die Informationssicherheitspolitik ein langfristiges Dokument dar, dennoch ist auch sie regelmäßig auf ihre Aktualität und Übereinstimmung mit den tatsächlichen Anforderungen zu überprüfen und bei Bedarf entsprechend anzupassen.

Als Richtwert hierfür kann ein Zeitraum von zwei bis drei Jahren angesehen werden, nach dem die Informationssicherheitspolitik spätestens überprüft und aktualisiert werden sollte. Kommt es jedoch zwischenzeitlich zu gravierenden Änderungen im IT-System, in der Organisationsstruktur oder in den Bedrohungen, so ist eine sofortige Überarbeitung der Informationssicherheitspolitik in die Wege zu leiten.

Die Verantwortung dafür ist dezidiert festzulegen. Im Allgemeinen wird sie bei der für die IT-Sicherheit beauftragten Person liegen.

4 Risikoanalyse

Eine wesentliche Voraussetzung für erfolgreiches Informationssicherheitsmanagement ist die Einschätzung der bestehenden Sicherheitsrisiken. In einer Risikoanalyse wird versucht, diese Risiken zu erkennen und zu bewerten und so das Gesamtrisiko zu ermitteln. Ziel ist es, in weiterer Folge dieses Risiko so weit zu reduzieren, dass das verbleibende Restrisiko quantifizierbar und akzeptierbar wird.

Das nachfolgende Kapitel beschreibt die drei heute meist verbreiteten Strategien zur Risikoanalyse - detaillierte Risikoanalyse, Grundschutzansatz und kombinierter Ansatz - und stellt ihre Vor- und Nachteile und ihre typischen Einsatzbereiche gegenüber.

4.1 Risikoanalysestrategien

Es ist empfehlenswert, eine Strategie zur Risikoanalyse festzulegen. Diese sollte für die gesamte Organisation gültig sein und festlegen, wie die Ziele der Risikoanalyse - Erkennen und Bewerten von Einzelrisiken und Gesamtrisiko - erreicht werden sollen.

Mögliche Risikoanalysestrategien sind:

- Detaillierte Risikoanalyse: Für alle IT-Systeme wird eine detaillierte Risikoanalyse durchgeführt. Diese Methode führt zu effektiven und angemessenen Sicherheitsmaßnahmen, benötigt jedoch viel Zeit und Aufwand, so dass neben hohen Kosten auch die Gefahr besteht, dass für kritische Systeme nicht schnell genug Schutzmaßnahmen ergriffen werden können.
- Grundschutzansatz: Unabhängig vom tatsächlichen Schutzbedarf wird für alle IT-Systeme von einer pauschalisierten Gefährdungslage ausgegangen. Als Sicherheitsmaßnahmen kommen sog. Grundschutzmaßnahmen (Baseline Security Controls) zum Einsatz. Durch den Verzicht auf eine detaillierte Risikoanalyse spart diese Vorgehensweise Ressourcen und führt schnell zu einem relativ hohen Niveau an Sicherheit. Der Nachteil liegt darin, dass der Grundschutzlevel für das betrachtete IT-System möglicherweise nicht angemessen sein könnte.
- Kombinierter Ansatz: In einem ersten Schritt wird in einer Schutzbedarfsfeststellung (High Level Risk Analysis) der Schutzbedarf für die einzelnen IT-Systeme ermittelt. Für IT-Systeme der Schutzbedarfskategorie “niedrig bis mittel” wird auf eine detaillierte Risikoanalyse verzichtet. Dies erlaubt eine schnelle und effektive Auswahl von grundlegenden Sicherheitsmaßnahmen bei gleichzeitiger Gewährleistung eines angemessenen Schutzniveaus. IT-Systeme der Schutzbedarfskategorie “hoch bis sehr hoch” sind einer detaillierten Risikoanalyse zu unterziehen, auf deren Basis individuelle Sicherheitsmaßnahmen ausgewählt werden. Diese Option kombiniert die Vorteile des Grundschutz- und des Risikoanalyseansatzes, da alle IT-Systeme mit hohem Schutzbedarf wirksam und angemessen geschützt werden, und Maßnahmen für die anderen Systeme mit Hilfe des Grundschutzes schnell und effektiv ausgewählt werden können. Sie wird in den meisten Einsatzumgebungen die empfehlenswerte Strategie zur Risikoanalyse darstellen.

Im Folgenden werden die drei angeführten Risikoanalysestrategien näher erläutert.

4.2 Detaillierte Risikoanalyse

Eine detaillierte Risikoanalyse für ein IT-System umfasst die Identifikation der bestehenden Risiken sowie eine Abschätzung ihrer Größe.

Dazu werden die Werte (Assets), Bedrohungen und Schwachstellen identifiziert und die daraus resultierenden Risiken ermittelt.

Die erstmalige Durchführung einer detaillierten Risikoanalyse und die anschließende Erstellung eines Sicherheitskonzeptes erfordern einen Aufwand, der zumindest im Bereich von Wochen, möglicherweise auch von Monaten liegt.

Eine detaillierte Risikoanalyse umfasst folgende Schritte:

Schritt 1:

Hier sind die zu analysierenden IT-Systeme zu spezifizieren und anzugeben, ob und in welchem Maße auch andere Objekte (z.B. Gebäude und Infrastruktur) in die Analyse einbezogen werden sollen.

Schritt 2:

Ziel dieses Schrittes ist die Erfassung aller bedrohten Objekte, die innerhalb des im vorangegangenen Schritt festgesetzten Analysebereiches liegen.

Schritt 3:

In diesem Schritt wird der Wert der bedrohten Objekte ermittelt.

Die Wertanalyse umfasst im Einzelnen:

- die Festlegung der Bewertungsbasis für Sachwerte
- die Festlegung der Bewertungsbasis für immaterielle Werte
- die Ermittlung der Abhängigkeiten zwischen den Objekten
- die Bewertung der bedrohten Objekte und der möglichen Schäden (Impact Analyse)

Schritt 4:

Die Objekte sind vielfachen Bedrohungen ausgesetzt, die sowohl aus Nachlässigkeit und Versehen als auch aus Absicht resultieren können.

Die Bedrohungsanalyse umfasst:

- die Identifikation möglicher Bedrohungen (Katastrophen, Fehlbedienung, bewusste Angriffe) und möglicher Angreifer/innen (Mitarbeiter/innen, Leasingpersonal, Außenstehende, ...)
- die Ermittlung der Eintrittswahrscheinlichkeiten

Schritt 5:

Eine Bedrohung kann nur durch die Ausnutzung einer vorhandenen Schwachstelle wirksam werden. Es ist daher erforderlich, mögliche Schwachstellen des Systems zu identifizieren und ihre Bedeutung zu klassifizieren.

Zu untersuchen sind dabei insbesondere die Bereiche Organisation, Hard- und Software, Personal sowie Infrastruktur.

Schritt 6:

Zur Vermeidung unnötiger Aufwände und Kosten sind die bereits existierenden Sicherheitsmaßnahmen zu erfassen und auf ihre Auswirkungen hinsichtlich der Gesamtsystem-sicherheit sowie auf korrekte Funktion zu prüfen.

Geplante neue Sicherheitsmaßnahmen müssen mit den existierenden kompatibel sein und eine wirtschaftlich und technisch sinnvolle Ergänzung darstellen.

Schritt 7:

In diesem Schritt werden die Einzelrisiken und das Gesamtrisiko ermittelt und bewertet.

Schritt 8:

Eine Auswertung und Aufbereitung des Ergebnisses schließt die Risikoanalyse ab.

Bei der Durchführung einer Risikoanalyse sind folgende Prinzipien zu beachten:

- Das gesamte Verfahren muss transparent gemacht werden.
- Es dürfen keine versteckten Annahmen gemacht werden, die z.B. dazu führen, dass Bedrohungen unbetrachtet bleiben.
- Alle Bewertungen müssen begründet werden, um subjektive Einflüsse zu erkennen und so weit wie möglich zu vermeiden.
- Alle Schritte müssen so dokumentiert werden, dass sie später auch für andere nachvollziehbar sind. Ein derartiges Vorgehen erleichtert auch eine spätere Überarbeitung des Informationssicherheitskonzeptes.
- Der Aufwand für die Durchführung des Verfahrens sollte dem Wert der IT-Anwendungen und den Werten der Institution im Allgemeinen angemessen sein.

In den nachfolgenden Kapiteln werden die einzelnen Schritte einer Risikoanalyse detailliert behandelt. Das vorliegende Handbuch gibt Hinweise und Unterstützung zur Durchführung dieser Schritte. Die Wahl einer konkreten Risikoanalysemethode sowie ein etwaiger Einsatz von Tools zur Unterstützung dieser Analyse bleiben der durchführenden Institution überlassen. Wichtig ist, dass alle der im Folgenden angeführten Schritte durchgeführt werden und die geforderten Ergebnisse liefern.

4.2.1 Abgrenzung des Analysebereiches

Vor Beginn einer Risikoanalyse ist es erforderlich, den zu analysierenden Bereich genau abzugrenzen. Dabei ist anzugeben, ob sich die Analyse auf Hardware, Software und Daten des betrachteten IT-Systems beschränkt oder ob und in welchem Ausmaß andere Werte wie Gebäude und Infrastruktur, Personen, immaterielle Güter, Fähigkeiten und Leistungen einbezogen werden sollen.

4.2.2 Identifikation der bedrohten Objekte (Werte, assets)

In diesem Schritt sind alle bedrohten Objekte (assets), die innerhalb des festgestellten Analysebereiches liegen, zu erfassen.

Unter den bedrohten Objekten einer Organisation ist alles zu verstehen, was für diese schutzbedürftig ist, also alle Objekte, von denen der Betrieb des IT-Systems und seine Anwendungen und damit die Funktionsfähigkeit der Organisation abhängen. Dazu zählen etwa:

- physische Objekte: beispielsweise Gebäude, Infrastruktur, Hardware, Datenträger, Paperware
- logische Objekte: beispielsweise Software, Daten, Information
- Personen
- Fähigkeiten: etwa Herstellen eines Produktes oder Erbringen einer Dienstleistung
- immaterielle Güter: beispielsweise Image, Vertrauen in die Institution oder gute Beziehungen zu anderen Organisationen

Zwischen den bedrohten Objekten bestehen grundsätzlich komplexe Abhängigkeiten. Die Vertraulichkeit, Integrität oder Verfügbarkeit eines Objektes setzt vielfach die Vertraulichkeit, Integrität oder Verfügbarkeit eines anderen Objektes voraus. Beispiele dafür sind etwa die Erfordernis einer funktionsfähigen Infrastruktur (Stromversorgung, Klimaanlage, ...) für den Betrieb eines IT-Systems oder die Abhängigkeit der Software von unversehrter und verfügbarer Hardware.

Die Identifizierung der bedrohten Objekte sowie ihre nachfolgende Bewertung stellen wesentliche Voraussetzungen für ein erfolgreiches Informationssicherheitsmanagement dar. Dabei ist es den Erfordernissen im Einzelfall anzupassen, in welcher Tiefe und in welchem Detaillierungsgrad die einzelnen Objekte analysiert werden sollen; in vielen Fällen wird eine Zusammenfassung in Gruppen sinnvoll sein und beitragen, den Analyseaufwand zu begrenzen.

4.2.3 Wertanalyse (Impact Analyse)

In diesem Schritt wird der Wert der im vorangegangenen Schritt identifizierten Objekte ermittelt.

Die Wertanalyse umfasst im Einzelnen:

- die Festlegung der Bewertungsbasis für Sachwerte
- die Festlegung der Bewertungsbasis für immaterielle Werte
- die Ermittlung der Abhängigkeiten zwischen den Objekten
- die Bewertung der bedrohten Objekte und der möglichen Schäden

4.2.3.1 Festlegung der Bewertungsbasis für Sachwerte

Zunächst ist zu entscheiden, ob die Bewertung quantitativ oder qualitativ erfolgen soll.

Eine quantitative Bewertung kann etwa beruhen auf

- dem Zeitwert eines Objektes,
- dem Wiederbeschaffungswert eines Objektes,
- dem Wert, den das Objekt für eine/n potentiellen Angreifer/in hätte, oder
- dem Schaden, der sich aus dem Verlust oder der Modifikation eines zu schützenden Objektes für die betroffene Organisation ergibt.

Eine qualitative Bewertung erfolgt durch Einteilung in Klassen. Beispiele hierfür sind etwa:

- 3-stufige Bewertung: gering - mittel - hoch
- 5-stufige Bewertung: unbedeutend - gering - mittel - hoch - sehr hoch

Als Basis für eine qualitative Bewertung ist festzulegen, was die einzelnen Klassen bedeuten bzw. wie sie definiert sind.

4.2.3.2 Festlegung der Bewertungsbasis für immaterielle Werte

Auch für immaterielle Werte, wie etwa Bewahrung des guten Rufes oder Gewährleistung der Vertraulichkeit, kann eine quantitative oder eine qualitative Bewertungsbasis festgelegt werden.

Eine quantitative Bewertung kann in diesem Fall beruhen auf

- dem Wert, den das Objekt für eine/n potentiellen Angreifer/in hätte (z.B. vertrauliche Information), oder
- dem Schaden, der sich aus einem Angriff auf das zu schützende Objekt für die betroffene Organisation ergibt.

Es ist zu beachten, dass die potentiellen Schäden den eigentlichen (Zeit- oder Wiederbeschaffungs)Wert beträchtlich übersteigen können.

4.2.3.3 Ermittlung der Abhängigkeiten zwischen den Objekten

Es ist wichtig, auch die gegenseitige Abhängigkeit von Objekten festzustellen, da diese Einfluss auf die Bewertung der einzelnen zu schützenden Objekte haben kann.

So ist etwa die Funktionsfähigkeit der Hardware abhängig von der Funktionsfähigkeit der Stromversorgung und eventuell der Klimaanlage. Die Integrität von Information bedingt die Integrität und Verfügbarkeit der Hard- und Software, die zu ihrer Verarbeitung bzw. Speicherung eingesetzt wird.

4.2.3.4 Bewertung der bedrohten Objekte

Mit Ausnahme der Festsetzung von Zeit- oder Wiederbeschaffungswert wird die Bewertung von bedrohten Objekten in der Regel sehr subjektiv sein. Es ist daher notwendig, im Rahmen der Analyse möglichst genaue Bewertungsbasen und Regeln vorzugeben und diese eventuell durch Beispiele zu illustrieren sowie möglichst viele unterschiedliche Personen nach ihrer Einschätzung zu befragen.

Durchführung:

- Die Person, die die Risikoanalyse durchführt, erstellt eine Liste der zu bewertenden Objekte und gibt die Bewertungsbasen vor.
- Die Bewertung sollte durch die Applikations-/Projektverantwortlichen sowie die betroffenen Benutzer/innen vorgenommen werden.
- Unterstützung in der Bewertung kann von verschiedenen Abteilungen, etwa Finanzen, Einkauf, IT, ... kommen.
- Es ist Aufgabe derjenigen Person, der die Risikoanalyse durchführt, die einzelnen Bewertungen auf Plausibilität und Konsistenz zu prüfen und ein konsolidiertes Ergebnis zu erarbeiten.

Ergebnis der Wertanalyse:

Aufstellung der bedrohten Objekte und ihres Wertes für die Organisation.

4.2.4 Bedrohungsanalyse

Lt. ISO/IEC 13335 ist eine Bedrohung ein "möglicher Anlass für ein unerwünschtes Ereignis, das zu einem Schaden für das System oder die Organisation führen kann".

Die zu schützenden Objekte sind vielfältigen Bedrohungen ausgesetzt. Im Rahmen der Risikoanalyse müssen diese identifiziert werden, weiters ist ihre Schwere und Eintrittswahrscheinlichkeit abzuschätzen.

Bedrohungen sind charakterisiert durch:

- ihren Ursprung: Bedrohungen durch die Umwelt oder durch den Menschen, wobei letztere wieder in absichtliche oder zufällige Bedrohungen zu unterteilen sind. Im Falle absichtlicher Bedrohungen ist zwischen Innentätern und Außentätern zu unterscheiden.
- die Motivation: Motivation für (absichtliche) Bedrohungen können etwa finanzielle Gründe, Wettbewerbsvorteile, Rache, aber auch Geltungssucht oder erhoffte Publicity sein.
- die Häufigkeit des Auftretens,
- die Größe des Schadens, der durch diese Bedrohung verursacht werden kann.

Für einige umweltbedingte Bedrohungen (etwa Erdbeben, Blitzschlag, ...) liegen statistische Daten vor, die für die Einschätzung hilfreich sein können.

Die Bedrohungsanalyse umfasst im Einzelnen:

- die Identifikation möglicher Bedrohungen
- die Ermittlung der Eintrittswahrscheinlichkeiten

4.2.4.1 Identifikation möglicher Bedrohungen

Bedrohungen können unterteilt werden in:

- Höhere Gewalt
  (etwa Blitzschlag, Feuer, Erdbeben, Personalausfall)
- Organisatorische Mängel
  (etwa fehlende oder unzureichende Regelungen für Wartung, Dokumentation, Test und Freigabe, fehlende Auswertung von Protokolldaten, mangelhafte Kennzeichnung von Datenträgern)
- Menschliche Fehlhandlungen
  (etwa fehlerhafte Systemnutzung oder -administration, fahrlässige Zerstörung von Geräten oder Daten, Nichtbeachtung von Sicherheitsmaßnahmen)
- Technisches Versagen
  (etwa Ausfall von Versorgungs- und Sicherheitseinrichtungen, Softwarefehler, defekte Datenträger)
- Vorsätzliche Handlungen
  (etwa Manipulation/Zerstörung von Geräten, Manipulation an Daten oder Software, Viren, trojanische Pferde, Abhören, Wiedereinspielen von Nachrichten, Nichtanerkennen einer Nachricht, Maskerade)

Es ist wichtig, alle wesentlichen Bedrohungen zu erfassen, da andernfalls Sicherheitslücken bestehen bleiben können.

Bei der Identifikation von möglichen Bedrohungen können Bedrohungskataloge hilfreich sein, die den Charakter von Checklisten haben. Solche Kataloge finden sich etwa in BSI 7105, S 207 ff und in ISO/IEC 27005. In den IT-Grundschutzkatalogen des BSI gibt es eine umfangreiche Sammlung von so genannten “Gefährdungen”, die ihrerseits eine Kombination aus Bedrohungen und Schwachstellen darstellen. Es ist jedoch zu betonen, dass keine derartige Liste vollständig sein kann, und darüber hinaus auch Bedrohungen einem ständigen Wandel und einer ständigen Weiterentwicklung unterworfen sind. Es ist daher immer erforderlich, über Bedrohungskataloge hinaus auch die Möglichkeit weiterer Bedrohungen in Betracht zu ziehen.

4.2.4.2 Ermittlung der Eintrittswahrscheinlichkeiten

In diesem Schritt der Risikoanalyse ist zu bestimmen, mit welcher Wahrscheinlichkeit eine Bedrohung im betrachteten Umfeld eintreten wird.

Diese ist abhängig von:

- der Häufigkeit der Bedrohung (Wahrscheinlichkeit des Auftretens anhand von Erfahrungen, Statistiken, ...),
- der Motivation und den vorausgesetzten Fähigkeiten und Ressourcen einer/eines potentiellen Angreiferin/Angreifers,
- Einschätzung der Attraktivität und Verwundbarkeit des IT-Systems bzw. seiner Komponenten,
- Umweltfaktoren und organisationsspezifischen Einflüssen.

Auch die Eintrittswahrscheinlichkeit kann quantitativ oder qualitativ bewertet werden.

Da eine quantitative Bewertung in vielen Fällen eine Genauigkeit vortäuschen könnte, die durch die ungenaue Methode der Schätzung nicht zu rechtfertigen ist, ist in den letzten Jahren ein Trend in Richtung qualitativer Bewertung zu erkennen.

Bewährt haben sich hier etwa drei- bis fünfteilige Skalen, wie beispielsweise:

4: sehr häufig
3: häufig
2: mittel
1: selten
0: sehr selten

Diese allgemeinen Bedeutungen der Skalenwerte sind für den spezifischen Anwendungsbereich zu konkretisieren.

Beispiel:

4: einmal pro Minute
3: einmal pro Stunde
2: einmal pro Tag
1: einmal pro Monat
0: einmal im Jahr

Ergebnis der Bedrohungsanalyse:

Liste von Bedrohungen, der von ihnen bedrohten Objekte und ihrer Eintrittswahrscheinlichkeiten.

4.2.5 Schwachstellenanalyse

Unter einer Schwachstelle (vulnerability) versteht man eine Sicherheitsschwäche eines oder mehrerer Objekte, die durch eine Bedrohung ausgenützt werden kann.

Typische Beispiele für Schwachstellen sind etwa:

- Mangelnder baulicher Schutz von Räumen mit IT-Einrichtungen
- Nachlässige Handhabung von Zutrittskontrollen
- Spannungs- oder Temperaturschwankungen bei Hardwarekomponenten
- kompromittierende Abstrahlung
- Spezifikations- und Implementierungsfehler
- schwache Passwortmechanismen
- unzureichende Ausbildung, mangelndes Sicherheitsbewusstsein

Eine Schwachstelle selbst verursacht noch keinen Schaden, sie ist aber die Voraussetzung, die es einer Bedrohung ermöglicht, wirksam zu werden und damit ein IT-System zu beeinträchtigen. Auf Schwachstellen, für die eine korrespondierende Bedrohung existiert, sollte daher sofort reagiert werden.

Eine Schwachstellenanalyse ist die Überprüfung von Sicherheitsschwächen, die durch festgestellte Bedrohungen ausgenutzt werden können. Diese Analyse muss sowohl das Umfeld als auch bereits vorhandene Schutzmaßnahmen mit einbeziehen. Es ist wichtig, jede Schwachstelle daraufhin zu bewerten, wie leicht es ist, sie auszunutzen.

Beispielhafte Auflistungen von Schwachstellen, die auf typische Problembereiche hinweisen, finden sich etwa in ISO/IEC 27005, Annex D sowie in BSI 7105, S 199 ff.

Ergebnis der Schwachstellenanalyse:

Liste von potentiellen Schwachstellen mit Angaben darüber, wie leicht diese für einen Angriff ausgenützt werden können.

4.2.6 Identifikation bestehender Sicherheitsmaßnahmen

Sicherheitsmaßnahmen sind Verfahrensweisen, Prozeduren und Mechanismen, die eine oder mehrere der nachfolgenden Funktionen erfüllen:

- Vermeidung von Risiken,
- Verkleinerung von Bedrohungen oder Schwachstellen,
- Entdeckung unerwünschter Ereignisse,
- Eingrenzung der Auswirkungen eines unerwünschten Ereignisses,
- Überwälzung von Risiken oder
- Wiederherstellung eines früheren Zustandes.

Wirksame IT-Sicherheit verlangt im Allgemeinen eine Kombination von verschiedenen Typen von Maßnahmen.

Da die Sicherheitsmaßnahmen, die aufgrund einer Risikoanalyse ausgewählt werden, in der Regel zusätzlich zu bereits bestehenden Maßnahmen eingeführt werden sollen, ist es notwendig, alle bereits existierenden oder geplanten Sicherheitsmaßnahmen zu identifizieren und ihre Auswirkungen zu überprüfen, um unnötigen Aufwand zu vermeiden.

Stellt sich heraus, dass eine bereits existierende oder geplante Maßnahme ihren Anforderungen nicht gerecht wird, so ist zu prüfen, ob sie ersatzlos entfernt, durch andere Maßnahmen ersetzt oder aus Kostengründen belassen werden soll.

Im Rahmen dieses Schrittes sollte auch geprüft werden, ob die bereits existierenden Sicherheitsmaßnahmen korrekt zum Einsatz kommen. Falsch oder unvollständig eingesetzte Sicherheitsmaßnahmen stellen eine zusätzliche potentielle Schwachstelle eines Systems dar.

Ergebnis:

Aufstellung aller bereits existierenden oder geplanten Sicherheitsmaßnahmen mit Angaben über ihren Implementierungsstatus und ihren Einsatz.

4.2.7 Risikobewertung

Ein Risiko ist die Möglichkeit, dass eine Bedrohung unter Ausnutzung einer Schwachstelle Schaden an einem Objekt oder den Verlust eines Objektes und damit direkt oder indirekt einen Schaden verursacht.

Ziel dieses Schrittes ist es, die Risiken, denen ein IT-System und seine Objekte ausgesetzt sind, zu erkennen und zu bewerten, um auf dieser Basis geeignete und angemessene Sicherheitsmaßnahmen auswählen zu können.

Risiken sind eine Funktion folgender Parameter:

- Wert der bedrohten Objekte (Schadensausmaß),
- Möglichkeit, eine Schwachstelle durch eine Bedrohung auszunutzen,
- Eintrittswahrscheinlichkeit einer Bedrohung,
- bereits existierende oder geplante Sicherheitsmaßnahmen, die dieses Risiko reduzieren könnten.

Wie diese Größen miteinander verknüpft werden, um die Höhe der Einzelrisiken und des Gesamtrisikos zu bestimmen, ist abhängig von der gewählten Risikoanalysemethode. Wieder können quantitative oder qualitative Bewertungen vorgenommen oder aber beide Möglichkeiten kombiniert werden.

ISO/IEC 27005 gibt im Anhang vier Beispiele für Methoden zur Risikobewertung.

Es ist zu beachten, dass jegliche Änderung an Werten, Bedrohungen, Schwachstellen oder Sicherheitsmaßnahmen bedeutenden Einfluss auf die Einzelrisiken und auf das Gesamtrisiko haben kann.

Ergebnis:

Quantitative oder qualitative Bewertung von Einzelrisiken und Gesamtrisiko für den betrachteten Analysebereich.

4.2.8 Auswertung und Aufbereitung der Ergebnisse

Der adäquaten Aufbereitung, Auswertung und Interpretation der Ergebnisse einer Risikoanalyse kommt wachsende Bedeutung zu. Da die Risikoanalyse auch als Grundlage für weitreichende weiterführende Entscheidungen dient, ist auf eine klare Darstellung der Situation sowie eine umfassende Ergebnisdarstellung zu achten. Hilfreich dabei sind graphische und tabellarische Darstellungen.

4.3 Grundschutzansatz

Die im Rahmen dieses Handbuches empfohlene Vorgehensweise zur Grundschutzanalyse folgt im Wesentlichen den Vorgaben zum IT-Grundschutz des BSI. In diesem Kapitel wird eine kurze Zusammenfassung des Verfahrens, angepasst an die Erfordernisse der öffentlichen Verwaltung in Österreich, gegeben. Details zum Verfahren finden sich im BSI-Standard 100-2, Kataloge zu Gefährdungen und Sicherheitsmaßnahmen in [BSI-1] bzw. [BSI-2].

4.3.1 Die Idee des IT-Grundschutzes

Ziel des Grundschutzansatzes ist es, den Aufwand für die Erstellung eines Informationssicherheitskonzeptes angemessen zu begrenzen.

Dies wird dadurch erreicht, dass von einer pauschalisierten Gefährdungslage ausgegangen und damit auf eine detaillierte Risikoanalyse verzichtet wird. Die Auswahl der zu realisierenden Sicherheitsmaßnahmen erfolgt auf der Basis vorgegebener Kataloge.

Die Vorteile dieser Vorgehensweise sind:

- Der Aufwand für die Risikoanalyse wird stark reduziert.
- Der Einsatz von Grundschutzmaßnahmen führt schnell zu einem relativ hohen Niveau an Sicherheit gegen die häufigsten Bedrohungen.

Zudem sind Grundschutzmaßnahmen meist stark verbreitet und damit relativ kostengünstig und schnell zu implementieren.

Dem stehen folgende Nachteile gegenüber:

- Der Grundschutzlevel kann für das betrachtete System zu hoch oder zu niedrig sein. Ist er zu hoch, werden unnötige finanzielle und personelle Ressourcen verbraucht, ist er zu niedrig, bleiben unter Umständen untragbare Risiken bestehen.
- Aufgrund der fehlenden Risikoanalyse kann unter Umständen eine angemessene Reaktion auf sicherheitsrelevante Hard- oder Softwareänderungen schwierig sein.

Die Wahl eines Grundschutzansatzes wird daher in folgenden Fällen empfohlen:

- Wenn feststeht, dass im betrachteten Bereich nur IT-Systeme mit niedrigem oder mittlerem („normalem“) Schutzbedarf zum Einsatz kommen.
- Falls in einem Bereich (IT-System, Abteilung, ...) noch keine oder offensichtlich zu schwache Sicherheitsmaßnahmen vorhanden sind, kann die Realisierung von Grundschutzmaßnahmen dazu beitragen, rasch ein relativ gutes Niveau an IT-Sicherheit zu erreichen. In diesem Fall sollte aber in einem nachfolgenden Schritt geprüft werden, ob das erreichte Niveau bereits ausreichend ist oder weitere Analysen und Maßnahmen erforderlich sind.
- Als Teil eines umfassenden Risikoanalysekonzeptes (”kombinierter Ansatz”): Wird zunächst in einem ersten Schritt festgestellt, welche IT-Systeme besonders schutzbedürftig sind (”Schutzbedarfsfeststellung”), so besteht die Möglichkeit, den Arbeitsaufwand für die Risikoanalyse und die Auswahl spezifischer Sicherheitsmaßnahmen auf diese hochschutzbedürftigen Systeme zu konzentrieren. Für alle anderen Systeme können Grundschutzmaßnahmen eingesetzt werden, ohne damit unangemessene Sicherheitsrisiken einzugehen. Details dazu s. Kapitel Kombinierter Ansatz.

4.3.2 Grundschutzanalyse und Auswahl von Maßnahmen

Im Folgenden wird ein reiner Grundschutzansatz beschrieben, d.h. es wird davon ausgegangen, dass entweder bereits eine Schutzbedarfsfeststellung erfolgt ist und damit die IT-Systeme identifiziert sind, für die der IT-Grundschutz zu konzipieren ist, oder dass bewusst (zunächst) ein reiner Grundschutzansatz gewählt wird. Ein kombinierter Ansatz und die Stellung des IT-Grundschutzes in einem solchen werden im nachfolgenden Kapitel beschrieben.

Eine Grundschutzanalyse besteht im Wesentlichen aus den folgenden beiden Teilschritten:

Schritt 1: Nachbildung eines IT-Systems oder eines IT-Verbundes (Kombination mehrerer IT-Systeme) durch vorhandene Bausteine (”Modellierung”)

Schritt 2: Soll-Ist-Vergleich zwischen vorhandenen und empfohlenen Maßnahmen

4.3.2.1 Modellierung

Die Modellierung eines IT-Systems oder eines IT-Verbundes ist abhängig vom zugrunde liegenden Baustein- und Maßnahmenkatalog, da versucht werden muss, das System durch die vorhandenen Bausteine möglichst genau nachzubilden.

Eine der umfassendsten und ausgereiftesten Sammlungen von Bausteinen und Maßnahmen stellt das IT-Grundschutzhandbuch des BSI dar (BSI GSHB). Anhand dieses Werkes soll nachfolgend die Modellierung eines IT-Verbundes beschrieben werden.

Zentrale Aufgabe des Schrittes “Modellierung” ist es, den betrachteten IT-Verbund mit Hilfe der vorhandenen Bausteine des IT-Grundschutzes nachzubilden. Als Ergebnis wird ein Modell des IT-Verbundes erstellt, das aus verschiedenen, ggf. auch mehrfach verwendeten Bausteinen des Handbuchs besteht und eine Abbildung zwischen den Bausteinen und den sicherheitsrelevanten Aspekten des IT-Verbundes beinhaltet.

Um die Abbildung eines im Allgemeinen komplexen IT-Verbunds auf die Bausteine des Handbuchs zu erleichtern, bietet es sich an, die Sicherheitsaspekte gruppiert nach bestimmten Themen zu betrachten.

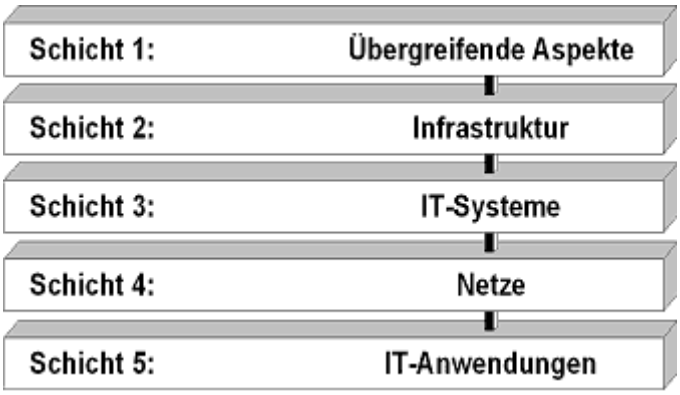

Abbildung 2: Schichten des IT-Grundschutzmodells nach [BSI GSHB]

Die Sicherheitsaspekte eines IT-Verbunds werden wie folgt den einzelnen Schichten zugeordnet:

- Schicht 1 umfasst sämtliche übergreifenden Sicherheitsaspekte, die für sämtliche oder große Teile des IT-Verbunds gleichermaßen gelten. Dies betrifft insbesondere übergreifende Konzepte und die daraus abgeleiteten Regelungen. Typische Bausteine der Schicht 1 sind unter anderem Informationssicherheitsmanagement, Organisation, Datensicherungskonzept und Computer-Virenschutzkonzept.
- Schicht 2 befasst sich mit den baulich-technischen Gegebenheiten, in der Aspekte der infrastrukturellen Sicherheit zusammengeführt werden. Dies betrifft insbesondere die Bausteine Gebäude, Räume, Schutzschränke und häuslicher Arbeitsplatz.
- Schicht 3 betrifft die einzelnen IT-Systeme des IT-Verbunds, die ggf. in Gruppen zusammengefasst wurden. Hier werden die Sicherheitsaspekte sowohl von Clients als auch von Servern, aber auch von Stand-alone-Systemen behandelt. In die Schicht 3 fallen damit beispielsweise die Bausteine Unix-System, Tragbarer PC, Windows NT Netz und TK-Anlage.
- Schicht 4 betrachtet die Kommunikations- und Vernetzungsaspekte der IT-Systeme, wie etwa die Bausteine Netz- und Systemmanagement und Firewalls.
- Schicht 5 schließlich beschäftigt sich mit den eigentlichen IT-Anwendungen, die im IT-Verbund genutzt werden. In dieser Schicht können unter anderem die Bausteine E-Mail, WWW-Server, Faxserver und Datenbanken zur Modellierung verwendet werden.

Die in diesem Schritt zu leistende Aufgabe besteht darin, das reale IT-System durch die vorhandenen Bausteine möglichst genau nachzubilden.

Abschließend sollte überprüft werden, ob die Modellierung des Gesamtsystems vollständig ist und keine Lücken aufweist. Es wird empfohlen, hierzu den Netzplan oder eine vergleichbare Übersicht über den IT-Verbund heranzuziehen und die einzelnen Komponenten systematisch durchzugehen. Jede Komponente sollte entweder einer Gruppe zugeordnet oder einzeln modelliert worden sein.

Wichtig ist, dass nicht nur alle Hard- und Software-Komponenten in technischer Hinsicht nachgebildet sind, sondern dass auch die zugehörigen organisatorischen, personellen und infrastrukturellen Aspekte vollständig abgedeckt sind.

4.3.2.2 Soll-Ist-Vergleich zwischen vorhandenen und empfohlenen Maßnahmen

Im zweiten Schritt der Grundschutzanalyse wird die Modellierung nach IT-Grundschutz als Prüfplan verwendet, um festzustellen, welche Standardsicherheitsmaßnahmen bereits umgesetzt wurden, bzw. welche nicht oder unzureichend umgesetzt wurden.

Das SOLL besteht aus den in den einzelnen Bausteinen empfohlenen Maßnahmen. Der Vergleich mit den vorhandenen Maßnahmen ergibt als Resultat die Maßnahmen, die es noch für den IT-Grundschutz umzusetzen gilt.

Der eigentliche Soll-Ist-Vergleich soll mittels Interviews und stichprobenartiger Kontrollen durchgeführt werden.

Vorgehen bei Abweichungen

Für die Errichtung eines IT-Grundschutzes sollten zwar prinzipiell alle im Baustein vorgeschlagenen IT-Grundschutzmaßnahmen umgesetzt werden, es besteht jedoch die Möglichkeit, dass bei bestimmten Einsatzumgebungen empfohlene Grundschutzmaßnahmen nicht umgesetzt werden können oder sollten. Diese Abweichung von der Empfehlung ist dann zu dokumentieren und zu begründen.

An dieser Stelle sollten auch eventuell vorhandene über den IT-Grundschutz hinausgehende IT-Sicherheitsmaßnahmen herausgearbeitet und dokumentiert werden.

Dokumentation der Ergebnisse

Zu jeder Maßnahme sollten

- der Umsetzungsgrad (ja/teilweise/nein/entbehrlich) sowie, soweit zu diesem Zeitpunkt bereits möglich,
- die Verantwortlichkeiten für die Umsetzung
- der Zeitpunkt für die Umsetzung und
- eine Kostenschätzung

angegeben werden.

Für die Durchführung einer Grundschutzanalyse in einer komplexen Einsatzumgebung empfiehlt sich der Einsatz eines Tools. Bekanntestes Beispiel ist das im Auftrag des BSI entwickelte “IT-Grundschutz-Tool”. Hierdurch ergeben sich komfortable Möglichkeiten zur Auswertung und Revision der Ergebnisse, beispielsweise die Suche nach bestimmten Einträgen, der Generierung benutzerdefinierter Reports sowie Statistikfunktionen.

Ergebnis

Die beschriebene Vorgehensweise liefert als Ergebnis eine Liste von Maßnahmen, die es für die Erreichung des IT-Grundschutzes noch umzusetzen gilt.

4.4 Kombinierter Ansatz

Die Stärken beider oben diskutierter Risikoanalysestrategien - Zeit sparende Auswahl kostengünstiger IT-Sicherheitsmaßnahmen durch Grundschutzanalysen und wirksame Reduktion hoher Sicherheitsrisiken durch detaillierte Risikoanalysen - kommen in einem sog. kombinierten Ansatz zum Tragen.

Dabei wird zunächst ermittelt, welche IT-Systeme hohe oder sehr hohe Sicherheitsanforderungen haben, und welche niedrige bis mittlere haben (Schutzbedarfsfeststellung). Das Ergebnis dieses Schrittes ist eine Einteilung in zwei Schutzbedarfskategorien: “niedrig bis mittel” und “hoch bis sehr hoch”.

IT-Systeme der Schutzbedarfskategorie “niedrig bis mittel” werden einer Grundschutzanalyse unterzogen, während IT-Systeme der Schutzbedarfskategorie “hoch bis sehr hoch” einer detaillierten Risikoanalyse zu unterziehen sind, auf deren Basis individuelle Sicherheitsmaßnahmen ausgewählt werden.

Alternativ dazu können auch etwa drei Schutzbedarfskategorien gewählt werden (s. Kap. 4.4.1, zweites Beispiel). Dabei werden IT-Systeme der Schutzbedarfskategorie “normal” einer Grundschutzanalyse unterzogen. IT-Systeme der Schutzbedarfskategorie “hoch” sind einer eingehenderen Betrachtung zu unterziehen. Wahlweise sind auch hier Grundschutzmaßnahmen (ev. in verstärktem Maße) anzuwenden, oder es ist eine detaillierte Risikoanalyse durchzuführen. IT-Systeme der Schutzbedarfskategorie “sehr hoch” sind jedenfalls einer detaillierten Risikoanalyse zu unterziehen, auf deren Basis individuelle Sicherheitsmaßnahmen ausgewählt werden.

Generell empfiehlt es sich, zunächst eine Grundschutzanalyse für alle Systeme durchzuführen, anschließend eine eventuell erforderliche detaillierte Risikoanalyse für Systeme höherer Schutzbedarfskategorien.

Vorteile eines kombinierten Ansatzes

- Die Vorgehensweise ermöglicht es, rasch einen relativ guten Sicherheitslevel für alle IT-Systeme zu realisieren.
- Die in der Schutzbedarfsfeststellung erarbeiteten Erkenntnisse können die Grundlage für eine Prioritätenreihung für die nachfolgenden Aktivitäten bilden.
- Der Aufwand kann auf hochsicherheitsbedürftige Systeme konzentriert werden.
- Das Verfahren findet im Allgemeinen hohe Akzeptanz, da es mit verhältnismäßig geringem Initialaufwand rasch sichtbare Erfolge bringt.

Empfehlung:

Aus diesen Gründen wird empfohlen, als Risikoanalysestrategie einen kombinierten Ansatz zu wählen.

4.4.1 Festlegung von Schutzbedarfskategorien

Voraussetzung für eine Schutzbedarfsfeststellung ist die Festlegung von Schutzbedarfskategorien.

Die nachfolgende Tabelle gibt eine Orientierungshilfe für die Festlegung der Schutzbedarfskategorien und damit die Klassifizierung der Anwendungen anhand der maximal möglichen Schäden anhand von Grenzwerten. Diese sind jedoch nur als Beispiele zu sehen. Jede Organisation sollte für sich prüfen, ob diese Klassifizierung ihren Anforderungen entspricht und gegebenenfalls eigene Grenzwerte und Einordnungen festlegen.

Weiters ist darauf hinzuweisen, dass die in der Tabelle angeführten sieben Schadenskategorien nicht vollständig sein müssen. Für alle Schäden, die sich nicht in diesen Kategorien abbilden lassen, ist ebenfalls eine Aussage zu treffen, wo die Grenze zwischen “niedrig bis mittel” und “hoch bis sehr hoch” zu ziehen ist.

	Schutzbedarfskategorie "niedrig bis mittel"	**Schutzbedarfskategorie "hoch bis sehr hoch"**
1. Verstoß gegen Gesetze, Vorschriften oder Verträge	▫ Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen ▫ Geringfügige Vertragsverletzungen mit geringen Konventionalstrafen ▫ Ein möglicher Missbrauch personenbezogener Daten hat nur geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse der/s Betroffenen.	▫ Schwere Verstöße gegen Gesetze u. Vorschriften (Strafverfolgung) ▫ Vertragsverletzungen mit hohen Konventionalstrafen oder Haftungsschäden ▫ Ein möglicher Missbrauch personenbezogener Daten hat erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse der/s Betroffenen (Verlust der Vertraulichkeit oder Integrität sensibler Daten)
2. Beeinträchtigung der persönlichen Unversehrtheit	▫ Eine Beeinträchtigung erscheint nicht möglich.	▫ Eine über Bagatellverletzungen hinausgehende Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.
3. Beeinträchtigung der Aufgabenerfüllung	▫ Es kann zu einer leichten bis maximal mittelschweren Beeinträchtigung der Aufgabenerfüllung kommen. ▫ Eine Zielerreichung ist mit vertretbarem Mehraufwand möglich.	▫ Es kann zu einer schweren Beeinträchtigung der Aufgabenerfüllung bis hin zur Handlungsunfähigkeit der betroffenen Organisation kommen. ▫ Bedeutende Zielabweichung in Qualität und/oder Quantität.
4. Vertraulichkeit der verarbeiteten Information	▫ Es werden nur Daten der Sicherheitsklassen OFFEN und EINGESCHRÄNKT verarbeitet bzw. gespeichert.	▫ Es werden auch Daten der Sicherheitsklassen VERTRAULICH, GEHEIM und/oder STRENG GEHEIM verarbeitet bzw. gespeichert.
5. Dauer der Verzichtbarkeit	▫ Die maximal tolerierbare Ausfallszeit der Anwendung beträgt mehrere Stunden bis mehrere Tage.	▫ Die maximal tolerierbare Ausfallszeit des Systems beträgt lediglich einige Minuten.
6. Negative Außenwirkung	▫ Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.	▫ Eine breite Beeinträchtigung des Vertrauens in die Organisation oder ihr Ansehen ist zu erwarten.
7. Finanzielle Auswirkungen	▫ Der finanzielle Schaden ist kleiner als (z.B.) Euro 50.000.--.	▫ Der zu erwartende finanzielle Schaden ist größer als (z.B.) Euro 50.000.--.

Tabelle 1: Beispiel für die Festlegung der Schutzbedarfskategorien

Eine andere Möglichkeit besteht darin, drei Schutzbedarfskategorien zu definieren:

Schutzbedarfskategorie “normal”: Die Schadensauswirkungen sind begrenzt und überschaubar. Maßnahmen des IT-Grundschutzes reichen im Allgemeinen aus. Diese Kategorie entspricht der obigen Kategorie “niedrig bis mittel”.

Schutzbedarfskategorie “hoch”: Die Schadensauswirkungen können beträchtlich sein. Wahlweise können weiter (verstärkte) Grundschutzmaßnahmen eingesetzt oder eine detaillierte Risikoanalyse durchgeführt werden.

Schutzbedarfskategorie “sehr hoch”: Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen. IT-Grundschutzmaßnahmen alleine reichen nicht aus, die erforderlichen Sicherheitsmaßnahmen sollten individuell auf Basis einer Risikoanalyse ermittelt werden.

Die nachfolgende Tabelle gibt eine Orientierungshilfe für die Festlegung der Schutzbedarfskategorien und damit die Klassifizierung der Anwendungen anhand der oben angeführten Einteilungen. Diese sind wiederum als Beispiele zu sehen. Jede Organisation sollte für sich prüfen, ob diese Klassifizierung ihren Anforderungen entspricht und gegebenenfalls eigene Grenzwerte und Einordnungen festlegen.

	Schutzbedarfs-kategorie “normal“	**Schutzbedarfs-kategorie “hoch“**	**Schutzbedarfs-kategorie “sehr hoch”**
1. Verstoß gegen Gesetze, Vorschriften oder Verträge	▫ Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen ▫ Geringfügige Vertragsverletzungen mit keinen oder geringen Konventionalstrafen ▫ Ein möglicher Missbrauch personenbezogener Daten hat nur geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse der/s Betroffenen.	▫ Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen ▫ Vertragsverletzungen mit hohen Konventionalstrafen ▫ Ein möglicher Missbrauch personenbezogener Daten hat erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse der/s Betroffenen.	▫ Schwere Verstöße gegen Gesetze und Vorschriften (Strafverfolgung) ▫ Vertragsverletzungen, deren Haftungsschäden ruinös sind ▫ Ein möglicher Missbrauch personenbezogener Daten würde für die/den Betroffene/n den gesellschaftlichen oder wirtschaftlichen Ruin bedeuten.
2. Beeinträchtigung der persönlichen Unversehrtheit	▫ Eine Beeinträchtigung erscheint nicht möglich.	▫ Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.	▫ Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. ▫ Gefahr für Leib und Leben

3. Beeinträchtigung der Aufgabenerfüllung	▫ Es kann zu einer leichten bis maximal mittelschweren Beeinträchtigung der Aufgabenerfüllung kommen. ▫ Eine Zielerreichung ist mit vertretbarem Mehraufwand möglich.	▫ Es kann zu einer schweren Beeinträchtigung der Aufgabenerfüllung kommen. ▫ Bedeutende Zielabweichung in Qualität und/oder Quantität.	▫ Es kann zu einer sehr schweren Beeinträchtigung der Aufgabenerfüllung bis hin zur Handlungsunfähigkeit der betroffenen Organisation kommen.
4. Vertraulichkeit der verarbeiteten Information	▫ Es werden nur Daten der Sicherheitsklassen OFFEN und EINGESCHRÄNKT verarbeitet bzw. gespeichert.	▫ Es werden auch Daten der Klasse VERTRAULICH verarbeitet bzw. gespeichert.	▫ Es werden auch Daten der Klassen GEHEIM und/oder STRENG GEHEIM verarbeitet bzw. gespeichert.
5. Dauer der Verzichtbarkeit	▫ Die maximal tolerierbare Ausfallszeit der Anwendung beträgt mehr als 24 Stunden.	▫ Die maximal tolerierbare Ausfallszeit des Systems liegt zwischen einer und 24 Stunden.	▫ Die maximal tolerierbare Ausfallszeit des Systems ist kleiner als eine Stunde.
6. Negative Außenwirkung	▫ Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.	▫ Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.	▫ Eine landesweite breite Ansehens- oder Vertrauensbeeinträchtigung, evtl. sogar existenzgefährdender Art, ist zu erwarten.
7. Finanzielle Auswirkungen	▫ Der finanzielle Schaden liegt unter (z.B.) Euro 50.000.--.	▫ Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.	▫ Der finanzielle Schaden ist für die Institution existenzbedrohend.

Tabelle 2: Beispiel für alternative Festlegung der Schutzbedarfskategorien

4.4.2 Schutzbedarfsfeststellung

Die Schutzbedarfsfeststellung bildet die Grundlage für eine Entscheidung über die weitere Vorgehensweise und ist daher mit entsprechender Sorgfalt durchzuführen.

Die Schutzbedarfsfeststellung erfolgt in 3 Schritten:

Schritt 1: Erfassung aller vorhandenen oder geplanten IT-Systeme
Schritt 2: Erfassung der IT-Anwendungen und Zuordnung zu den einzelnen IT-Systemen
Schritt 3: Schutzbedarfsfeststellung für jedes IT-System

4.4.2.1 Erfassung aller vorhandenen oder geplanten IT-Systeme

Zunächst werden die vorhandenen und geplanten IT-Systeme aufgelistet. Hierbei steht die technische Realisierung eines IT-Systems im Vordergrund, z.B. Stand-Alone-PC, Server, PC-Client, Windows-Server. An dieser Stelle soll nur das System als solches erfasst werden (z.B. Windows-Server), nicht die einzelnen Bestandteile, wie Rechner, Tastatur, Bildschirm, Drucker etc., aus denen das IT-System zusammengesetzt ist.

Zur Reduktion der Komplexität kann man gleiche IT-Systeme zu Gruppen zusammenfassen, wenn von Anwendungsstruktur und -ablauf vergleichbare Anwendungen auf diesen Systemen laufen. Dies gilt insbesondere für PCs, die oft in großer Anzahl vorhanden sind.

4.4.2.2 Erfassung der IT-Anwendungen und Zuordnung zu den einzelnen IT-Systemen

Ziel dieses Schrittes ist es, alle oder zumindest die wichtigsten auf dem betrachteten IT-System laufenden oder geplanten IT-Anwendungen zu erfassen.

Diese sollten anschließend - soweit zu diesem Zeitpunkt bereits möglich - nach ihrem Sicherheitsbedarf vorsortiert werden. Dabei sind zuerst diejenigen Anwendungen des jeweiligen IT-Systems zu benennen,

- deren Daten/Informationen und Programme den höchsten Bedarf an Vertraulichkeit haben,
- deren Daten/Informationen und Programme den höchsten Bedarf an Integrität aufweisen,
- die die kürzeste tolerierbare Ausfallszeit haben.

4.4.2.3 Schutzbedarfsfeststellung für jedes IT-System

In dieser Phase soll die Frage beantwortet werden, welche Schäden zu erwarten sind, wenn Vertraulichkeit, Integrität oder Verfügbarkeit einer IT-Anwendung und/oder der zugehörigen Informationen ganz oder teilweise verloren gehen. Die zu erwartenden Schäden bestimmen den Schutzbedarf. Dabei ist es unbedingt auch erforderlich, die Applikations-/Projektverantwortliche/n und die Benutzer/innen der betrachteten IT-Anwendungen nach ihrer Einschätzung zu befragen.

Als Orientierungshilfe für die Einordnung von IT-Anwendungen in Schutzbedarfskategorien kann die in Abschnitt 4.4.1 angeführte Tabelle dienen. Es ist aber empfehlenswert, eine den spezifischen Anforderungen der betroffenen Organisation entsprechende modifizierte Tabelle zu erstellen.

Die Ermittlung des Schutzbedarfes erfolgt nach dem Maximum-Prinzip. Ist für alle auf einem System laufenden Anwendungen ein normaler Schutzbedarf erhoben worden, so ist das gesamte System in die Schutzbedarfskategorie “normal” einzuordnen. Die Realisierung von Grundschutzmaßnahmen bietet hier in der Regel einen ausreichenden Schutz. Wurde dagegen mindestens eine Applikation mit hohem oder sehr hohem Schutzbedarf ermittelt, so ist das gesamte IT-System in die Schutzbedarfskategorie “hoch” bzw. “sehr hoch” einzuordnen.

4.4.3 Durchführung von Grundschutzanalysen und detaillierten Risikoanalysen

Für alle IT-Systeme der Schutzbedarfskategorie “niedrig bis mittel” bzw. “normal” ist eine Grundschutzanalyse gemäß der in Kapitel Grundschutzansatz beschriebenen Vorgehensweise durchzuführen.

Alle IT-Systeme der Schutzbedarfskategorie “hoch bis sehr hoch” sind einer detaillierten Risikoanalyse zu unterziehen. Die Auswahl einer konkreten Methode zur Risikoanalyse sowie der eventuelle Einsatz eines Tools zur Unterstützung dieser Analyse bleiben der durchführenden Institution überlassen. Details dazu finden sich in Kapitel 4.2 „Detaillierte Risikoanalyse“ dieses Handbuches.

Geht man von drei Schutzbedarfskategorien aus, so ist für IT-Systeme der Schutzbedarfskategorie “hoch” zu überlegen, ob mit (ev. verstärkten) Grundschutzmaßnahmen das Auslangen gefunden werden kann, oder eine detaillierte Risikoanalyse erforderlich ist. IT-Systeme der Schutzbedarfskategorie “sehr hoch” sind jedenfalls einer detaillierten Risikoanalyse zu unterziehen.

4.5 Akzeptables Restrisiko

Sicherheitsmaßnahmen können für gewöhnlich Risiken nur teilweise mindern. Im Allgemeinen verbleibt ein Restrisiko, dessen Abdeckung wirtschaftlich nicht mehr vertretbar wäre. Es ist notwendig, diese Restrisiken so exakt wie möglich zu quantifizieren und sie dann bewusst zu akzeptieren. Dieser Prozess wird als “Risikoakzeptanz” bezeichnet.

Um ein organisationsweit einheitliches Niveau des Restrisikos zu gewährleisten, ist es hilfreich, diesen Prozess durch generelle Richtlinien zu unterstützen. Diese sollten im Rahmen der Informationssicherheitspolitik definiert werden (vgl. Kapitel 3.2.4 „Risikoanalysestrategien, akzeptables Restrisiko und Akzeptanz von außergewöhnlichen Restrisiken“) und festlegen, welche Risiken die betroffene Organisation generell zu akzeptieren bereit ist.

Dabei ist zu beachten, dass durch Kumulationseffekte oder gegenseitige Beeinflussungen eine Reihe von kleinen Einzelrisiken zu einem inakzeptablen Restrisiko führen kann.

Die Entscheidung über die Akzeptanz von Restrisiken ist daher immer eine für das spezielle System zu treffende Managemententscheidung.

4.6 Akzeptanz von außergewöhnlichen Restrisiken

Verbleibt nach Durchführung aller vorgesehenen Sicherheitsmaßnahmen ein Restrisiko, das höher ist als das generell akzeptable, so sollten zusätzliche Sicherheitsmaßnahmen vorgesehen und damit das Risiko weiter reduziert werden.

Ist dies technisch nicht möglich oder unwirtschaftlich, so besteht in begründeten Ausnahmefällen die Möglichkeit, dieses erhöhte Restrisiko bewusst anzunehmen.

Die Entscheidung über die Akzeptanz eines außergewöhnlichen Restrisikos ist durch das Management zu treffen, die genauen Verantwortlichkeiten dafür sind in der Informationssicherheitspolitik festzulegen. Die Entscheidung ist schriftlich zu begründen und durch die Leitung der Organisation in schriftlicher Form zu akzeptieren.

5 Erstellung von Sicherheitskonzepten

Ausgehend von den in der Risikoanalyse ermittelten Sicherheitsanforderungen wird ein Sicherheitskonzept erstellt. Dies erfolgt durch die Auswahl geeigneter Maßnahmen, die die Risiken auf ein akzeptables Maß reduzieren und unter dem Gesichtspunkt von Kosten und Nutzen eine optimale Lösung darstellen.

Ein Sicherheitskonzept enthält

- die Beschreibung des Ausgangszustandes einschließlich der bestehenden Risiken (Ergebnisse der vorangegangenen Risikoanalyse),
- die Festlegung der durchzuführenden Maßnahmen,
- die Begründung der Auswahl unter Kosten/Nutzen-Aspekten und hinsichtlich des Zusammenwirkens der einzelnen Maßnahmen,
- eine Abschätzung des Restrisikos sowie eine verbindliche Aussage über die Akzeptanz des verbleibenden Restrisikos,
- die Festlegung der Verantwortlichkeiten für die Auswahl und Umsetzung der Maßnahmen sowie für die regelmäßige Überprüfung des Konzeptes sowie
- eine Prioritäten-, Termin- und Ressourcenplanung für die Umsetzung.

Die Erstellung eines Sicherheitskonzeptes erfolgt in vier Schritten:

Schritt 1: Auswahl von Maßnahmen
Schritt 2: Prüfung von Restrisiken und Risikoakzeptanz
Schritt 3: Erstellung von Sicherheitsrichtlinien
Schritt 4: Erstellung eines Informationssicherheitsplanes
Diese vier Schritte werden in den folgenden Kapiteln näher beschrieben.

5.1 Auswahl von Maßnahmen

Sicherheitsmaßnahmen sind Verfahrensweisen, Prozeduren und Mechanismen, die die Sicherheit von Informationen und der sie verarbeitenden IT-Systeme erhöhen. Dies kann auf unterschiedliche Arten erreicht werden.

Sicherheitsmechanismen können

- Risiken vermeiden,
- Bedrohungen oder Schwachstellen verkleinern,
- unerwünschte Ereignisse entdecken,
- die Auswirkung eines unerwünschten Ereignisses eingrenzen,
- Risiken überwälzen oder
- es möglich machen, einen früheren Zustand wiederherzustellen.

5.1.1 Klassifikation von Sicherheitsmaßnahmen

Je nach Betrachtungsweise kann eine Klassifikation von Sicherheitsmaßnahmen hinsichtlich nachfolgender Kriterien getroffen werden.

5.1.1.1 Klassifikation nach Art der Maßnahmen

Dies ist die "klassische" Einteilung der Sicherheitsmaßnahmen.

Man unterscheidet:

- (informations-)technische Maßnahmen
- bauliche Maßnahmen
- organisatorische Maßnahmen
- personelle Maßnahmen

5.1.1.2 Klassifikation nach Anwendungsbereichen

Man unterscheidet:

Maßnahmen, die organisationsweit (oder in Teilen der Organisation) einzusetzen sind.

Dazu gehören:

- Etablierung eines ISM-Prozesses und Erstellung von Informationssicherheitspolitiken
- organisatorische Maßnahmen (z.B. Kontrolle von Betriebsmitteln, Dokumentation, Rollentrennung)
- Überprüfung der IT-Sicherheitsmaßnahmen auf Übereinstimmung mit den Informationssicherheitspolitiken (Security Compliance Checking), Auditing
- Reaktion auf sicherheitsrelevante Ereignisse (Incident Handling)
- personelle Maßnahmen (incl. Schulung und Bildung von Sicherheitsbewusstsein)
- bauliche Sicherheit und Infrastruktur
- Notfallvorsorge

Systemspezifische Maßnahmen.

Die Auswahl systemspezifischer Maßnahmen hängt in hohem Maße vom Typ des zu schützenden IT-Systems ab. Man unterscheidet etwa:

- Nicht-vernetzte Systeme (Stand-Alone-PCs)
- Workstations in einem Netzwerk
- Server in einem Netzwerk

5.1.1.3 Klassifikation nach Gefährdungen und Sicherheitsanforderungen

Ausgehend von den Grundbedrohungen gegen ein IT-System (Verlust der Vertraulichkeit, Integrität, Verfügbarkeit, etc.) werden die typischen Gefährdungen ermittelt.

Man unterscheidet daher:

- Maßnahmen zur Gewährleistung der Vertraulichkeit (confidentiality)
- Maßnahmen zur Gewährleistung der Integrität (integrity)
- Maßnahmen zur Gewährleistung der Verfügbarkeit (availability)
- Maßnahmen zur Gewährleistung der Zurechenbarkeit (accountability)
- Maßnahmen zur Gewährleistung der Authentizität (authenticity)
- Maßnahmen zur Gewährleistung der Zuverlässigkeit (reliability)

Wirksame Informationssicherheit verlangt im Allgemeinen eine Kombination von verschiedenen Sicherheitsmaßnahmen, wobei auf die Ausgewogenheit von technischen und nicht-technischen Maßnahmen zu achten ist.

5.1.2 Ausgangsbasis für die Auswahl von Maßnahmen

Liste existierender bzw. geplanter Sicherheitsmaßnahmen:

Bei der Auswahl von Sicherheitsmaßnahmen zur Verminderung der Risiken wird vorausgesetzt, dass im vorhergehenden Schritt - der Risikoanalyse - die bereits existierenden Sicherheitsmaßnahmen aufgelistet wurden.

Im Fall einer detaillierten Risikoanalyse erfolgt dies im Rahmen der “Identifikation bestehender Schutzmaßnahmen” (vgl. Kapitel 4.2.6), die als Ergebnis eine Aufstellung aller existierenden oder bereits geplanten Schutzmaßnahmen mit Angaben über ihren Implementierungsstatus und ihren Einsatz liefern soll. Bei einer Grundschutzanalyse werden die vorhandenen Maßnahmen im Rahmen des Soll-Ist-Vergleiches (vgl. Kapitel 4.3.2.2) ermittelt.

Ergebnisse der Risikobewertung:

Die Auswahl der Sicherheitsmaßnahmen, die die Risiken auf ein definiertes und beherrschbares Maß reduzieren, muss auf den Ergebnissen der Risikobewertung basieren.

Diese Auswahl wird von einer Reihe von Faktoren beeinflusst:

- der Stärke der einzelnen Maßnahmen
- ihrer Benutzerfreundlichkeit und Transparenz für die Anwender/innen
- der Art der Schutzfunktion (Verringerung von Bedrohungen, Erkennen von Verletzungen, ...)

In der Regel stehen verschiedene mögliche Sicherheitsmaßnahmen zur Auswahl. Um die sowohl aus Sicherheits- als auch aus Wirtschaftlichkeitsüberlegungen effizienteste Lösung zu finden, kann im Einzelfall eine Kosten-/Nutzen-Analyse bzw. ein direkter Vergleich einzelner Sicherheitsmaßnahmen (trade-off analysis) notwendig sein.

5.1.3 Auswahl von Maßnahmen auf Basis einer detaillierten Risikoanalyse

Wurde eine detaillierte Risikoanalyse durchgeführt, so stehen für die Auswahl von geeigneten Sicherheitsmaßnahmen detailliertere und spezifischere Informationen zur Verfügung als im Fall einer Grundschutzanalyse. Je genauer und aufwändiger die Risikoanalyse durchgeführt wurde, desto qualifizierter ist im Allgemeinen die für den Auswahlprozess zur Verfügung stehende Information.

In der Mehrzahl der Fälle wird es verschiedene Maßnahmen zur Erfüllung einer bestimmten Sicherheitsanforderung geben, die sich jedoch hinsichtlich ihrer Effizienz und ihrer Kosten unterscheiden. Umgekehrt kann eine Maßnahme gleichzeitig mehrere Sicherheitsanforderungen abdecken.

Welche der in Frage kommenden Maßnahmen tatsächlich ausgewählt und implementiert werden, hängt von den speziellen Umständen ab. Generell ist festzuhalten, dass Sicherheitsmaßnahmen einen oder mehrere der folgenden Aspekte abdecken können:

- Vorbeugung (präventive Maßnahmen)
- Aufdeckung (detektive Maßnahmen)
- Abschreckung
- Schadensbegrenzung
- Wiederherstellung eines früheren Zustandes
- Bildung von Sicherheitsbewusstsein
- Risikoüberwälzung

Welche dieser Eigenschaften notwendig bzw. wünschenswert ist, ist vom spezifischen Fall abhängig. In der Regel wird man Maßnahmen bevorzugen, die mehrere dieser Aspekte abdecken. Es ist aber auch darauf zu achten, dass die Gesamtheit der ausgewählten Maßnahmen ein ausgewogenes Verhältnis der einzelnen Aspekte aufweist, dass also nicht beispielsweise ausschließlich detektive oder ausschließlich präventive Maßnahmen zum Einsatz kommen.

5.1.4 Auswahl von Maßnahmen im Falle eines Grundschutzansatzes

Grundsätzlich ist die Auswahl von Sicherheitsmaßnahmen im Falle eines Grundschutzansatzes relativ einfach. In Maßnahmenkatalogen wird eine Reihe von Schutzmaßnahmen gegen die meisten üblichen Bedrohungen angeführt. Die betreffenden Bedrohungen werden a priori, d.h. ohne weitere Risikoanalyse, als relevant für die durchführende Organisation angenommen. Die empfohlenen Maßnahmen werden mit den existierenden oder bereits geplanten Maßnahmen verglichen. Die noch nicht existierenden bzw. geplanten Maßnahmen werden in eine Liste von noch zu realisierenden Maßnahmen zusammengefasst.

Standardwerke zur Auswahl von Maßnahmen:

In Teil 2 dieses Sicherheitshandbuches werden die wichtigsten Grundschutzmaßnahmen für die öffentliche Verwaltung in Österreich aufgeführt. Alternativ kann auch auf andere bestehende Kataloge zurückgegriffen werden.

Eine sehr umfangreiche Sammlung von Grundschutzmaßnahmen, die kontinuierlich weiterentwickelt werden, findet sich etwa in den Maßnahmenkatalogen zum IT-Grundschutz des BSI (vgl. Kapitel 4.3 dieses Handbuches). Die Unterstützung durch das “IT-Grundschutz-Tool” erleichtert die Auswahl, Dokumentation und Verwaltung der Maßnahmen.

5.1.5 Auswahl von Maßnahmen im Falle eines kombinierten Risikoanalyseansatzes

Im Falle eines kombinierten Ansatzes werden zunächst anhand eines Grundschutzkataloges entsprechende Schutzmaßnahmen ausgewählt und umgesetzt, die einerseits ein adäquates Sicherheitsniveau für Systeme der Schutzbedarfsklasse "niedrig bis mittel" gewährleisten, andererseits auch für hochschutzbedürftige Systeme bereits ein gewisses Maß an Schutz bieten. Anschließend werden die noch fehlenden Sicherheitsmaßnahmen für IT-Systeme mit hohen bis sehr hohen Sicherheitsanforderungen ausgewählt.

5.1.6 Bewertung von Maßnahmen

Unabhängig von der verfolgten Strategie ist es in jedem Fall notwendig, die Auswirkungen der ausgewählten Maßnahmen zu analysieren. Damit soll gewährleistet werden, dass die zusätzlichen Maßnahmen mit dem IT-Gesamtkonzept und den bereits bestehenden Sicherheitsmaßnahmen verträglich sind, d.h. dass sie einander ergänzen und unterstützen und sich nicht etwa gegenseitig behindern oder in ihrer Wirkung schwächen. In diesem Stadium ist auch die Einbeziehung der betroffenen Benutzer/innen zu empfehlen, da die Wirksamkeit von Sicherheitsmaßnahmen stark davon abhängt, in welchem Maß sie akzeptiert oder aber abgelehnt oder umgangen werden. Die Akzeptanz von Maßnahmen steigt, wenn ihre Notwendigkeit für die Benutzer/innen einsichtig ist.

Zur Bewertung von Sicherheitsmaßnahmen ist wie folgt vorzugehen:

- Erfassung aller Bedrohungen, gegen die die ausgewählten Maßnahmen wirken,
- Beschreibung der Auswirkung der Einzelmaßnahmen,
- Beschreibung des Zusammenwirkens der ausgewählten und der bereits vorhandenen Sicherheitsmaßnahmen,
- Überprüfung, ob und inwieweit die Maßnahmen zu Behinderungen beim Betrieb des IT-Systems führen können,
- Überprüfung der Vereinbarkeit der Maßnahmen mit geltenden rechtlichen Vorschriften und Richtlinien und
- Bewertung, in welchem Ausmaß die Maßnahmen eine Reduktion der Risiken bewirken.

Bevor die Maßnahmen umgesetzt werden, sollte die Leitungsebene entscheiden, ob die Kosten für die Realisierung der Maßnahmen im richtigen Verhältnis zur Reduzierung der Risiken stehen und ob die Risiken auf ein akzeptables Maß beschränkt werden.

5.1.7 Rahmenbedingungen

Bei der Auswahl und Umsetzung von Sicherheitsmaßnahmen sind stets auch Rahmenbedingungen zu berücksichtigen, die entweder durch das Umfeld vorgegeben oder durch das Management festgelegt werden.

Beispiele für solche Rahmenbedingungen sind:

- Zeitliche Rahmenbedingungen:
  Wie schnell ist auf ein erkanntes Risiko zu reagieren? Wann kann/muss eine Maßnahme realisiert sein?
- Finanzielle Rahmenbedingungen:
  Im Allgemeinen werden budgetäre Einschränkungen existieren. Die Kosten für Sicherheitsmaßnahmen müssen in einem angemessenen Verhältnis zum Wert der zu schützenden Objekte stehen.
- Umweltbedingungen:
  Auch durch das Umfeld vorgegebene Rahmenbedingungen, wie etwa die Lage eines Gebäudes, klimatische Bedingungen und Platzangebot können die Auswahl von Sicherheitsmaßnahmen beeinflussen.
- Technische Rahmenbedingungen:
  z.B. Kompatibilität von Hard- und/oder Software

Weitere Einschränkungen können organisatorischer, personeller, gesetzlicher oder sozialer Natur sein.

Auch Rahmenbedingungen können im Laufe der Zeit, durch soziale Veränderungen oder durch Veränderungen im technischen oder organisatorischen Umfeld, einem Wandel unterliegen und sind daher regelmäßig zu überprüfen und zu hinterfragen.

5.2 Risikoakzeptanz

Absolute Sicherheit ist nicht erreichbar - auch nach Auswahl und Umsetzung aller angemessenen Sicherheitsmaßnahmen verbleibt im Allgemeinen ein Restrisiko. Um zu entscheiden, ob dieses für die betreffende Organisation tragbar ist oder weitere Maßnahmen zu veranlassen sind, ist wie folgt vorzugehen:

Schritt 1: Quantifizierung des Restrisikos

In diesem ersten Schritt ist das Restrisiko so exakt wie möglich zu ermitteln. Dabei bedient man sich am besten der Verfahren und Erkenntnisse aus der vorangegangenen Risikoanalyse.

Schritt 2: Bewertung der Restrisiken

Die verbleibenden Restrisiken sind als “akzeptabel” oder “nicht-akzeptabel” zu klassifizieren. Die Entscheidungsgrundlage dafür sollte in der (organisationsweiten) Informationssicherheitspolitik festgelegt sein (vgl. Kapitel 3.2.4 „Risikoanalysestrategien, akzeptables Restrisiko und Akzeptanz von außergewöhnlichen Restrisiken“, Schritt 2, sowie Kapitel 4.5 „Akzeptables Restrisiko“). Akzeptable Restrisiken können in Kauf genommen werden, nicht-akzeptable bedürfen einer weiteren Analyse.

Schritt 3: Entscheidung über nicht-akzeptable Restrisiken

Die weitere Behandlung von nicht-akzeptablen Restrisiken sollte stets eine Management-Entscheidung sein. Es besteht die Möglichkeit, zu untersuchen, wie weit und mit welchen Kosten nicht-akzeptable Restrisiken weiter verringert werden können, und zusätzliche, eventuell mit hohen Kosten verbundene Maßnahmen auszuwählen. Die Alternative dazu ist eine bewusste und dokumentierte Akzeptanz des erhöhten Restrisikos.

Schritt 4: Akzeptanz von außergewöhnlichen Restrisiken

Ist eine weitere Reduktion des Restrisikos nicht möglich, unwirtschaftlich oder aufgrund gegebener Rahmenbedingungen nicht wünschenswert, so besteht in begründeten Ausnahmefällen die Möglichkeit einer bewussten Akzeptanz dieses erhöhten Restrisikos. Das Vorgehen dabei und die Verantwortlichkeiten dafür sind in der Informationssicherheitspolitik festzulegen.

5.3 Sicherheitsrichtlinien

5.3.1 Aufgaben und Ziele

Für alle komplexen oder stark verbreiteten IT-Systeme sollten spezifische Sicherheitsrichtlinien erarbeitet werden. Typische Beispiele sind etwa eine PC-Sicherheitsrichtlinie, eine Netzsicherheitsrichtlinie oder eine Internet-Sicherheitsrichtlinie.

5.3.2 Inhalte

Eine Sicherheitsrichtlinie 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 Informationssicherheitsziele des Systems
- Abhängigkeit der Organisation vom betrachteten IT-System; dabei ist zu untersuchen, wie weit die Aufgabenerfüllung der Organisation durch eine Verletzung der Vertraulichkeit, Verfügbarkeit oder Integrität des Systems oder darauf verarbeiteter Information gefährdet wird.
- Investitionen in das System (Entwicklungs-, Beschaffungs- und Wartungskosten, Kosten für den laufenden Betrieb)
- 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 den laufenden Betrieb (Wartung) der Sicherheitsmaßnahmen
- Verantwortlichkeiten

5.3.3 Fortschreibung der Sicherheitsrichtlinien

Auch eine Sicherheitsrichtlinie stellt kein einmal erstelltes, unveränderbares Dokument dar, sondern ist regelmäßig auf Aktualität zu überprüfen und bei Bedarf entsprechend anzupassen.

Insbesondere ist es von Bedeutung, dass die Liste der existierenden bzw. noch umzusetzenden Sicherheitsmaßnahmen stets dem tatsächlich aktuellen Stand entspricht.

5.3.4 Verantwortlichkeiten

Die Verantwortlichkeiten für die Erstellung und Fortschreibung der Sicherheitsrichtlinien sind im Einzelnen in der Informationssicherheitspolitik festzulegen (vgl. dazu Kapitel 3.2.2 „Organisation und Verantwortlichkeiten für Informationssicherheit“). Im Allgemeinen wird diese Verantwortung bei der/dem für das gegenständliche System zuständigen Bereichs-IT-Sicherheitsbeauftragten liegen, die/der sie mit der/dem IT-Sicherheitsbeauftragten abstimmen wird. Letztere/r hat dafür Sorge zu tragen, dass die einzelnen Sicherheitsrichtlinien mit der organisationsweiten Informationssicherheitspolitik kompatibel sind und auch untereinander ein einheitliches, vergleichbares Niveau aufweisen.

5.4 Informationssicherheitsplan

Der Informationssicherheitsplan beschreibt, wie die ausgewählten Sicherheitsmaßnahmen umgesetzt werden. Er enthält eine Prioritäten- und Ressourcenplanung sowie einen Zeitplan für die Umsetzung der Maßnahmen.

Im Detail sind für jedes System zu erstellen:

- eine Liste der vorhandenen sowie eine Liste der noch zu implementierenden Sicherheitsmaßnahmen; für jede dieser Maßnahmen sollte eine Aussage über ihre Wirksamkeit sowie möglicherweise notwendige Verbesserungen oder Verstärkungen getroffen werden.
- eine Prioritätenreihung für die Implementierung der ausgewählten Sicherheitsmaßnahmen bzw. die Verbesserung bestehender Maßnahmen.
- eine Kosten- und Aufwandsschätzung für Implementierung und Wartung der Maßnahmen.
- Detailplanung für die Implementierung.
  Diese soll folgende Punkte umfassen:
  - Prioritäten
  - Zeitplan, abhängig von Prioritäten und Ressourcen
  - Budget
  - Verantwortlichkeiten
  - Schulungs- und Sensibilisierungsmaßnahmen
  - Test- und Abnahmeverfahren und -termine
  - Nachfolgeaktivitäten
- eine Bewertung des nach der Implementierung aller Maßnahmen zu erwartenden Restrisikos.

Weiters sollte der Sicherheitsplan auch die Kontrollmechanismen festlegen, die den Fortschritt der Implementierung der ausgewählten Maßnahmen bewerten, und Möglichkeiten des Eingriffes bei Abweichungen vom vorgesehenen Prozess oder bei notwendigen Änderungen definieren.

5.5 Fortschreibung des Sicherheitskonzeptes

Auch das Sicherheitskonzept muss laufend fortgeschrieben werden.

Anlässe für eine neue Untersuchung und das Fortschreiben des Konzeptes können sein:

- Ablauf eines vorgeschriebenen oder vereinbarten Zeitraumes (z.B. jährliches Update)
- Eintritt von Ereignissen, die die Bedrohungslage verändern, wie etwa politische oder gesellschaftliche Entwicklungen oder das Bekannt werden neuer Attacken
- Eintritt von Ereignissen, die die Werte verändern können, wie etwa die Änderungen von Organisationszielen oder Aufgabenbereichen, Änderungen am Markt oder die Einführung neuer Applikationen
- Ereignisse, die die Eintrittswahrscheinlichkeit von Bedrohungen verändern, wie etwa die Entwicklung neuer Techniken oder veränderte Einsatzbedingungen (Einsatzort, IT-Ausstattung, ...)
- neue Möglichkeiten für Sicherheitsmaßnahmen, etwa aufgrund von Preisänderungen oder der Verfügbarkeit neuer Technologien

Voraussetzungen für eine effiziente und zielgerichtete Fortschreibung des Sicherheitskonzeptes sind

- die laufende Überprüfung von Akzeptanz und Einhaltung der Sicherheitsmaßnahmen
- die Protokollierung von Schadensereignissen
- die Kontrolle der Wirksamkeit und Angemessenheit der Maßnahmen

Ob eine neuerliche Risikoanalyse erforderlich ist oder lediglich die Auswahl der Maßnahmen überarbeitet wird, hängt vom Ausmaß der eingetretenen Veränderungen ab.

6 Umsetzung des Informationssicherheitsplanes

Die korrekte und effiziente Implementierung von Sicherheitsmaßnahmen und ihr zielgerichteter Einsatz hängen in hohem Maße von der Qualität des im vorangegangenen Schritt erstellten Informationssicherheitsplanes ab. Dieser muss gut strukturiert, genau dokumentiert und den tatsächlichen Anforderungen der betroffenen Institution angepasst sein.

Bei der Umsetzung des Planes ist zu beachten, dass

- Verantwortlichkeiten rechtzeitig und eindeutig festgelegt werden,
- finanzielle und personelle Ressourcen rechtzeitig zugewiesen werden,
- die Maßnahmen korrekt umgesetzt werden,
- die Kosten sich in dem vorher abgeschätzten Rahmen halten und
- der Zeitplan eingehalten wird.

Gleichzeitig mit der Implementierung der Sicherheitsmaßnahmen sollten auch entsprechende Schulungs- und Sensibilisierungsmaßnahmen gesetzt werden, um die optimale Einhaltung und Akzeptanz der Maßnahmen bei den Anwendern/innen zu erreichen.

Als letzter Schritt der Umsetzung des Informationssicherheitsplanes sind die implementierten Maßnahmen in ihrer tatsächlichen Einsatzumgebung auf ihre Auswirkungen zu testen und abzunehmen (Akkreditierung).

Es empfiehlt sich, die Umsetzung des Informationssicherheitsplanes im Rahmen eines Projektes abzuwickeln.

6.1 Implementierung von Maßnahmen

Sobald der Informationssicherheitsplan erstellt und verabschiedet wurde, sind die einzelnen Maßnahmen zu implementieren, auf ihre Übereinstimmung mit der Sicherheitspolitik zu überprüfen (Security Compliance Checking) und auf Korrektheit und Vollständigkeit zu testen.

Dabei ist zu beachten, dass ein Teil der Maßnahmen systemspezifisch sein wird, ein anderer Teil aber organisationsweit einzusetzen ist (vgl. dazu auch Kapitel 5.1.).

Die Abstimmung der einzelnen systemspezifischen Informationssicherheitspläne für die Gesamtorganisation obliegt in der Regel der/dem IT-Sicherheitsbeauftragten. Sie/er hat dafür Sorge zu tragen, dass

- die systemübergreifenden, organisationsweiten Maßnahmen vollständig und angemessen, sowie nicht redundant oder widersprüchlich sind, und
- die systemspezifischen Maßnahmen kompatibel sind und ein einheitliches, angemessenes Sicherheitsniveau haben.

Besonderer Wert ist auf eine detaillierte, korrekte und aktuelle Dokumentation dieser Implementierungen zu legen.

Schritt 1: Implementierung der Sicherheitsmaßnahmen

Die Implementierung der ausgewählten Sicherheitsmaßnahmen hat anhand des Informationssicherheitsplanes, entsprechend der vorgegebenen Zeitpläne und Prioritäten, zu erfolgen.

Die Verantwortlichkeiten dafür sind im Detail festzulegen.

Schritt 2: Tests

Tests sollen sicherstellen, dass die Implementierung korrekt durchgeführt und abgeschlossen wurde.

Es wird empfohlen, für die Tests einen Testplan zu erstellen, der

- die Testmethoden,
- die Testumgebung sowie
- die Zeitpläne für die Durchführung der Tests

beinhaltet.

Die durchgeführten Tests sind im Detail zu beschreiben und die Ergebnisse in einem standardisierten Testbericht festzuhalten.

Abhängig von der speziellen Bedrohungslage und der Art der Maßnahmen kann die Durchführung von Penetrationstests erforderlich sein.

Schritt 3: Prüfung der Maßnahmen auf Übereinstimmung mit der Informationssicherheitspolitik (Security Compliance Checking)

Security Compliance Checks sind sowohl im Rahmen der Implementierung der Maßnahmen als auch als wiederholte Aktivität zur Gewährleistung der Informationssicherheit im laufenden Betrieb (s. dazu auch Kapitel 7) durchzuführen.

Dabei sind zu prüfen:

- die vollständige und korrekte Umsetzung der Sicherheitsmaßnahmen
- der korrekte Einsatz der implementierten Sicherheitsmaßnahmen
- die Einhaltung der organisatorischen Sicherheitsmaßnahmen im täglichen Betrieb

Dokumentation

Die Dokumentation der implementierten Maßnahmen stellt einen wichtigen Teil der gesamten Sicherheitsdokumentation dar und ist notwendige Voraussetzung für die Kontinuität und Konsistenz des Informationssicherheitsprozesses. Die wichtigsten Anforderungen an die Dokumentation:

- Aktualität: Alle Sicherheitsmaßnahmen sind stets auf dem aktuellen Stand der Realisierung zu beschreiben.
- Vollständigkeit

- Hoher Detaillierungsgrad: Die Sicherheitsmaßnahmen sind so detailliert zu beschreiben, dass zum einen eventuell bestehende Sicherheitslücken erkannt werden können, zum anderen ausreichend Information für einen korrekten und effizienten Einsatz der Maßnahmen zur Verfügung steht.
- Gewährleistung der Vertraulichkeit: Dokumentation über Sicherheitsmaßnahmen kann unter Umständen sehr vertrauliche Information enthalten und ist daher entsprechend zu schützen. So weit wie möglich sollte bei der Klassifizierung und Behandlung solcher Dokumente auf die Vorgaben im Rahmen der Informationssicherheitspolitik der Organisation zurückgegriffen werden (vgl. dazu Kapitel 3.2.5). Es kann im Einzelfall notwendig sein, weitere Verfahrensweisen zur Erstellung, Verteilung, Benutzung, Aufbewahrung und Vernichtung von sicherheitsrelevanter Dokumentation zu entwickeln. Diese Verfahrensweisen sind ebenfalls entsprechend zu dokumentieren.
- Konfigurations- und Integritätskontrolle: Es ist sicherzustellen, dass keine unauthorisierten Änderungen der Dokumentation erfolgen, die eine - beabsichtigte oder unbeabsichtigte - Beeinträchtigung der implementierten Maßnahmen nach sich ziehen könnten.

6.2 Sensibilisierung (Security Awareness)

Nur durch Verständnis und Motivation ist eine dauerhafte Einhaltung und Umsetzung der Richtlinien und Vorschriften zur Informationssicherheit zu erreichen. Um das Sicherheitsbewusstsein aller Mitarbeiter/innen zu fördern und den Stellenwert der Informationssicherheit innerhalb einer Organisation zu betonen, sollte ein umfassendes, organisationsweites Sensibilisierungsprogramm erstellt werden, das zum Ziel hat, Informationssicherheit zu einem integrierten Bestandteil der täglichen Arbeit zu machen.

Das Sensibilisierungsprogramm sollte systemübergreifend sein. Es ist Aufgabe der dafür verantwortlichen Person - dies wird in der Regel die/der IT-Sicherheitsbeauftragte sein - die Anforderungen aus den einzelnen Teilbereichen und systemspezifische Anforderungen hier einfließen zu lassen und entsprechend zu koordinieren.

Das Sensibilisierungsprogramm sollte folgende Punkte umfassen:

- Information aller Mitarbeiter/innen über die Informationssicherheitspolitik der Organisation. Im Rahmen einer Einführung sollten insbesondere folgende Punkte erläutert werden:
  - die Informationssicherheitsziele und -politik der Institution sowie deren Erläuterung,
  - die Bedeutung der Informationssicherheit für die Institution,
  - Organisation und Verantwortlichkeiten im Bereich der Informationssicherheit,
  - die Risikoanalysestrategie,
  - die Sicherheitsklassifizierung von Daten,
  - ausgewählte Sicherheitsmaßnahmen (insbesondere solche, die für die gesamte Organisation Gültigkeit haben),
- die wichtigsten Ergebnisse der Risikoanalysen (Bedrohungen, Schwachstellen, Risiken, ...),
- die Pläne zur Implementierung und Überprüfung der Sicherheitsmaßnahmen,
- die Auswirkungen von sicherheitsrelevanten Ereignissen für einzelne Anwender/innen und für die gesamte Institution,
- die Notwendigkeit, Sicherheitsverstöße zu melden und zu untersuchen, und
- die Konsequenzen bei Nichteinhaltung von Sicherheitsvorgaben.

Zur Sensibilisierung der Mitarbeiter/innen können u.a. folgende Maßnahmen beitragen:

- regelmäßige Veranstaltungen zum Thema Informationssicherheit
- Publikationen
- schriftliche Festlegung der Berichtswege und Handlungsanweisungen im Falle eines vermuteten Sicherheitsproblems (z.B. Auftreten eines Virus, Hacker-Angriff, ...)

Das Sensibilisierungsprogramm sollte jede/n Mitarbeiter/in der Institution auf ihre/seine Verantwortlichkeit für Informationssicherheit hinweisen. Dabei ist insbesondere die Verantwortung des Managements für Informationssicherheit zu betonen ("Informationssicherheit als Managementaufgabe"). Die organisationsweite Planung dieser Veranstaltungen sollte die/der IT-Sicherheitsbeauftragte übernehmen. Gegebenenfalls liefern Bereichs-IT-Sicherheitsbeauftragte Informationen, wann und wo solche Veranstaltungen nötig sind.

Die Veranstaltungen zum Sensibilisierungsprogramm sollten in regelmäßigen Zeitabständen wiederholt werden, um das vorhandene Wissen aufzufrischen und neue Mitarbeiter/innen zu informieren. Darüber hinaus sollte jede/r neue, beförderte oder versetzte Mitarbeiter/in so weit in Fragen der Informationssicherheit geschult werden, wie es der neue Arbeitsplatz verlangt.

Das Sensibilisierungsprogramm ist regelmäßig auf seine Wirksamkeit und Aktualität zu überprüfen und laufend an Veränderungen in der Informationssicherheitspolitik sowie an neue Technologien anzupassen.

6.3 Schulung

Über das allgemeine Sensibilisierungsprogramm hinaus sind spezielle Schulungen zu Teilbereichen der Informationssicherheit erforderlich, wenn sich durch Sicherheitsmaßnahmen einschneidende Veränderungen, z.B. im Arbeitsablauf, ergeben.

Weiters sind Personen, die in besonderem Maße mit Informationssicherheit zu tun haben, speziell dafür auszubilden und zu schulen. Dazu zählen etwa:

- die/der IT-Sicherheitsbeauftragte und die Bereichs-IT-Sicherheitsbeauftragten
- die Mitglieder des Informationssicherheitsmanagement-Teams
- Mitarbeiter/innen, die zu EINGESCHRÄNT; VERTRAULICH, GEHEIM oder STRENG GEHEIM eingestuften Informationen Zugang haben
- Mitarbeiter/innen mit spezieller Verantwortung für die Systementwicklung (z.B. Projektleiter/innen)
- Mitarbeiter/innen mit spezieller Verantwortung für den Betrieb eines IT-Systems oder einer wichtigen Applikation (z.B. Applikationsverantwortliche)
- Mitarbeiter/innen, die mit Aufgaben der IT-Sicherheitsverwaltung betraut sind (z.B. Vergabe von Zutritts-, Zugangs- und Zugriffsrechten)

Das Schulungsprogramm ist von jeder Organisation spezifisch für ihren Bedarf zu entwickeln. Besondere Betonung ist dabei auf die Schulung der korrekten Implementierung und Anwendung von Sicherheitsmaßnahmen zu legen. Typische Beispiele für die Themen, die im Rahmen von Schulungsveranstaltungen behandelt werden sollten, sind:

- Sicherheitspolitik und -infrastruktur:
  Rollen und Verantwortlichkeiten, Organisation des Informationssicherheitsmanagements, Behandlung von sicherheitsrelevanten Vorfällen, regelmäßige Überprüfung von Sicherheitsmaßnahmen und ähnliches
- Bauliche Sicherheit:
  Schutz von Gebäuden, Serverräumen, Büroräumen und Versorgungseinrichtungen mit besonderer Betonung der Verantwortung der einzelnen Mitarbeiter/innen (z.B. Handhabung von Zutrittskontrollmaßnahmen, Brandschutz)
- Personelle Sicherheit
- Hardware- und Softwaresicherheit:
  Dazu gehören etwa Identifikation und Authentisierung, Berechtigungssysteme, Protokollierung, Wiederaufbereitung und Virenschutz.
- Netzwerksicherheit:
  Netzwerkinfrastruktur, LANs, Inter-/Intranets, Verschlüsselung, digitale Signaturen u.ä.
- Business Continuity Planung

Schulungs- und Sensibilisierungsveranstaltungen zum Thema Informationssicherheit müssen zeitgerecht geplant und umgesetzt werden, um keine Sicherheitslücken durch mangelndes Wissen oder Sicherheitsbewusstsein entstehen zu lassen.

6.4 Akkreditierung

Unter Akkreditierung eines IT-Systems versteht man die Sicherstellung, dass dieses den Anforderungen der Informationssicherheitspolitik und der Sicherheitsrichtlinien 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 eine spezifische Anwendung - in Echtbetrieb gehen.

Techniken zur Akkreditierung sind:

- Prüfung der Maßnahmen auf Übereinstimmung mit der Informationssicherheitspolitik (Security Compliance Checking), vgl. auch Kapitel Implementierung von Maßnahmen 6.1 und Überprüfung von Maßnahmen auf Übereinstimmung mit der Informationssicherheitspolitik (Security Compliance Checking) 7.1.2.
- 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 Neuakkreditierung durchzuführen ist, sollten in den zugehörigen Sicherheitsrichtlinien festgelegt werden.

7 Informationssicherheit im laufenden Betrieb

Umfassendes Informationssicherheitsmanagement beinhaltet nicht zuletzt auch die Aufgabe, die Informationssicherheit im laufenden Betrieb aufrechtzuerhalten. Ein Sicherheitskonzept ist kein statisches, unveränderbares Dokument, sondern muss stets auf seine Wirksamkeit, Aktualität und die Umsetzung in der täglichen Praxis überprüft werden. Weiters muss eine angemessene Reaktion auf alle sicherheitsrelevanten Änderungen sowie auf sicherheitsrelevante Ereignisse gewährleistet sein.

Ziel aller Follow-Up-Aktivitäten ist es, das erreichte Sicherheitsniveau zu erhalten bzw. weiter zu erhöhen. Verschlechterungen der Wirksamkeit von Sicherheitsmaßnahmen - sei es durch eine Veränderung der Bedrohungslage oder durch falsche Verwendung der implementierten Sicherheitsmaßnahmen - sollen erkannt und entsprechende Gegenmaßnahmen eingeleitet werden.

7.1 Aufrechterhaltung des erreichten Sicherheitsniveaus

Das nach der Umsetzung des Informationssicherheitsplanes erreichte Sicherheitsniveau lässt sich nur dann aufrechterhalten, wenn

- Wartung und administrativer Support der Sicherheitseinrichtungen gewährleistet sind,
- die realisierten Maßnahmen regelmäßig auf ihre Übereinstimmung mit der Informationssicherheitspolitik geprüft (Security Compliance Checking) und
- die IT-Systeme fortlaufend überwacht werden (Monitoring).

Die Verantwortlichkeiten für diese Aktivitäten müssen im Rahmen der organisationsweiten Informationssicherheitspolitik bzw. in den einzelnen Sicherheitsrichtlinien detailliert festgelegt werden. Generell gilt auch hier, dass die Verantwortung für systemspezifische Maßnahmen bei den einzelnen Bereichs-IT-Sicherheitsbeauftragten - soweit definiert - liegen sollte, die Verantwortung für organisationsweite Sicherheitsmaßnahmen sowie die Gesamtverantwortung bei der/dem Sicherheitsbeauftragten.

Von besonderer Wichtigkeit für die Aufrechterhaltung oder weitere Erhöhung eines einmal erreichten Sicherheitsniveaus ist eine permanente Sensibilisierung aller betroffenen Mitarbeiter/innen für Fragen der Informationssicherheit (vgl. dazu auch Kapitel 6.2).

7.1.1 Wartung und administrativer Support von Sicherheitseinrichtungen

Viele Sicherheitsmaßnahmen erfordern zur Gewährleistung ihrer einwandfreien Funktionsfähigkeit Wartung und administrativen Support. Zu diesen Aufgaben zählen etwa die regelmäßige Auswertung und Archivierung von Protokollen, Backup und Restore sowie die Wartung von sicherheitsrelevanten Komponenten, die Überprüfung der Parametereinstellungen und eventueller Rechte auf mögliche nichtautorisierte Änderungen, die Reinitialisierung von Startwerten oder Zählern sowie Updates der Sicherheitssoftware, wenn verfügbar (besonders, aber nicht ausschließlich, im Bereich Virenschutz).

Alle Wartungs- und Supportaktivitäten sollten nach einem detailliert festgelegten Plan erfolgen und regelmäßig durchgeführt werden.

Die Wartung von Sicherheitseinrichtungen hat in Abstimmung mit den Verträgen, die mit den Lieferfirmen geschlossen wurden, zu erfolgen und darf nur durch dafür authorisierte Personen vorgenommen werden.

Die Kosten für Wartungs- und Supportaufgaben können im Einzelfall beträchtlich sein und sollten daher bereits bei der Auswahl der Sicherheitsmaßnahmen bekannt sein und in den Entscheidungsprozess mit einfließen.

Um die Aufrechterhaltung eines einmal erreichten Sicherheitsniveaus zu gewährleisten, ist sicherzustellen, dass

- die erforderlichen finanziellen und personellen Ressourcen zur Wartung von Sicherheitseinrichtungen zur Verfügung stehen,
- organisatorische Regelungen existieren, die die Aufrechterhaltung der Informationssicherheitsmaßnahmen im laufenden Betrieb ermöglichen und unterstützen,
- die Verantwortungen im laufenden Betrieb klar zugewiesen werden,
- die Maßnahmen regelmäßig daraufhin geprüft werden, ob sie wie beabsichtigt funktionieren und
- Maßnahmen verstärkt werden, falls sich neue Schwachstellen zeigen.

Alle Wartungs- und Supportaktivitäten im Sicherheitsbereich sollten protokolliert werden. Der regelmäßigen Auswertung dieser Protokolle kommt besondere Bedeutung für die gesamte Informationssicherheit zu.

7.1.2 Überprüfung von Maßnahmen auf Übereinstimmung mit der Informationssicherheitspolitik (Security Compliance Checking)

Zielsetzung

Zur Gewährleistung eines angemessenen und gleich bleibenden Sicherheitsniveaus ist dafür Sorge zu tragen, dass alle Maßnahmen so eingesetzt werden, wie es im Sicherheitskonzept und im Informationssicherheitsplan vorgesehen ist. Dies muss für alle IT-Systeme, -Projekte und Applikationen sowohl während der Planungsphase als auch im laufenden Betrieb und letztlich auch bei der Außerbetriebnahme sichergestellt sein.

Dabei ist zu prüfen,

- ob die Sicherheitsmaßnahmen vollständig und korrekt umgesetzt werden,
- der korrekte Einsatz der implementierten Sicherheitsmaßnahmen gewährleistet ist (Stichproben!) und
- die organisatorischen Sicherheitsvorgaben im täglichen Betrieb eingehalten und akzeptiert werden.

Weiters sind die getroffenen Maßnahmen regelmäßig auf Übereinstimmung mit gesetzlichen und betrieblichen Vorgaben zu überprüfen.

Die Prüfungen können durch externe oder interne Auditoren durchgeführt werden und sollten soweit möglich auf standardisierten Tests und Checklisten basieren.

Zeitpunkte

Security Compliance Checks sollten zu folgenden Zeitpunkten bzw. bei Eintreten folgender Ereignisse durchgeführt werden:

- für neue IT-Systeme oder relevante neue Anwendungen: nach der Implementierung (vgl. dazu auch Kap. 5.1 und Kap. 5.4)
- für bereits in Betrieb befindliche IT-Systeme oder Applikationen: nach einer bestimmten, in den Sicherheitsrichtlinien vorzugebenden Zeitspanne (z.B. jährlich) sowie bei signifikanten Änderungen.

7.1.3 Fortlaufende Überwachung der IT-Systeme (Monitoring)

Monitoring ist eine laufende Aktivität mit dem Ziel, zu überprüfen, ob das IT-System, seine Benutzer/innen und die Systemumgebung das im Informationssicherheitsplan festgelegte Sicherheitsniveau beibehalten. Dazu wird ein Plan für eine kontinuierliche Überwachung der IT-Systeme im täglichen Betrieb erstellt.

Wo technisch möglich und sinnvoll, sollte das Monitoring durch die Ermittlung von Kennzahlen unterstützt werden, die eine rasche und einfache Erkennung von Abweichungen von den Sollvorgaben ermöglichen. Solche Kennzahlen können beispielsweise die Systemverfügbarkeit, die Zahl der Hacking-Versuche über Internet oder die Wirksamkeit des Passwortmechanismus betreffen.

Alle Änderungen der potentiellen Bedrohungen, Schwachstellen, zu schützenden Werte und Sicherheitsmaßnahmen können möglicherweise signifikante Auswirkungen auf das Gesamtrisiko haben. Aus diesem Grund ist eine fortlaufende Überwachung folgender Bereiche erforderlich:

- Wert der zu schützenden Objekte:
  Sowohl die Werte von Objekten als auch, daraus resultierend, die Sicherheitsanforderungen an das Gesamtsystem können im Laufe des Lebenszyklus eines IT-Projektes oder -Systems erheblichen Änderungen unterliegen. Mögliche Gründe dafür sind eine Änderung der IT-Sicherheitsziele, neue Applikationen oder die Verarbeitung von Daten einer höheren Sicherheitsklasse auf existierenden Systemen oder Änderungen in der HW-Ausstattung.
- Bedrohungen und Schwachstellen:
  Organisatorisch oder technologisch (hier insbesondere durch neue Technologien in der Außenwelt) bedingt können sowohl die Wahrscheinlichkeit des Eintritts einer Bedrohung als auch die potentielle Schadenshöhe im Laufe der Zeit starken Änderungen unterliegen und sind daher regelmäßig zu evaluieren. Neue potentielle Schwachstellen sind so früh wie möglich zu erkennen und abzusichern.
- Sicherheitsmaßnahmen:
  Die Wirksamkeit der implementierten Sicherheitsmaßnahmen ist laufend zu überprüfen. Es ist sicherzustellen, dass sie einen angemessenen und den Vorgaben der Sicherheitsrichtlinien entsprechenden Schutz bieten. Änderungen in den Werten der bedrohten Objekte, den Bedrohungen und den Schwachstellen, aber auch durch den Einsatz neuer Technologien, können die Wirksamkeit der Sicherheitsmaßnahmen nachhaltig beeinflussen.

Durch ein kontinuierliches Monitoring soll die Leitung der Institution ein klares Bild darüber bekommen, was durch die Sicherheitsmaßnahmen erreicht wurde (Soll-/Ist-Vergleich), ob die Ergebnisse den Sicherheitsanforderungen der Institution genügen sowie über den Erfolg einzelner spezifischer Aktivitäten zur Informationssicherheit.

Werden im Rahmen des kontinuierlichen Monitoring signifikante Abweichungen des tatsächlichen Risikos von dem im Sicherheitskonzept festgelegten akzeptablen Restrisiko festgestellt, so sind entsprechende Gegenmaßnahmen zu setzen.

7.2 Change Management

Aufgabe des Change Managements ist es, neue Sicherheitsanforderungen zu erkennen, die sich aus Änderungen am IT-System ergeben. Sind signifikante Hardware- oder Softwareänderungen in einem IT-System geplant, so sind die Auswirkungen auf die Gesamtsicherheit des Systems zu untersuchen.

Es ist dafür Sorge zu tragen, dass auf alle sicherheitsrelevanten Änderungen angemessen reagiert wird. Dazu gehören zum Beispiel:

- Änderungen in der Aufgabenstellung oder in der Wichtigkeit der Aufgabe für die Institution,
- räumliche Änderungen, z.B. nach einem Umzug,
- Änderungen in der Bewertung der eingesetzten IT, der notwendigen Vertraulichkeit, Integrität oder Verfügbarkeit und
- Änderungen bei Bedrohungen oder Schwachstellen.

Alle Änderungen und die dazugehörigen Entscheidungsgrundlagen sind schriftlich zu dokumentieren.

Abhängig von der Bedeutung des Systems und dem Grad der Änderung kann eine neuerliche Risikoanalyse erforderlich werden.

7.3 Reaktion auf sicherheitsrelevante Ereignisse (Incident Handling)

Unter sicherheitsrelevanten Ereignissen sind alle Vorkommnisse zu verstehen, die Sicherheitsprobleme aufdecken oder nach sich ziehen. Dazu zählen etwa Einbruchsversuche in das System (Hacking), das Auftreten von Viren oder das Ausspähen von Passwörtern.

Auch bei Vorhandensein wirksamer Sicherheitsmaßnahmen und eines hohen Sicherheitsniveaus ist das Auftreten solcher Ereignisse nicht gänzlich zu verhindern. Jede Institution muss ein vitales Interesse daran haben, dass auf sicherheitsrelevante Ereignisse so schnell und effektiv wie möglich reagiert wird. Darüber hinaus können und sollen Informationen über derartige Vorkommnisse der Vorbeugung künftiger Schadensereignisse dienen.

Daher sind alle Mitarbeiter/innen über ihre Verantwortung bei Eintreten sicherheitsrelevanter Ereignisse, die vorgesehenen Meldewege und zu setzenden Aktionen zu unterrichten.

Incident Handling Plan

Zur Sicherstellung einer angemessenen Behandlung von sicherheitsrelevanten Ereignissen ist es empfehlenswert, detaillierte Vorgaben in Form eines "Incident Handling Planes" (IHP) auszuarbeiten und allen Mitarbeitern/innen bekannt zu machen.

Der Incident Handling Plan legt in schriftlicher Form und verbindlich fest:

- 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.

Einrichtung von CERTs

Ein CERT (Computer Emergency Response Team) ist eine Gruppe von Personen, die

- die Ursachen und Auswirkungen von sicherheitsrelevanten Vorfällen untersucht,
- Vorfälle aufzeichnet und auswertet,
- Hilfestellung bei der Behandlung von sicherheitsrelevanten Vorfällen gibt.

Ob innerhalb einer Institution ein (oder ev. auch mehrere) CERT(s) eingerichtet wird, hängt in erster Linie von der Größe dieser Institution und der erwarteten Anzahl und Schwere der Vorfälle ab. In kleineren Institutionen wird eine Behandlung und Aufzeichnung der sicherheitsrelevanten Vorfälle durch eine in der Informationssicherheitspolitik zu benennende Person - dies wird im Allgemeinen die/der IT-Sicherheitsbeauftragte sein - angemessen sein, in großen oder besonders sicherheitssensiblen Institutionen ist die Einrichtung von CERTs zu empfehlen.

Darüber hinaus besteht auch die Möglichkeit, institutionsübergreifende CERTs einzurichten, die es ermöglichen, Daten über sicherheitsrelevante Vorfälle auszutauschen und damit auf eine breitere Information, etwa über die Häufigkeit des Eintretens von Bedrohungen oder über neue Angriffe, zurückzugreifen. In diesem Fall sollten gemeinsame Protokollierungsvorgaben, Formulare, Bewertungsmethoden und Datenbankstrukturen erarbeitet werden, die den Austausch und die Auswertung von Information erleichtern.

Im Rahmen eines Public-Privat-Partnership wurde vom Bundeskanzleramt in Zusammenarbeit mit dem Zentrum für sichere Informationstechnik - Austria (A-SIT) und der ISPA (Internet Service Providers Austria) eine Plattform zur Kommunikation und Handlungsabstimmung bei sicherheitsrelevanten Vorfällen erstellt. Sie trägt den Namen CIRCA (Computer Incidents Response and Coordination Austria) und ist unter http://www.circa.at erreichbar.

8 Industrielle Sicherheit

Im Zusammenhang mit Informationssicherheit werden unter dem Begriff „Industrielle Sicherheit" Regelungen für den Umgang mit klassifizierten Informationen (das sind gemäß Informationssicherheitsgesetz EINGESCHRÄNKT, VERTRAULICH, GEHEIM, oder STRENG GEHEIM klassifizierte Dokumente) in Unternehmen bzw. in der Industrie verstanden. Diese Regelungen sehen unter anderem vor, dass die Sicherheit der betroffenen Unternehmen, Einrichtungen und Anlagen sowie ihres Personals im Rahmen einer so genannten Sicherheitsüberprüfung (Facility Clearance) überprüft wird.

Für die Teilnahme österreichischer Unternehmen an manchen Forschungsprogrammen wie zum Beispiel der Europäischen Weltraumagentur (ESA) ist die Vorlage solch einer staatlichen Bescheinigung erforderlich, wonach das Unternehmen und die Forschungseinrichtung die verlangten Standards der Geheimhaltung erfüllen (Sicherheitsunbedenklichkeitsbescheinigung).

Betroffen sind alle Unternehmen, welche Aufträge im Zusammenhang mit klassifizierten Informationen ausführen wollen bzw. sich an Ausschreibungsverfahren zu derartigen Aufträgen beteiligen wollen.

Im Rahmen eines Vertrages verpflichtet sich das Unternehmen die entsprechenden Rechtsvorschriften und internationalen Standards für die Behandlung klassifizierter Dokumente einzuhalten.

8.1 Beschreibung der generellen Anforderungen

Auf Grund der diversen rechtlichen Grundlagen müssen die Sicherheitsmaßnahmen

- alle Personen, die Zugang zu klassifizierten Informationen haben, die Träger von klassifizierten Informationen und alle Gebäude, in denen sich derartige klassifizierte Informationen und wichtige Einrichtungen befinden, umfassen;
- so ausgelegt sein, dass Personen, die aufgrund ihrer Stellung die Sicherheit von klassifizierten Informationen und wichtigen Einrichtungen, in denen klassifizierte Informationen aufbewahrt werden, gefährden könnten, erkannt und vom Zugang ausgeschlossen oder fern gehalten werden;
- verhindern, dass unbefugte Personen Zugang zu klassifizierten Informationen oder zu Einrichtungen, in denen klassifizierte Informationen aufbewahrt werden, erhalten;
- dafür sorgen, dass klassifizierte Informationen nur unter Beachtung des für alle Aspekte der Sicherheit grundlegenden Prinzips „Kenntnis nur wenn nötig" (Need-to-know Prinzip) verbreitet werden;
- die Integrität (d. h. Verhinderung von Verfälschungen, unbefugten Änderungen oder unbefugten Löschungen) und die Verfügbarkeit (d. h. keine Verweigerung des Zugangs für Personen, die ihn benötigen und dazu befugt sind) aller Informationen gewährleisten.

Alle Gebäude, Bereiche, Büros, Räume, Kommunikations- und Informationssysteme usw. in denen als klassifiziert eingestufte Informationen und/oder ihr Material aufbewahrt werden und/oder in denen damit gearbeitet wird, müssen durch geeignete Maßnahmen des Geheimschutzes gesichert werden. Die Maßnahmen des Schutzes zielen darauf ab, das Eindringen unbefugter Personen von außen zu verhindern, von Tätigkeiten illoyaler Angehöriger des Personals (Spionage von innen) abzuschrecken bzw. diese zu verhindern und aufzudecken.

Im Wesentlichen werden dafür abgesicherte Sicherheitsbereiche eingerichtet und der Zugang zu diesen kontrolliert. Für die Lagerung von klassifizierten Informationen werden Sicherheitsbehältnisse (z. B. Tresore) vorgesehen. Weiters sind Maßnahmen zum Sicht- und Abhörschutz zu treffen. Außerdem ist zu dokumentieren, wann wer welche klassifizierte Information erhält. Die Gestaltung der Maßnahmen im Einzelnen ist von der Klassifizierungsstufe abhängig.

Personen-Zertifizierung

Alle Personen, die Zugang zu Informationen haben, welche als „VERTRAULICH“ oder höher eingestuft sind, müssen einer Sicherheitsüberprüfung unterzogen werden, bevor sie Zugangsermächtigung erhalten.

8.2 Rechtlicher Hintergrund

Rechtsgrundlagen

Als Rechtsgrundlagen sind zu nennen:

- Informationssicherheitsgesetz [InfoSiG]
- Informationssicherheitsverordnung [InfoSiV]
- Sicherheitspolizeigesetz [SPG]
- Militärbefugnisgesetz [MBG]
- Verordnung des Bundesministers für Verkehr, Innovation und Technologie über die Kostenersatzpflicht für die Ausstellung einer Sicherheitsunbedenklichkeitsbescheinigung [BMVIT]
- Verordnung des Bundesministers für Landesverteidigung über die Ausstellung von Sicherheitsunbedenklichkeitsbescheinigungen [SUBV]
- Sicherheitsgebühren-Verordnung [SGV]

Informationssicherheitsgesetz [InfoSiG] und –verordnung [InfoSiV] regeln den nationalen Umgang mit klassifizierten Informationen.

Für die Personen-Überprüfung sind das Sicherheitspolizeigesetz [SPG] mit seinen Verordnungen, insbesondere die Sicherheitsgebühren-Verordnung [SGV] und die Verordnung, mit der Form und Inhalt der Sicherheitserklärung einschließlich der Zustimmungserklärung erlassen und die Sicherheitsgebühren-Verordnung geändert werden [SEV] und das Militärbefugnisgesetz [MBG] relevant.

Die Verordnungen BMVIT [BMVIT] und BMLV [SUBV] regeln die Kosten für die Ausstellung von Sicherheitsunbedenklichkeitsbescheinigungen.

Beschlüsse der ISK:

- Beschluss über die Verwendung von Sicherheitsbehältnissen für klassifizierte Dokumente [TRES]

EU-Ratsbeschlüsse:

- Beschluss des Rates vom 19. März 2001 über die Annahme der Sicherheitsvorschriften des Rates (2001/264/EG) [EU2001]
- Beschluss des Rates vom 10. Februar 2004 zur Änderung des Beschlusses 2001/264/EG über die Annahme der Sicherheitsvorschriften des Rates (2004/194/EG) [EU2004]
- Beschluss des Rates vom 20. Dezember 2005 zur Änderung des Beschlusses 2001/264/EG über die Annahme der Sicherheitsvorschriften des Rates (2005/952/EG) [EU2005]

Mit dem Ratsbeschluss 2001/246/EG [EU2001] wurde festgelegt, wie EU-Verschlusssachen in den öffentlichen Einrichtungen der Mitgliedsstaaten zu behandeln sind. Der materielle Geheimschutz wird definiert in Abschnitt IV: „Hauptziel der Maßnahmen des materiellen Geheimschutzes ist es, zu verhindern, dass Unbefugte Zugang zu EU Verschlusssachen erhalten."

Im Ratsbeschluss 2004/194/EG [EU2004] werden die Anhänge 1 (Verzeichnis der nationalen Sicherheitsbehörden) und 2 (Vergleichstabelle der nationalen Sicherheitseinstufungen) des Ratsbeschlusses EU2001 ergänzt.

Der Ratsbeschluss 2005/952/EG [EU2005] legt fest, dass die Bestimmungen des Ratsbeschlusses EU2001 auch anzuwenden sind, wenn industrielle oder andere Einrichtungen vertraglich mit Aufgaben betraut werden, bei denen EU-Verschlusssachen relevant sind.

Beschlüsse der Kommission:

- Beschluss der Kommission vom 1. Februar 2005, 2001/844/EC, ECSC, Euratom in der sich diese inhaltlich an den Ratsbeschluss anlehnen
- Beschluss der Kommission vom 2. August 2006, 2006/548/EC, ECSC, Euratom hinsichtlich industrieller Sicherheit

Beschlüsse der NATO:

- NATO Security Committee, Directive on Industrial Security, „Security Policy", AC735-D/2003-REV1, 26. Juli 2005 [NATO35]
- North Atlantic Council, C-M(2002)49, Security within the North Atlantic Treaty Organisation (NATO) mit den Subdokumenten [NATO49]
  - AC/35-D/2000 directive on Personnel Security
  - AC/35-D/2001 Directive on Physical Security
  - AC/35-D/2002 Directive on Security of Information
  - AC/35-D/2003 Directive on Industrial Security
  - AC/35-D/2004 Primary Directive on INFOSEC
  - AC/35-D/2005 INFOSEC Management Directive for CIS

Beschlüsse der Multinational Industrial Security Working Group MISWG:

- Doc. Number 1: Arrangements for the International Hand Carriage of Classified Documents, Equipment and/or Components
- Doc. Number 3: Use of Cryptographic Systems
- Doc. Number 4: Security Clauses
- Doc. Number 5: Program/Project Security Instruction
- Doc. Number 6: Procedures for the Protection of Restricted Information
- Doc. Number 7: International Visit Procedures
- Doc. Number 8: Controlled Unclassified Information Clauses
- Doc. Number 9: Security Education and Awareness
- Doc. Number 10: Transportation Plan for the Movement of Classified Material as Freight
- Doc. Number 11: Control of Security Cleared Facilities
- Doc. Number 12: Facility Security Clearance Information Sheet
- Doc. Number 13: Protection of Information Handled in it and Communication Systems
- Doc. Number 14: Contract Security Clauses
- Doc. Number 15: International Transportation by Commercial Carriers of Classified Documents and Equipment or Components as Freight
- Doc. Number 16: Guidelines for Assessing Protection and Control of Classified Information in a Multinational Non-NATO Cooperative Defence Program
- Doc. Number 17: International Hand Carriage of Classified Documents, Equipment and /of Components by Visitors
- Doc. Number 18: International Industrial Security Requirements Guidance Annex
- Doc. Number 19: Personal Security Clearance Information Sheet
- Doc. Number 20: International Transfer of Material Classified Restricted by Express Commercial Couriers
- Doc. Number 21: Role of the Facility Security Officer

8.3 Ausstellung einer Sicherheitsunbedenklichkeitsbescheinigung

8.3.1 Ablauf

- Anträge auf Ausstellung einer Sicherheitsunbedenklichkeitsbescheinigung sind beim zuständigen Ministerium einzubringen: Dabei handelt es sich um jenes Ministerium in dessen Zuständigkeitsbereich die betreffende industrielle Tätigkeit oder Forschungstätigkeit laut Bundesministeriengesetz fällt.
- Das Unternehmen verpflichtet sich gegenüber der Republik Österreich vertraglich zur Einhaltung der einschlägigen gesetzlichen Bestimmungen. Alle Personen, die im Unternehmen mit klassifizierten Informationen befasst werden sollen, sind gem. § 6 InfoSiV zu unterweisen. Die Nachweise der durchgeführten Unterweisungen sind an das zuständige Ministerium zu übermitteln.
- Personelle Sicherheitsüberprüfung (Personenzertifizierung): Alle Personen, die im Unternehmen Informationen erhalten sollen, welche als „VERTRAULICH“ oder höher (bzw. in einer äquivalenten ausländischen Klassifizierungsstufe eingestuft sind), werden einer Sicherheitsüberprüfung unterzogen. Das Unternehmen beantragt eine Überprüfung für jede/n betroffene/n Mitarbeiter/in. Die Sicherheitsüberprüfung wird gemäß §§ 55 bis 55 b [SPG] vom BMI oder im Falle der Zuständigkeit des BMLV die einer Sicherheitsüberprüfung analoge Verlässlichkeitsprüfung nach den §§ 23 und 24 [MBG] A.2 vom BMLV durchgeführt.

- Materielle Sicherheitsüberprüfung
  - Erstellen eines Sicherheitskonzeptes (inkl. der „Systemspezifischen Sicherheitsanforderungen“ [SSRS] für IT-Anwendungen) durch das Unternehmen
  - Umsetzen des Sicherheitskonzeptes und Dokumentation derselben (für IT-Anwendungen „SecOPs“ [SECOPS]) durch das Unternehmen
  - Überprüfung durch das BMI bzw. BMLV
- Ausstellung der Sicherheitsunbedenklichkeitsbescheinigung durch die/den Leiter/in der ISK bei zivilen Projekten bzw. die/den Leiter/in des Abwehramtes bei militärisch klassifizierten Projekten. Diese Bestätigung über die erfolgreiche Sicherheitsüberprüfung bezieht sich nur auf das konkrete Projekt, für welches die Überprüfung beantragt wurde und gilt für den angegebenen Zeitraum.
- In der Folge über die komplette Projektdauer: regelmäßige Überprüfung durch das zuständige Ministerium, Kommunikation mit dem ISB (z.B. bei Änderungen, Besuchsverfahren)

8.3.2 Verantwortlichkeiten und Kontakte

Antragstellung

Der Antrag auf Ausstellung einer Sicherheitsunbedenklichkeitsbescheinigung ist beim zuständigen Ministerium einzubringen. Dabei handelt es sich um jenes Ministerium in dessen Zuständigkeitsbereich der Auftragsgegenstand fällt. Unter http://www.austria.gv.at/ ist eine Liste der Ministerien zu finden. Bei Unklarheiten in der Zuständigkeit wird durch das ISB die Federführung festgelegt.

Durchführung der Sicherheitsüberprüfung und Ausstellung der Sicherheitsunbedenklichkeitsbescheinigung

- Büro der Informationssicherheitskommission (ISB), Bundeskanzleramt, Ballhausplatz 2, 1014 Wien
- Bundesministerium für Inneres, BVT/3, Herrengasse 7, Postfach 100, 1014 Wien
- Bundesministerium für Landesverteidigung, Abwehramt, Postfach 888, 1035 Wien

Durchführung der personellen Sicherheitsüberprüfung, Verlässlichkeitsprüfung

- Bundesministerium für Inneres, BVT, Herrengasse 7, Postfach 100, 1014 Wien
- Bundesministerium für Landesverteidigung, Abwehramt, Postfach 888, 1035 Wien

Verantwortlichkeiten im Unternehmen

Im Unternehmen sind eine Stelle (SOA - System Operational Authority) und eine verantwortliche Person (Informationssicherheitsbeauftragter) zu definieren, die für alle Sicherheitsmaßnahmen und für die Erstellung und Einhaltung der SSRS und der SecOPs verantwortlich sind.

Geheimhaltungsgrade und Kennzeichnungen

Österreich:	▫ STRENG GEHEIM (SG)	▫ GEHEIM (G)	▫ VERTRAULICH (V)	▫ EINGESCHRÄNKT (E)
EU Einstufung:	▫ TRES SECRET UE ▫ EU TOP SECRET	▫ SECRET UE	▫ CONFIDENTIEL UE	▫ RESTREINT UE
NATO:	▫ Cosmic Top Secret	▫ NATO Secret	▫ NATO Confidential	▫ NATO Restricted

Tabelle 3: Geheimhaltungsgrade und Kennzeichnung

Für einen kompletten Vergleich nationaler Sicherheitseinstufungen der EU-Mitgliedsstaaten siehe Ratsbeschluss 2001/264/EG [EU2004].

Anhang A:

A.1 Literatur

[BS 7799-1]	British Standards Institute: "Code of practice for information security management", 1999 (entspricht [ISO/IEC 17799])
[BS 7799-2]	British Standards Institute: "Specification for information security management systems", 2002
[BSI 7105]	Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn: "IT-Sicherheitshandbuch", BSI 7105
[BSI 100-1]	Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn: "Managementsysteme für Informationssicherheit (ISMS)"
[BSI 100-2]	Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn: "IT-Grundschutz-Vorgehensweise"
[BSI 100-3]	Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn: "Risikoanalyse auf der Basis von IT-Grundschutz"
[BSI-1]	Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn: Gefährdungskatalog, www.bsi.de
[BSI-2]	Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn: Maßnahmenkataloge, www.bsi.de
[KFall]	Bundeskanzleramt: "Katastrophenvorsorge- und Ausfallssicherheitsüberlegungen im IT-Bereich", vom Oktober 2002 (nicht öffentlich)
[OECD-02]	Organisation for Economic Co-operation and Development (OECD): "Guidelines for the Security of Information Systems and Networks", 2002

Tabelle 4: Literaturverweise

A.2 Gesetzestexte

Die zitierten Gesetzestexte können online über das Rechtsinformationssystem des Bundes unter folgender URL abgerufen werden: http://www.ris.bka.gv.at.

Die Bundesgesetzblätter sind bei der Wiener Zeitung Digitale Publikationen GmbH (vormals Österreichische Staatsdruckerei - Wiener Zeitung), die Landesgesetzblätter bei den Ämtern der Landesregierungen erhältlich.

[DSG 2000]	"Bundesgesetz über den Schutz personenbezogener Daten" (Datenschutzgesetz 2000 - DSG 2000), BGBl. I Nr. 165/1999 i.d.g.F.
[InfoSiG]	Bundesgesetz über die Umsetzung völkerrechtlicher Verpflichtungen zur sicheren Verwendung von Informationen (Informationssicherheitsgesetz, InfoSiG), BGBl. I Nr. 23/2002 i.d.g.F.
[InfoSiV]	Informationssicherheitsverordnung (InfoSiV), BGBl. I Nr. 23/2002
[BMVIT]	Verordnung des Bundesministers für Verkehr, Innovation und Technologie über die Kostenersatzpflicht für die Ausstellung einer Sicherheitsunbedenklichkeitsbescheinigung, BGBl. II, Nr. 393/2004
[EU2001]	Beschluss des Rates vom 19. März 2001 über die Annahme der Sicherheitsvorschriften des Rates (2001/264/EG), ABl. L 101 vom 11.4.2001, S. 1
[EU2004]	Beschluss des Rates vom 10. Februar 2004 zur Änderung des Beschlusses 2001/264/EG über die Annahme der Sicherheitsvorschriften des Rates (2004/194/EG), ABl. L 63 vom 28.2.2004, S. 48
[EU2005]	Beschluss des Rates vom 20. Dezember 2005 zur Änderung des Beschlusses 2001/264/EG über die Annahme der Sicherheitsvorschriften des Rates (2005/952/EG), ABl. L 346 vom 29.12.2005, S. 18
[MBG]	Bundesgesetz, mit dem ein Bundesgesetz über Aufgaben und Befugnisse im Rahmen der militärischen Landesverteidigung (Militärbefugnisgesetz - MBG) eingeführt sowie das Sperrgebietsgesetz 1995 geändert werden, BGBl. I Nr. 86/2000 in der Fassung BGBl. I Nr. 115/2006
[NATO35]	Nato Security Committee, Directive on Industrial Security, „Security Policy“, AC735-D/2003-REV1, 26. Juli 2005
[NATO49]	North Atlantic Council, C-M(2002)49, Security within the North Atlantic Treaty Organisation (NATO) mit den Subdokumenten
[SPG]	Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz - SPG), BGBl. I Nr. 566/1991 in der Fassung BGBl. I. Nr. 56/2006
[SGV]	Verordnung des Bundesministers für Inneres über die Höhe der Gebühren für Sicherheitsüberprüfungen, Sicherheitsgebühren-Verordnung 389/1996 idF. 399/2001
[SEV]	Verordnung des Bundesministeriums für Inneres, mit der Form und Inhalt der Sicherheitserklärung einschließlich der Zustimmungserklärung erlassen und die Sicherheitsgebühren-Verordnung geändert werden BGBl 114/2000

[SUBV]	Verordnung des Bundesministers für Landesverteidigung über die Ausstellung von Sicherheitsunbedenklichkeitsbescheinigungen (SUBV), BGBl. II Nr. 195/2006
[KO2005]	Beschluss der Kommission vom 1. Februar 2005, 2001/844/EC, ECSC, Euratom
[KO2006]	Beschluss der Kommission vom 2. August 2006, 2006/548/EC, ECSC, Euratom
[SSRS]	Infosec Office, Februar 2003, Guidelines for the development of Security requirements
[SECOPS]	Infosec Office, Februar 2003, Guidelines for the structure and content of Security Operation Procedures (SecOPs)
[TRES]	Beschluss der ISK über die Verwendung von Sicherheitsbehältnissen für klassifizierte Dokumente

Tabelle 5: Gesetzestexte

A.3 Glossar

Akkreditierung (accreditation)	Verfahren, das ein IT-System zum Betrieb in einer speziellen Umgebung freigibt
Applikation (application)	(auch: IT-Applikation, Anwendung, IT-Anwendung) Einsatz eines IT-Systems zur Erfüllung von Aufgaben, die in einem eingegrenzten fachlichen Bereich liegen und durch gemeinsame Merkmale ausgezeichnet sind
Auswirkung (impact)	Folgen eines unerwünschten Vorfalls
Authentizität (authenticity)	Eigenschaft, die sicherstellt, dass die von einem Subjekt oder einer Ressource behauptete Identität zutrifft. Authentizität betrifft Entitäten wie Benutzer/innen, Prozesse, Systeme und Informationen.
Authentisierung (authentication)	Nachweis der angegebenen Identität
Bedrohung (threat)	möglicher Anlass für ein unerwünschtes Ereignis, das zu einem Schaden des Systems oder der Organisation führen kann
bedrohtes Objekt (asset)	(auch als "Wert" bezeichnet) alles, was für die Organisation schutzbedürftig ist
CERT	Computer Emergency Response Team; Gruppe von Personen, die die Ursachen und Auswirkungen von sicherheitsrelevanten Vorfällen aufzeichnet und analysiert und Hilfestellung bei ihrer Behandlung gibt.
Entität (entity)	genau abgrenzbares Exemplar von Personen, Systemen, Begriffen etc.
Evaluation (evaluation)	Prüfung und Bewertung eines IT-Systems oder eines IT-Produktes anhand definierter Evaluationskriterien (z.B. ITSEC, Common Criteria)
Grundschutz (baseline security)	Schutzmaßnahmen, die ein angemessenes Sicherheitsniveau für IT-Systeme mit mittlerem Schutzbedarf gewährleisten
Grundschutzanalyse	Risikoanalyse für IT-Systeme, die von einer pauschalisierten Gefährdungslage ausgeht; Ergebnis ist eine Liste von umzusetzenden Standardsicherheitsmaßnahmen
Identifikation (identification)	Bestimmung der Identität eines Subjektes bzw. Objektes
Informationssicherheit (information security)	Sammelbegriff aller Aspekte zum Schutz von Information vor Verlust, unbefugter Veränderung und unbefugter Kenntnisnahme; umfasst sowohl elektronisch gespeicherte und verarbeitete Information als auch Information in verbaler oder schriftlicher Form
Integrität (integrity)	Unverfälschtheit und Korrektheit von Daten bzw. Systemen
IT-Sicherheit (IT security)	alle Aspekte in Verbindung mit der Definition, Erreichung und Aufrechterhaltung von Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit, Authentizität und Zuverlässigkeit in einem IT-System

IT-Sicherheitspolitik, organisationsweite (IT security policy, corporate)	Leitlinien und Vorgaben, die grundlegende Ziele, Strategien, Verantwortlichkeiten und Methoden für die Gewährleistung der IT-Sicherheit in einer Organisation festlegen
IT-Sicherheitskonzept (IT security concept)	Summe von (geplanten und realisierten) Maßnahmen verschiedener Art, die erst in ihrer Kombination die gewünschte Schutzwirkung ergeben; die Erstellung eines IT-Sicherheitskonzeptes umfasst Festlegung von Maßnahmen, Restrisikoakzeptanz und Erstellung von IT-Systemsicherheitspolitiken und eines Sicherheitsplanes
IT-System (IT system)	Kombination von Hard- und Software mit einem bestimmten Zweck und einer spezifischen Betriebsumgebung
IT-Systemsicherheitspolitik (IT system security policy)	Leitlinien, Regeln und Praktiken, die vorschreiben, in welcher Weise sensitive Informationen und Betriebsmittel innerhalb eines bestimmten IT-Systems behandelt, geschützt und verteilt werden
Objekt (object)	passive Entität, die Informationen enthält oder empfängt
Objekt, bedrohtes	s. bedrohtes Objekt
Restrisiko (residual risk)	Risiko, das nach der Umsetzung von Schutzmaßnahmen verbleibt
Risiko (risk)	Maß für die Gefährdung, die von einer Bedrohung ausgeht
Risikoanalyse (risk analysis)	Prozess, der die Sicherheitsrisiken identifiziert, ihre Größenordnung bestimmt und die Bereiche identifiziert, die Schutzmaßnahmen erfordern
Risikomanagement (risk management)	Methodisches Vorgehen zur Erkennung, Bewertung, Handhabung und Reduktion von Risiken
Schaden (damage)	Minderung des Wertes eines Objektes bei Eintritt einer Bedrohung
Schutzbedarf	Maß für die möglichen Schäden, die beim IT-Einsatz entstehen können, und für die Notwendigkeit, den Eintritt solcher Schäden zu verhindern
Schutzbedarfsfeststellung (high level risk analysis)	Ermittlung des Schutzbedarfes für ein IT-System; im Fall eines kombinierten Risikoanalyse-Ansatzes werden etwa die Schutzbedarfskategorien "niedrig bis mittel" und "hoch bis sehr hoch" unterschieden
Schutzmaßnahme (safeguard)	Verfahrensweise oder Mechanismus zur Verringerung von Risiken
Schwachstelle (vulnerability)	Sicherheitsschwäche eines oder mehrerer Objekte, die durch eine Bedrohung ausgenutzt werden kann
Sicherheitsmanagement (security management)	kontinuierlicher Prozess zur Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit, Authentizität und Zuverlässigkeit von IT-Systemen

Sicherheitsmaßnahme (safeguard)	s. Schutzmaßnahme
Subjekt (subject)	aktive Entität, normalerweise in der Form einer Person, eines Prozesses oder von Geräten
Verfügbarkeit (availability)	Eigenschaft, auf Verlangen einer berechtigten Entität zugreifbar und benutzbar zu sein
Vertraulichkeit (confidentiality)	Eigenschaft, dass Information nur befugten Entitäten in der zulässigen Weise zugänglich ist
Vertrauenswürdigkeit (assurance)	Eigenschaft, die das Maß an Vertrauen ausdrückt, das man in die Sicherheit eines IT-Systems haben kann
Virus (virus)	(auch: Computer-Virus) Nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom/von der Anwender/in nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt
Zertifizierung (certification)	Formale Erklärung, die die Ergebnisse einer Evaluierung und die ordnungsgemäße Anwendung der benutzten Evaluationskriterien bestätigt
Zugriff (access)	Vorgang, der einem Nutzer Daten, Programme oder Ressourcen eines IT-Systems zugänglich macht. Dieser Vorgang kann beispielsweise lesend, schreibend oder ausführend erfolgen.
Zurechenbarkeit (accountability)	Eigenschaft, die sicherstellt, dass die Aktivitäten einer Entität eindeutig auf diese Entität zurückgeführt werden können
Zutritt (access)	Betreten von Bereichen (z.B. Räumen), in denen Teile des IT-Systems aufgestellt sind, durch Personen
Zuverlässigkeit (reliability)	Eigenschaft eines gleich bleibenden, beabsichtigten Verhaltens und Ergebnisses

Tabelle 6: Glossar

Österreichisches Informationssicherheitshandbuch

Teil 2: Informationssicherheitsmaßnahmen

Version 2.3
April 2007

BUNDESKANZLERAMT ÖSTERREICH

1 Bauliche und infrastrukturelle Maßnahmen

Die in diesem Abschnitt beschriebenen Maßnahmen dienen dem Schutz von Informationssystemen 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

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

INF 1.1 Geeignete Standortauswahl

Relevanz: Management; Umsetzung/Wartung;

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 Informationssicherheit 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 und CRT-Bildschirmen 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.
- Streunende Haustiere können Fehlalarme von Bewegungsmeldern verursachen.

INF 1.2 Anordnung schützenswerter Gebäudeteile

Relevanz: Management; Umsetzung/Wartung;

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

Relevanz: Umsetzung/Wartung; Anwender/innen;

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 Mitarbeiterinnen/Mitarbeitern ist durch Regelungen bekannt zu geben, welche Maßnahmen zum Einbruchschutz beachtet werden müssen.

In Anhang A sind relevante ÖNORMEN zum Einbruchschutz angeführt.

INF 1.4 Zutrittskontrolle

Relevanz: Management; Umsetzung/Wartung;

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- und 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/innen, Operator, Fachabteilungsmitarbeiter/innen, Kundinnen/Kunden, Angehörige von Lieferfirmen etc.) Zutritt zu 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 und Datenträgern den unerlaubten Zugriff von Wartungstechnikerinnen/Wartungstechnikern auf die Datenträger.
- *Bestimmung einer/eines Verantwortlichen für Zutrittskontrolle:*
  Diese/r vergibt die Zutrittsberechtigungen an die einzelnen Personen entsprechend den in 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. Solche Zeitabhängigkeiten können etwa sein: Zutritt nur während der Arbeitszeit oder befristeter Zutritt bis zu einem fixierten Datum.
- *Festlegung der Zutrittskontrollmedien:*
  Es ist festzulegen, ob die Identifikation bzw. die Authentisierung durch Überwachungspersonal (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 Randbedingungen 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 der/des Einzelnen.
- *Behandlung von Ausnahmesituationen:*
  Es ist u.a. sicherzustellen, dass im Brandfall die Mitarbeiter/innen schnellstmöglich die gefährdeten Zonen verlassen können.

Weiters sind folgende Fragen zu klären:

- Sind beim Betreten und/oder Verlassen eines geschützten Bereiches Vereinzelungsmechanismen (Drehtüren, Schleusen, ...) notwendig?
- Welche Maßnahmen sind bei unautorisierten Zutrittsversuchen zu setzen?
- Ist eine Nullsummenprüfung (Anmerkung - Nullsummenprüfung: Feststellung der Anzahl der im geschützten Bereich befindlichen Personen durch Vergleich der Zu- und Abgänge. Voraussetzung für eine Nullsummenprüfung ist die Installation von Vereinzelungsmechanismen.) 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 einer Mitarbeiterin bzw. 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
- Erweiterungen des sicherheitsrelevanten Bereiches
- schlechter Benutzerakzeptanz:
  Die Akzeptanz durch die Benutzer/innen ist ein entscheidendes Kriterium. Mängel im Zutrittskontrollsystem (häufige Fehlalarme, Ausfälle, Wartezeiten, zu restriktive Handhabung, überflüssige bürokratische Abläufe) können dazu führen, dass auch grundsätzlich sicherheitsbewusste Mitarbeiter/innen bereit sind, die Regeln zu verletzen.

Mit der Standard- und Muster-Verordnung 2000 (StMV), BGBl. II Nr. 201/2000 i.d.g.F. wurde eine neue Musteranwendung "MA002 Zutrittskontrollsysteme" geschaffen (s. Anhang C.2 Musteranwendung MA002 Zutrittskontrollsysteme), die die Meldung beim Datenverarbeitungsregister erleichtert und daher für die Anwenderin bzw. den Anwender hilfreich sein kann.

INF 1.5 Verwaltung von Zutrittskontrollmedien

Relevanz: Umsetzung/Wartung;

Für alle Schlüssel eines Gebäudes ist ein Schließplan zu fertigen. Die Herstellung, Aufbewahrung, Verwaltung und Ausgabe von Schlüsseln ist zentral zu regeln. Reserveschlüssel sind vorzuhalten und gesichert aufzubewahren.

Zu beachten ist:

- Ist eine Schließanlage vorhanden, so sind für schutzbedürftige Bereiche eigene Schließgruppen zu bilden, ggf. einzelne Räume aus der Schließgruppe herauszunehmen und mit Einzelschließung zu versehen.
- Nicht ausgegebene Schlüssel und die Reserveschlüssel sind gegen unbefugten Zugriff geschützt aufzubewahren.
- Die Ausgabe der Schlüssel erfolgt gegen Quittung und ist zu dokumentieren.
- Es sind Vorkehrungen zu treffen, wie bei Verlust einzelner Schlüssel zu reagieren ist (Meldung, Ersatz, Kostenerstattung, Austausch des Schlosses, Austausch von Schließgruppen etc.).
- Bei Zuständigkeitsänderungen von Mitarbeiterinnen/Mitarbeitern sind deren Schließberechtigungen zu prüfen und Schlüssel gegebenenfalls einzuziehen.
- Beim Ausscheiden von Mitarbeiterinnen/Mitarbeitern sind alle Schlüssel einzuziehen (Aufnahme der Schlüsselverwaltung in den Laufzettel).
- Schlösser und Schlüssel zu besonders schutzbedürftigen Bereichen (zu denen nur sehr wenige Schlüssel ausgegeben werden sollten) können bei Bedarf getauscht werden, um so illegal nachgefertigten Schlüsseln die Funktion zu nehmen.
- Abhängig von der Sensibilität des zu schützenden Bereiches können auch gesperrte Schließsysteme zum Einsatz kommen, die die Anfertigung eines Schlüssels nur unter Vorliegen definierter Bedingungen (etwa schriftliche Zustimmung einer/eines Verantwortlichen) erlauben.

Das Gleiche gilt sinngemäß auch für alle anderen Zutrittskontrollmedien wie Magnetstreifen- oder Chipkarten, bzw. so genannte Multifunktionschipkarten.

INF 1.6 Portierdienst

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

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 einer Besucherin bzw. eines Besuchers bei der/dem Besuchten Rückfrage.
- Die Besucherin bzw. der Besucher wird zu der/dem Besuchten begleitet oder am Eingang abgeholt.
- Dem Portier müssen die Mitarbeiter/innen bekannt sein. Scheidet ein/e Mitarbeiter/in aus, ist auch der Portier zu unterrichten, ab wann dieser Mitarbeiterin bzw. 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.

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 1.7 Einrichtung einer Postübernahmestelle

Relevanz: Umsetzung/Wartung; Anwender/innen;

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

INF 1.8 Perimeterschutz

Relevanz: Umsetzung/Wartung;

Sofern es die Gegebenheiten und die Infrastruktur es zulassen sollten bereits auf dem Grundstück der Organisation zusätzliche Sicherheitseinrichtungen installiert werden, um äußeren Gefährdungen entgegenzuwirken.

Je nach Art und Topologie der Infrastruktur bzw. des Grundstückes können folgende Vorkehrungen sinnvoll sein:

- *Einfriedung des Grundstückes*
  z.B. Zaunanlage, Schutzmauer
- *Freiland Sicherungsmaßnahmen*
  z.B. entsprechende Geländegestaltung, geeignete Beleuchtung, Detektionssensorik, Schutz durch Bewachungsunternehmen
- *äußere Zutrittskontrollmechanismen*
  z.B. Videoüberwachung, Personen- und/oder Fahrzeugschleusen

Entscheidend ist, dass der Perimeterschutz in ein stimmiges Gesamtschutzkonzept eingebettet ist, in dem die Verhältnismäßigkeiten der einzelnen Schutzmaßnahmen aufeinander abgestimmt sind.

1.2 Brandschutz

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

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

Grundsätzlich ist davon auszugehen, dass die Arbeitgeber/innen und Arbeitnehmer/innen alle Maßnahmen zu ergreifen haben, um das Risiko einer Brandentstehung zu minimieren.

INF 2.1 Einhaltung von Brandschutzvorschriften und Auflagen

Relevanz: Management;

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

Brandverhütungsstellen und/oder Brandschutzexpertinnen/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 Arbeitnehmerschutzes und die Arbeitsstättenverordnung bei der Errichtung und beim Betrieb zu beachten, insbesondere

- Bundes-Bedienstetenschutzgesetz (B-BSG), BGBl. Nr. 70/1999 i.d.g.F.
- ArbeitnehmerInnenschutzgesetz (AschG), BGBl. Nr. 450/1994 i.d.g.F.

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

Relevanz: Umsetzung/Wartung;

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, Gardinen und dergleichen.

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 oder Räumen mit erhöhter Brandlast untergebracht sein.

INF 2.3 Organisation Brandschutz

Relevanz: Management;

Brandschutz umfasst sowohl präventive Maßnahmen, die die Möglichkeit einer Brandentstehung minimieren sollen, als auch Maßnahmen zur Brandbekämpfung und Evakuierung.

Präventive Maßnahmen können sowohl technischer (z.B. Ersatz leicht entzündlicher Arbeitsstoffe) als auch organisatorischer Natur sein. Organisatorische Maßnahmen umfassen personenbezogene Unterweisungen (keine Zigaretten in den Papierkorb, keine Verwendung von Heizstrahlern, Ausschalten von Kaffeemaschinen bei Dienstende, ...) sowie die Erstellung einer Brandschutzordnung.

Die Brandschutzordnung ist im Falle von erhöhtem Brandschutz zu erstellen und umfasst die zur Brandverhütung erforderlichen technischen und organisatorischen Vorkehrungen und Maßnahmen. Sie ist allen Bediensteten *jährlich einmal nachweislich* zur Kenntnis zu bringen.

Maßnahmen zur Brandbekämpfung und Evakuierung beinhalten u.a.

- Bestellung von Brandschutzbeauftragten
- Unterweisung der Arbeitnehmer/innen über die Verwendung der Feuerlöscheinrichtungen
- Ausarbeitung eines Evakuierungsplanes
- regelmäßige Brandschutzübungen

INF 2.4 Brandabschottung von Trassen

Relevanz: Umsetzung/Wartung;

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 (wieder zu verschließen). Um die Nachinstallation zu erleichtern, können geeignete Materialien verwendet werden. Entsprechende Richtlinien und Normen (etwa ÖNORM B 3836 und B 3850, siehe Anhang A) sind dabei zu beachten.

Brandabschottungen sind bautechnische Maßnahmen, die einen Durchbruch durch einen Brandabschnitt über eine bestimmte Zeitdauer gegen Durchtritt eines Brandes abdichten (z.B. bei Leitungs- oder Kabeldurchführungen).

Es sind hier verschiedene Systeme wie z.B. Brandschutzziegel, Brandschutzkissen oder Spachtelmassen am Markt. Wichtig ist neben einer Zulassung des Systems auch eine genaue Einhaltung der Verarbeitungsanleitungen.

Die Nichtabschottung von nachträglichen Verkabelungen ist ein immer wieder anzutreffender Schwachpunkt von baulichem Brandschutz.

Die angeführten Themenbereiche finden u.a. in den jeweiligen Bauordnungen der Länder, den Arbeitnehmerschutzvorschriften und in den behördlichen Vorschreibungen und Genehmigungen ihren Niederschlag.

Bei der Trassenplanung sollte die für den Brandschutz verantwortliche Person hinzugezogen werden.

INF 2.5 Verwendung von Brandschutztüren und Sicherheitstüren

Relevanz: Umsetzung/Wartung;

Brandschutztüren sind Brandschutzabschlüsse, welche hinsichtlich ihrer Brandwiderstandsdauer der ÖNORM B 3850 entsprechen müssen.

Im Regelfall ist bei der Bildung eines Brandabschnittes bezüglich der Tür eine geringere Brandwiderstandsklasse gefordert als bei der Brandwand (meistens F90 für Wände und T30 für Türen).

Brandschutztüren auf Verkehrswegen sind bei Vorhandensein einer Brandmeldeanlage an diese anzuschließen, um ein Aufkeilen zu verhindern. Ansonsten sollten bei solchen Türen Feststellanlagen mit oder ohne eigene Branderkennung (Brandmelder) installiert werden.

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 und Auflagen) besonders bei schutzbedürftigen Räumen wie Serverraum, Beleg- oder Datenträgerarchiv vorzusehen.

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 und Anschluss an die Brandmeldeanlage, der im Alarmfall aktiviert wird, eingesetzt werden.

INF 2.6 Brandmeldeanlagen

Relevanz: Umsetzung/Wartung;

Brandmeldeanlagen (BMA) dienen zur Überwachung eines bestimmten, besonders gefährdeten Bereiches oder eines gesamten Gebäudes. Derartige Brandmeldeanlagen können mit einer TUS-Leitung (Tonfrequentes Übertragungssystem) 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 6 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 mit einem TUS-Anschluss müssen, je nach Größe des Überwachungsbereiches, bis spätestens 2010 umgebaut werden und eine Interventionsschaltung aufweisen.

Derartige Anlagen werden von der Behörde vorgeschrieben und sind nach der TRVB S 123 (Brandmeldeanlagen) und TRVB S 114 (Anschaltebedingungen von Brandmeldeanlagen an öffentliche Feuerwehren) zu errichten. Sie sind jährlich durch eine Wartungsfirma und alle 2 Jahre durch eine autorisierte Prüfstelle zu überprüfen.

INF 2.7 Brandmelder

Relevanz: Umsetzung/Wartung;

Brandmelder dienen zur Früherkennung von Brandgefahren und werden in automatische und nichtautomatische Melder unterschieden, welche an einer Brandmeldeanlage hängen oder als Einzelmelder fungieren.

Bei automatischen Brandmeldern unterscheidet man:

Ionisationsrauchmelder
Bei Ionisationsrauchmeldern erfolgt die Branderkennung durch die Änderung des Stromflusses in der Ionisationskammer. Dieser Stromfluss wird durch Ionisation der Luft in der Messkammer erzeugt. Dringen nun Rauchpartikel, welche Träger der ionisierten Luftmoleküle sind, in die Kammer ein, ändert sich der Stromfluss.

Streulichtmelder
Die Erkennungsgröße ist bei diesem Melder die Streuung eines definierten Lichtstrahles durch eindringenden Rauch.

Wärmemelder (Maximal- oder Differentialmelder)
Als Kriterium wird entweder eine definierte Maximaltemperatur bzw. ein Temperaturanstieg herangezogen.

Flammenmelder
Bei Flammenmeldern erfolgt die Branderkennung durch die von Bränden ausgehende Strahlung.

Sie können auch bei starken Luftbewegungen eingesetzt werden und haben eine große Überwachungsfläche.

Nichtautomatische Brandmelder:

Druckknopfmelder
Durch Drücken des Melders wird die Brandmeldung über die Brandmeldeanlage direkt - ohne Verzögerung - an die Feuerwehr weitergeleitet.

Bei der Auswahl der Brandmelder sind folgende Kriterien zu beachten

- Art des Brandverlaufes
- Rauchentwicklung
- Rascher Temperaturanstieg
- Täuschungsanfälligkeit (z.B. Teeküchen - Aerosolbildung)
- Raumhöhen
- Überwachungsflächen

INF 2.8 Handfeuerlöscher (Mittel der Ersten und Erweiterten Löschhilfe)

Relevanz: Umsetzung/Wartung;

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

Diese Sofortbekämpfung ist nur möglich, wenn entsprechende Handfeuerlöscher in der jeweils geeigneten Brandklasse (ÖNORM EN 2:1993 02 01) in ausreichender Zahl und Größe im Gebäude zur Verfügung stehen. Dabei ist die räumliche Nähe zu schützenswerten Bereichen und Räumen wie Serverraum, Raum mit technischer Infrastruktur oder Belegarchiv anzustreben.

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

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 haben sich über die Standorte der nächsten Feuerlöscher zu informieren.
- Bei entsprechenden Brandschutzübungen sind die Mitarbeiter/innen in der Handhabung der Handfeuerlöscher zu unterweisen.

INF 2.9 Löschanlagen

Relevanz: Management; Umsetzung/Wartung;

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

der Behörde bei Vorlage einer erhöhten Brandgefährdung vorgeschrieben, um Entstehungsbrände effizient zu bekämpfen bzw. eine Ausbreitung zu unterbinden.

Sprinkleranlagen
Sprinkleranlagen sind automatisch wirkende Löschanlagen mit dem Löschmittel Wasser. Die Auslösung der Anlage erfolgt durch thermische Zerstörung der Sprinklerkopfabschlüsse (im Normalfall alkoholgefüllte Glasviolen). Dadurch wird der Austritt von Wasser durch den Sprinklerkopf freigegeben.

Bei der Auslegung der Anlage (Löschwasserleistung, Wirkfläche und Löschwasserbevorratung) ist die Brandbelastung des jeweils betroffenen Bereiches zu berücksichtigen.

CO2-Löschanlagen
CO2-Löschanlagen sind Gaslöschanlagen mit dem Löschmittel CO2. Bei der Planung ist neben der brandschutztechnisch richtigen Auslegung die erstickende Wirkung des CO2 als wesentlicher Faktor zu berücksichtigen. Es muss daher nach Branderkennung eine sofortige Alarmierung der betroffenen Personen und eine Schließung des Flutungsbereiches erfolgen. Die Einleitung des CO2 darf erst nach ausreichender Verzögerung zum Zwecke des Verlassens des Bereiches erfolgen. Die Auslösung des Löschmittels muss händisch unterbrechbar sein.

Halonlöschanlagen
Halonlöschanlagen sind Gaslöschanlagen mit dem Löschmittel Halon 1301. Bezüglich der Personengefährdung ist die Anlage nicht so kritisch wie eine CO2-Löschanlage anzusehen, da noch immer eine atembare Sauerstoffkonzentration vorliegt.

Anmerkung: Diese dürfen aufgrund des Halonverbotsgesetzes (HalonV), BGBl. Nr. 576/1990 i.d.g.F. nicht mehr in Verwendung stehen und sollten seit Ende 1999 durch alternative Löschmittel ersetzt sein. Auskunft darüber gibt die Halonbank-Verordnung (HalonbankV), BGBl. II Nr. 77/2000 i.d.g.F.

Schaumlöschanlagen
Schaumlöschanlagen sind Löschanlagen mit dem Löschmittel Schaum, welche ähnlich wie Sprinkleranlagen funktionieren.

INF 2.10 Brandschutzbegehungen

Relevanz: Umsetzung/Wartung; Anwender/innen;

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 wiederhergerichtet.

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 2.11 Rauchverbot

Relevanz: Management;

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.

INF 2.12 Rauchschutzvorkehrungen

Relevanz: Umsetzung/Wartung;

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

In diesem Sinne ist zu gewährleisten, dass

- rauchdichte Brandschutztüren verwendet werden (vgl. INF 2.5)
- Rauchschutztüren verwendet werden, die ggf. bei Rauchentwicklung selbsttätig geschlossen werden und die Rauchausbreitung verhindern
- Lüftungsanlage eine Ablüftung von Rauch vornehmen kann
- Lüftungs- und Klimaanlage selbsttätig auf Rauchentwicklung reagieren

1.3 Stromversorgung, Maßnahmen gegen elektrische und elektromagnetische Risiken

Relevanz: Management; Umsetzung/Wartung;

INF 3.1 Angepasste Aufteilung der Stromkreise

Relevanz: Umsetzung/Wartung;

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 etc. erforderlich werden.

INF 3.2 Not-Aus-Schalter

Relevanz: Umsetzung/Wartung;

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 nach Möglichkeit vorzusehen. Mit Betätigung des Not-Aus-Schalters wird dem Brand eine wesentliche Energiequelle genommen, was bei kleinen Bränden zu deren Verlöschen führen kann. Zumindest ist aber die Gefahr durch elektrische Spannungen beim Löschen des Feuers beseitigt.

Zu beachten ist, dass lokale unterbrechungsfreie Stromversorgungen (USV) nach Ausschalten der externen Stromversorgung die Stromversorgung selbsttätig übernehmen und die angeschlossenen Geräte unter Spannung bleiben. Daher ist bei der Installation eines Not-Aus-Schalters zu beachten, dass auch die USV abgeschaltet und nicht nur von der externen Stromversorgung getrennt wird (siehe auch INF 3.4 Lokale unterbrechungsfreie Stromversorgung).

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 unnotwendigerweise versehentlich oder absichtlich betätigt werden kann.

INF 3.3 Zentrale Notstromversorgung

Relevanz: Umsetzung/Wartung;

In Bereichen, in denen die Stromversorgung bei Ausfällen des öffentlichen Netzes über einen längeren Zeitraum aufrechtzuerhalten ist - dies kann sowohl für die Versorgung von IT-Anlagen als auch der Infrastruktur gelten - ist eine zentrale Notstromversorgung vorzusehen.

Diese wird in der Regel als Diesel-Notstrom-Aggregat realisiert. In einzelnen Fällen, wo die Verfügbarkeitsanforderungen es zulassen, kann die Notstromversorgung auch in Form einer zweiten Energieeinspeisung aus dem Netz eines zweiten Energieversorgungsunternehmens (EVU) realisiert werden.

INF 3.4 Lokale unterbrechungsfreie Stromversorgung

Relevanz: Umsetzung/Wartung;

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 bis 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 länger andauern. Die meisten modernen USV-Geräte bieten Rechnerschnittstellen an, die nach einer vorher festgelegten Zeit, entsprechend dem Zeitbedarf der IT und der Kapazität der USV, ein rechtzeitiges automatisches Herunterfahren (Shut-down) einleiten können. Für spezielle Anwendungsfälle (z.B. TK-Anlagen) kann die erforderliche Überbrückungszeit auch mehrere Stunden betragen.

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

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

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.

In diesem Zusammenhang ist auch INF 3.2 Not-Aus-Schalter zu beachten.

INF 3.5 Blitzschutzeinrichtungen (Äußerer Blitzschutz)

Relevanz: Umsetzung/Wartung;

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

Über diesen “Äußeren Blitzschutz” hinaus ist fast zwingend der “Innere Blitzschutz”, der Überspannungsschutz, erforderlich. Denn der äußere Blitzschutz schützt die elektrischen Betriebsmittel im Gebäude *nicht*. Dies ist nur durch einen Überspannungsschutz möglich (siehe dazu INF 3.6 Überspannungsschutz (Innerer Blitzschutz), dessen hohe Kosten dem Schutzgut gegenüber gerechtfertigt sein müssen).

INF 3.6 Überspannungsschutz (Innerer Blitzschutz)

Relevanz: Umsetzung/Wartung;

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 Blitzschlag 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

Relevanz: Umsetzung/Wartung;

Die Funktion informationstechnischer Geräte kann durch die elektromagnetische Strahlung benachbarter Einrichtungen beeinträchtigt werden. Mögliche Ursachen für solche Störstrahlungen sind Radarstrahlung, Mobilfunk-, 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.

Anmerkung: Diese Maßnahme behandelt den Schutz gegen Störstrahlung im täglichen Umfeld. Schutz gegen einen elektromagnetischen Puls (EMP) als Folge kriegerischer Handlungen gehen über den mittleren Schutzbedarf hinaus und sind daher nicht Gegenstand des vorliegenden Handbuches.

INF 3.8 Schutz gegen kompromittierende Abstrahlung

Relevanz: Management; Umsetzung/Wartung;

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. Daher 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 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. [Anmerkung: Für die Bedeutung des Wortes TEMPEST werden verschiedene Erklärungen genannt, z.B. “Temporary Emission and Spurious Transmission”, “Transient Electromagnetic Pulse Emanation Surveillance Technology” oder “Transient Electromagnetic Pulse Emanations Standard”. Es wird auch die Meinung vertreten, dass es sich nicht um ein Akronym, sondern um einen Codenamen ohne besondere Bedeutung handelt.]
- *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 mit einzubeziehen 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.

Selbst bei der Verwendung von kleinsten Geräten wie beispielsweise Kryptomodulen oder Smart Cards ist auf deren kompromittierende Strahlung zu achten. Gerade bei sicherheitsrelevanten Anwendungen (Zugangssystemen, kryptographische Anwendungen, etc.) ist deren Schutzbedarf immens. In diesem Zusammenhang sind die Möglichkeiten von Side-Channel-Attacken (Differential Power Analysis - DPA, Differential Electro-Manetic Analysis - DEMA) zu berücksichtigen. Demnach sind bereits bei der Anschaffung von Geräten jene mit entsprechenden Gegenmaßnahmen zu bevorzugen.

Auch das Überkoppeln auf Leitungen ist eine Auswirkung von kompromittierender elektromagnetischer Strahlung. Wird ein Signal leitungsgebunden übertragen, so ist der elektrische Leiter mit einem elektromagnetischen Feld umgeben. Dieses Feld erzeugt auf in unmittelbarer Umgebung des Leiters verlegten Kabeln Spannungen und Ströme, aus denen das Signal des ursächlichen Leiters wiedergewonnen werden kann. Dabei spielt es keine Rolle, ob es sich um eine analoge oder digitale Nachrichtenübertragung handelt. In beiden Fällen kann mit recht einfachen Maßnahmen das ursprüngliche Signal wiederaufbereitet werden. Geeignete Schutzmaßnahmen sind:

- Wahl geeigneter Kabeltypen wie beispielsweise Koaxial- oder Twisted-Pair-Kabeln
- Achten auf hochwertige Schirmung der Kabel (vorzugsweise ist doppelte Schirmung zu verwenden - Kombination aus Folien- und Geflechtschirmung)
- Verlegung parallel geführter Kabel in ausreichendem Abstand zueinander
- Verringerung des Signal-Oberwellengehaltes durch elektrische Filterung (besonders bei digitalen Übertragungen)
- Vorzugsweise Verwendung von Lichtwellenleitern (Gefahr des Übersprechens deutlich geringer aber in Folge mechanischer Beschädigungen des Kabels ebenfalls möglich)

INF 3.9 Schutz gegen elektrostatische Aufladung

Relevanz: Umsetzung/Wartung;

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

Relevanz: Umsetzung/Wartung;

INF 4.1 Lagepläne der Versorgungsleitungen

Relevanz: Umsetzung/Wartung;

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 und INF 3.8 Schutz gegen kompromittierende Abstrahlung.

INF 4.2 Materielle Sicherung von Leitungen und Verteilern

Relevanz: Umsetzung/Wartung;

In Räumen mit Publikumsverkehr oder in unübersichtlichen Bereichen eines Gebäudes und zugehöriger Bereiche ist es sinnvoll, Leitungen und Verteiler zu sichern.

Dies kann auf verschiedene Weise erreicht werden, etwa:

- Verlegung der Leitungen unter Putz,
- Nagetierschutz.
- Verlegung der Leitungen in Stahl- oder Kunststoffpanzerrohren,
- 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. Weitere Angaben zur geeigneten Aufstellung und Aufbewahrung von IT-Systemen sind unter Kapitel 1.5 „Geeignete Aufstellung und Aufbewahrung“ zu finden.

INF 4.3 Entfernen oder Kurzschließen und Erden nicht benötigter Leitungen

Relevanz: Umsetzung/Wartung;

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 Netz entfernt werden.

INF 4.4 Auswahl geeigneter Kabeltypen

Relevanz: Umsetzung/Wartung;

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.

Vgl. dazu auch INF 3.8 Schutz gegen kompromittierende Abstrahlung.

INF 4.5 Schadensmindernde Kabelführung

Relevanz: Umsetzung/Wartung;

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/der Benutzer/in zugänglich sind. Ein übersichtlicher Aufbau der Trassen erleichtert die Kontrolle. Trassen und einzelne Kabel sollen immer so verlegt werden, dass sie vor direkten Beschädigungen durch Personen, Fahrzeuge und Maschinen geschützt sind.

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

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

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

Bereiche mit hoher Brandgefahr sind zu meiden. Ist dies nicht möglich und ist der Betriebserhalt aller auf der Trasse liegenden Kabel erforderlich, ist der entsprechende Trassenbereich mit Brandabschottung (s.a. INF 2.4 „Brandabschottung von Trassen“) zu versehen. Ist der Betriebserhalt nur für einzelne Kabel erforderlich, ist dafür ein entsprechendes Kabel zu wählen.

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

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

INF 4.6 Vermeidung von wasserführenden Leitungen

Relevanz: Umsetzung/Wartung;

In Räumen oder Bereichen, in denen sich IT-Geräte mit zentralen Funktionen (z.B. Server) befinden, sollten wasserführende Leitungen aller Art vermieden werden. Die einzigen wasserführenden Leitungen sollten, wenn unbedingt erforderlich, Kühlwasserleitungen, Löschwasserleitungen und Heizungsrohre sein. Zuleitungen zu Heizkörpern sollten mit Absperrventilen, möglichst außerhalb des Raumes/Bereiches, versehen werden. Außerhalb der Heizperiode sind diese Ventile zu schließen.

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

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

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

1.5 Geeignete Aufstellung und Aufbewahrung

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

Bei der Aufstellung eines IT-Systems sind verschiedene Voraussetzungen zu beachten, die die Sicherheit des Systems gewährleisten bzw. erhöhen sollen. Über diese Sicherheitsaspekte (die 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 (INF 5.1: PCs, Notebooks, Telearbeitsplätze,..)
- Server (INF 5.2: neben Datenbankservern, Kommunikationsservern, etc. sind davon auch Telekommunikationsanlagen umfasst)
- Netzwerkkomponenten (INF 5.3: z.B. Modems, Router, Verteilerschränke, ...)

Wie für das gesamte Handbuch zutreffend und bereits in der Einleitung ausgeführt, wird auch 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 oben genannten Gruppen nicht möglich ist. So kann ein Fax etwa als Stand-alone-Gerät betrachtet werden, oder aber als Teil eines Arbeitsplatz-IT-Systems, falls die Möglichkeit besteht, ein 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

Relevanz: Umsetzung/Wartung; Anwender/innen;

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

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

- der Standort in der Nähe eines Fensters oder einer Tür erhöht die Gefahr des Beobachtens von außerhalb,
- das System sollte nicht in unmittelbarer Nähe der Heizung aufgestellt werden (Vermeidung von Überhitzung, aber auch kompromittierender Abstrahlung, vgl. INF 3.8 „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

Relevanz: Umsetzung/Wartung;

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, ist 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 Ausnahmesituationen nicht vorkommen können.

INF 5.3 Geeignete Aufstellung von Netzwerkkomponenten

Relevanz: Umsetzung/Wartung;

Unter 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 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

Relevanz: Umsetzung/Wartung; Anwender/innen;

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 der Benutzerin / des Benutzers liegen, muss sie/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/innen 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/innen 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 eingeschränkte, vertrauliche, geheime und/oder streng geheime bzw. personenbezogene und/oder sensible Daten (Definitionen s. Teil 1, Kapitel 3.2.5 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“ und Kapitel 5.1). Dabei ist zu beachten, dass die Zulässigkeit von Verschlüsselungstechnologien in den einzelnen Staaten unterschiedlich geregelt ist.
- 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 aufliegen. 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

Relevanz: Anwender/innen;

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 „Betriebsmittel und Datenträger“.

INF 5.6 Serverräume

Relevanz: Management; Umsetzung/Wartung;

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 2.8 Handfeuerlöscher
- INF 2.11 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

Relevanz: Umsetzung/Wartung; Anwender/innen;

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 und 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 [Anmerkung - RAL: Deutsches Institut für Gütesicherung und Kennzeichnung e.V. Bonn] 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 des Verbandes deutscher Maschinen- und Anlagenbau e.V. (VDMA) und RAL-RG 627 für Wertschränke. Hilfestellung bei der Bewertung des Widerstandswertes verschiedener Schutzschränke gibt das

VDMA-Einheitsblatt 24990, in dem Sicherheitsmerkmale von Schutzschränken kurz beschrieben werden.

Bei der Auswahl von Schutzschränken ist auch die zulässige Deckenbelastung am Aufstellungsort zu berücksichtigen. 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 eines Schutzschrankes festgelegt werden, welche Geräte bzw. welche Arten von Datenträgern in ihm aufbewahrt werden sollen. Die Innenausstattung des Schutzschrankes ist dieser Festlegung angemessen auszuwählen. Nachrüstungen sind in der Regel schwierig, da der Schutzwert des Schrankes und seine spezifische Zulassung beeinträchtigt werden können. Es sollte auch Raum für zukünftige Erweiterungen mit eingeplant werden.

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 und eine Tastatur auch Platz für einen Bildschirm und weitere Peripheriegeräte wie z.B. Bandlaufwerke vorgesehen werden, damit Administrationsarbeiten vor Ort durchgeführt werden können. Dazu ist zu beachten, dass die Ausstattung ergonomisch gewählt ist, damit Administrationsarbeiten am Server ungehindert durchgeführt werden können. So ist zum Beispiel ein ausziehbarer Boden für die Tastatur wünschenswert, der in einer Höhe angebracht wird, dass Administratoren Arbeiten sitzend durchführen können. Je nach Nutzung des Schrankes können auch eine Klimatisierung und/oder eine USV-Versorgung erforderlich sein. Die entsprechenden Geräte sollten dann im Schrank mit untergebracht werden. Andernfalls muss zumindest eine Lüftung vorhanden sein. Die Ausstattung des Schrankes mit einem lokal arbeitenden Brandfrüherkennungssystem, das im Brandfall die Stromzufuhr der Geräte unterbricht (auf der Eingangs- *und* der Ausgangsseite der USV, sofern diese vorhanden ist), ist empfehlenswert.

Nicht im gleichen Schrank untergebracht werden sollten Backup-Datenträger und Protokolldrucker. Backup-Datenträger würden im Falle einer Beschädigung des Servers vermutlich ebenfalls beschädigt. Die Protokollierung der Aktionen am Server dient auch zur Kontrolle der Administratoren. Es ist also nicht sinnvoll, ihnen, ggf. sogar als Einzigen, Zugriff auf die 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 Verlassen 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, arithmetische 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 eine/n Angreifer/in schwieriger ist, sich Zugriff zu verschaffen.

1.6 Weitere Schutzmaßnahmen

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

INF 6.1 Einhaltung einschlägiger Normen und Vorschriften

Relevanz: Umsetzung/Wartung;

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/die Benutzer/in und Sicherheit für den Betrieb gewährleisten. Bei der Planung und Errichtung von Gebäuden, bei deren Umbau, beim Einbau technischer Gebäudeausrüstungen (z.B. interne Versorgungsnetze wie Telefon- oder Datennetze) und bei Beschaffung und Betrieb von Geräten sind entsprechende Normen und Vorschriften unbedingt zu beachten.

In Anhang A werden einige dieser Normen beispielhaft angeführt.

INF 6.2 Regelungen für Zutritt zu Verteilern

Relevanz: Umsetzung/Wartung; Anwender/innen;

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

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

Mit möglich ist gemeint, dass

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

Mit geordnet ist gemeint, dass

- festgelegt ist, wer welchen Verteiler öffnen darf. Verteiler sollten verschlossen sein und dürfen nur von den für die jeweilige Versorgungseinrichtung zuständigen Personen geöffnet werden. Die Zugriffsmöglichkeiten können durch unterschiedliche Schlüssel und entsprechende Schlüsselverwaltung geregelt werden (siehe dazu INF 1.4 „Zutrittskontrolle“).

INF 6.3 Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile

Relevanz: Umsetzung/Wartung;

Schützenswerte Gebäudeteile sind z.B. Rechenzentrum, Serverraum, Datenträgerarchiv, Klimazentrale, Verteilungen der Stromversorgung, Schalträume, Ersatzteillager. Solche Bereiche sollten nach Möglichkeit keinen Hinweis auf ihre Nutzung tragen. Türschilder wie z.B. “Rechenzentrum” oder “EDV-Archiv” geben einem potentiellen Angreifer, der zum Gebäude Zutritt hat, Hinweise, um seine Aktivitäten gezielter und damit Erfolg versprechender vorbereiten 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 Gebäudeteile“), so sind geeignete Maßnahmen zu treffen, um den Einblick zu verhindern oder so zu gestalten, dass die Nutzung nicht offenbar wird. Dabei ist darauf zu achten, dass z.B. nicht nur ein Fenster einer ganzen Etage mit einem Sichtschutz versehen wird.

INF 6.4 Geschlossene Fenster und Türen

Relevanz: Umsetzung/Wartung; Anwender/innen;

Fenster und nach außen gehende Türen (Balkone, Terrassen) sind in Zeiten, in denen ein Raum nicht besetzt ist, zu schließen. Im Keller- und Erdgeschoss und, je nach Fassadengestaltung, auch in den höheren Etagen bieten sie einem/einer Einbrecher/in auch während der Betriebszeiten eine ideale Einstiegsmöglichkeit. Während normaler Arbeitszeiten und sichergestellter kurzer Abwesenheit der Mitarbeiterin/des Mitarbeiters kann von einer zwingenden Regelung für 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 jede/r Mitarbeiter/in vor ihrer/seiner Abwesenheit Unterlagen und den persönlichen Arbeitsbereich (Schreibtisch, Schrank und PC (Schloss für Diskettenlaufwerk, Tastaturschloss, Telefon) verschließen (s.a. PER 1.7 „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 eines 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 ist, dass keine schutzbedürftigen Gegenstände wie Unterlagen oder Datenträger offen aufliegen.

Es muss auf jeden Fall sichergestellt werden, dass die Passworteingabe keinesfalls umgangen werden kann.

INF 6.5 Alarmanlage

Relevanz: Umsetzung/Wartung;

Ist eine Alarmanlage für Einbruch oder Brand vorhanden und lässt sich diese mit vertretbarem Aufwand entsprechend erweitern, ist zu überlegen, ob zumindest die Kernbereiche der IT (Serverräume, Datenträgerarchive, Räume für technische Infrastruktur u.ä.) in die Überwachung durch diese Anlage mit eingebunden werden sollen. So lassen sich Gefährdungen wie Feuer, Einbruch, Diebstahl frühzeitig erkennen und Gegenmaßnahmen einleiten. Um die Schutzwirkung aufrechtzuerhalten, ist eine regelmäßige Wartung und Funktionsprüfung der 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 Anschluss 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.
- Besonders wirksam ist „Stiller Alarm mit Rückfrage“, dies erfordert jedoch zusätzlichen organisatorischen Aufwand.

INF 6.6 Fernanzeige von Störungen

Relevanz: Umsetzung/Wartung;

IT-Geräte und Supportgeräte, die keine oder nur seltene Bedienung durch eine Person erfordern, werden oft in ge- und verschlossenen Räumen untergebracht (z.B. Serverraum). Das führt dazu, dass Störungen, die sich in ihrem Frühstadium auf die IT noch nicht auswirken und einfach zu beheben sind, erst zu spät, meist durch ihre Auswirkungen auf die IT, entdeckt werden. Feuer, Funktionsstörungen einer USV oder der Ausfall eines Klimagerätes seien als Beispiele für solche “schleichenden” Gefährdungen angeführt.

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

INF 6.7 Klimatisierung

Relevanz: Umsetzung/Wartung;

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

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

Zusätzlich 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 eine Korrosion von IT-Bauteilen durch vorbeigeführte Luft aus der Klimaanlage zu vermeiden.

Um die Schutzwirkung aufrechtzuerhalten ist eine regelmäßige Wartung der Klimatisierungseinrichtung vorzusehen.

INF 6.8 Selbsttätige Entwässerung

Relevanz: Umsetzung/Wartung;

Alle Bereiche, in denen sich Wasser sammeln und stauen kann oder in denen fließendes oder stehendes Wasser nicht oder erst spät entdeckt wird und in denen das Wasser Schäden verursachen kann, sollten mit einer selbsttätigen Entwässerung und ggf. mit Wassermeldern ausgestattet sein. Zu diesen Bereichen gehören u. a. Keller, Lufträume unter Doppelböden, Lichtschächte und Heizungsanlagen.

INF 6.9 Videounterstützte Überwachung

Relevanz: Management; Umsetzung/Wartung;

Zur besseren Absicherung der Infrastruktur sollte bei Bedarf auf ein videounterstütztes Überwachungssystem zurückgegriffen werden.

Derartige Überwachungssysteme stellen eine sinnvolle Ergänzung der bestehenden Maßnahmen (vgl. Abschnitt 1.6) dar. Bei geeigneter Aufstellung ist auch die von Überwachungskameras ausgehende Abschreckung ein Vorteil derartiger Systeme. Im Zuge der Konzeption und Installation müssen Personal sowie zusätzliche technische und infrastrukturelle Vorkehrungen zur Auswertung vorgesehen werden.

Die Wahl der Aufstellungsplätze der Kameras sollte unter Beiziehung der Betriebsrätin/des Betriebsrates und unter Berücksichtigung des Datenschutzes erfolgen.

INF 6.10 Aktualität von Plänen

Relevanz: Umsetzung/Wartung;

Sämtliche Pläne sind aktuell zu halten und an geeigneten Stellen zu deponieren.

Nach jedem Eingriff der eine Aktualisierung der Pläne erforderlich macht (bauliche Maßnahmen o.ä.), sind diese umgehend auf den aktuellen Stand zu bringen. In diesem Zuge sind auch alle im Umlauf befindlichen Kopien der Pläne durch aktualisierte Kopien zu ersetzen.

INF 6.11 Vorgaben für ein Rechenzentrum

Relevanz: Management; Umsetzung/Wartung;

Ein Rechenzentrum gilt als schützenswert und sollte daher im Sinne eines Sicherheitsbereiches konzipiert sein.

In diesem Zusammenhang sind die im Kapitel 1 „Bauliche und infrastrukturelle Maßnahmen“ getroffenen Maßnahmen von besonderer Bedeutung. Aus diesem Katalog sollten folgende Punkte besonders beachtet werden:

- geeignete Standortwahl (INF 1.1 „Geeignete Standortauswahl“)
- ausreichender Einbruchschutz (INF 1.3 „Einbruchsschutz“)
- Zutrittskontrollen (INF 1.4 „Zutrittskontrolle“)
- Aufstellung und Anordnung von Geräten (Abschnitt 1.5 „Geeignete Aufstellung und Aufbewahrung“)

Weiters ist zu beachten:

- Verfügbarkeitsanforderungen (Abschnitt 7.2 „Strategie und Planung“)

2 Personelle Maßnahmen

Die Mitarbeiter/innen stellen eine der wichtigsten Ressourcen einer Organisation dar. IT-Sicherheit kann auch bei besten technischen Maßnahmen nur funktionieren, wenn die Mitarbeiter/innen ein ausgeprägtes Sicherheitsbewusstsein haben und bereit und fähig sind, die Vorgaben in der täglichen Praxis umzusetzen. Andererseits stellen Mitarbeiter/innen 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 Mitarbeiterinnen/Mitarbeitern auseinander zu setzen (”Know your Employee”).

Im Folgenden werden in Kapitel 2.1 Regelungen für eigene Mitarbeiter/innen 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/innen

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

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

Relevanz: Umsetzung/Wartung; Anwender/innen;

Bei der Einstellung von Mitarbeiterinnen/Mitarbeitern sind diese zur Einhaltung einschlägiger Gesetze (z.B. Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999 i.d.g.F.) § 15 “Datengeheimnis”, § 14 “Datensicherheitsmaßnahmen” und § 13 “Genehmigungspflichtige Übermittlung und Überlassung von Daten ins Ausland” sowie dem Informationssicherheitsgesetz (InfoSiG), BGBl. I Nr. 23/2002 i.d.g.F. für den Bereich der öffentlichen Verwaltung), Vorschriften und interner Regelungen zu verpflichten. Damit sollen neue Mitarbeiter/innen 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/innen 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. Remote Access und Anhang C)

PER 1.2 Aufnahme der sicherheitsrelevanten Aufgaben und Verantwortlichkeiten in die Stellenbeschreibung

Relevanz: Management;

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/innen mit speziellen Sicherheitsaufgaben (Mitglieder des IT-Sicherheitsmanagement-Teams, Datenschutzbeauftragte, 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 sowie eine zeitgerechte Einarbeitung unkundiger Mitarbeiter/innen unbedingt erforderlich sind.

Für die Vertretungsregelungen sind folgende Randbedingungen einzuhalten:

- Die Übernahme von Aufgaben im Vertretungsfall setzt voraus, dass der Verfahrens- oder Projektstand hinreichend dokumentiert ist.
- Die/der Vertreter/in muss so geschult werden, dass sie/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, eine/einen Vertreter/in zu schulen.
- Es muss festgelegt sein, welcher Aufgabenumfang im Vertretungsfall von wem wahrgenommen werden soll.
- Die/der Vertreter/in darf die erforderlichen Zugangs- und Zutrittsberechtigungen nur im Vertretungsfall erhalten.
- Ist es in Ausnahmefällen nicht möglich, für Personen eine/einen kompetente/n Vertreter/in zu benennen oder zu schulen, sollte frühzeitig überlegt werden, welche externen Kräfte für den Vertretungsfall eingesetzt werden können.
- Es sollte vermieden werden, dass Vertretungsregeln u.U. vorgesehene Mehraugenprinzipien unterlaufen, z.B. wenn sich zwei kollektiv Berechtigte wechselseitig vertreten.
- Im Zusammenhang mit der Verwendung von kryptographischen Systemen ist auch über ein Verfahren zur Offenlegung von kryptographischen Schlüsseln im Rahmen des Kryptokonzeptes zu achten (siehe auch Kapitel 5.11 „Kryptographische Maßnahmen“).

PER 1.4 Geregelte Verfahrensweise beim Ausscheiden von Mitarbeiterinnen/Mitarbeitern

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

Scheidet eine/ein Mitarbeiter/in aus, so sollten einige Punkte beachtet werden.

Dies wären:

- Vor dem Ausscheiden ist eine Einweisung der/des Nachfolgerin/Nachfolgers durchzuführen.
- Von der/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 die/den Ausscheidende/n 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.
- Vor der Verabschiedung sollte noch einmal explizit darauf hingewiesen werden, dass alle Verschwiegenheitserklärungen weiterhin in Kraft bleiben und keine im Rahmen der Tätigkeit erhaltenen Informationen weitergegeben werden dürfen.
- Nach Möglichkeit sollte eine Neuvergabe der User-ID an eine/einen andere/n Mitarbeiter/in vermieden/ausgeschlossen werden.
- Ist die ausscheidende Person eine/ein Funktionsträger/in in einem Notlaufplan, so ist der Notlaufplan zu aktualisieren.
- Sämtliche mit Sicherheitsaufgaben betrauten Personen, insbesondere der Portierdienst, sind über das Ausscheiden der/des Mitarbeiterin/Mitarbeiters zu unterrichten.
- Ausgeschiedenen Mitarbeiterinnen/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 der/des Ausscheidenden vorgezeichnet sind, die sie/er vor Verlassen der Behörde bzw. des Unternehmens zu erledigen hat.

PER 1.5 Geregelte Verfahrensweise bei Versetzung einer/eines Mitarbeiterin/Mitarbeiters

Relevanz: Umsetzung/Wartung;

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

PER 1.6 Gewährleistung eines positiven Betriebsklimas

Relevanz: Management;

Ein positives Betriebsklima motiviert die Mitarbeiter/innen einerseits zur Einhaltung von IT-Sicherheitsmaßnahmen und bewirkt andererseits die Reduzierung von fahrlässigen oder vorsätzlichen Handlungen (vgl. §126a zu Datenbeschädigung (StGB), BGBl. Nr. 60/1974 i.d.g.F.), die eine Störung des IT-Betriebs herbeiführen können. Daher sollte auch unter IT-Sicherheitsaspekten versucht werden, ein positives Betriebsklima zu erreichen.

Dazu gehört auch die ergonomische Gestaltung des Arbeitsplatzes. Hierzu besteht 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 betont.

Weiters ist bei der Ausstattung von Arbeitsplätzen darauf zu achten, dass die Einhaltung von 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 einer/eines Arbeitnehmerin/Arbeitnehmers sein. Daher ist es für jede Organisation wichtig, ihre Mitarbeiter/innen und eventuelle potentielle Probleme zu kennen (”Know your Employee”). In vielen Fällen kann es hilfreich sein, wenn eine Anlaufstelle zur Verfügung steht, die bei solchen Problemen konkrete Hilfe und Lösungsmöglichkeiten anbieten kann.

PER 1.7 Clear Desk Policy

Relevanz: Umsetzung/Wartung; Anwender/innen;

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

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

PER 1.8 Benennung eines vertrauenswürdigen Administrators und Vertreterin/Vertreters

Relevanz: Management; Umsetzung/Wartung;

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

Das hierfür eingesetzte Personal muss sorgfältig ausgewählt werden. Es soll regelmäßig darüber belehrt werden, dass die Befugnisse nur für die erforderlichen Administrationsaufgaben verwendet werden dürfen. Eine regelmäßige Kontrolle von 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/innen zum Abmelden

Relevanz: Umsetzung/Wartung; Anwender/innen;

Wird ein PC von mehreren Benutzerinnen/Benutzern genutzt und besitzen die einzelnen Benutzer/innen unterschiedliche Zugriffsrechte auf im PC gespeicherte Daten oder Programme, so kann der erforderliche Schutz mittels einer Zugriffskontrolle nur dann erreicht werden, wenn jede/r Benutzer/in sich nach Aufgabenerfüllung bzw. bei Verlassen des Arbeitsplatzes am PC abmeldet. Ist es einer/einem Dritten möglich, an einem PC unter der Identität einer/eines Anderen weiterzuarbeiten, so ist jegliche sinnvolle Zugriffskontrolle unmöglich. Daher sind alle PC-Benutzer/innen zu verpflichten, sich bei Verlassen des Arbeitsplatzes abzumelden.

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

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

PER 1.10 Kontrolle der Einhaltung der organisatorischen Vorgaben

Relevanz: Umsetzung/Wartung;

Mittels Protokollauswertung oder durch Stichproben ist in angemessenen Zeitabständen zu überprüfen, ob die Benutzer/innen eines IT-Systems die organisatorischen Vorgaben (etwa Verpflichtung zur Abmeldung nach Aufgabenerfüllung oder Verbot der Weitergabe von Passwörtern) auch tatsächlich einhalten.

Kontrollen sollten vor allen Dingen darauf ausgerichtet sein, Mängel abzustellen. Für die Akzeptanz von Kontrollen ist es wichtig, dass dies allen Beteiligten als Ziel der Kontrollen erkennbar ist und dass dabei keine Personen bloßgestellt werden oder als “Schuldige” identifiziert werden. Wenn die Mitarbeiter/innen dies befürchten müssen, besteht die Gefahr, dass sie nicht offen über ihnen bekannte Schwachstellen und Sicherheitslücken berichten, sondern versuchen, bestehende Probleme zu vertuschen. Es ist daher sinnvoll, während einer Kontrolle mit den Beteiligten über mögliche Problemlösungen zu sprechen und entsprechende Abhilfen vorzubereiten.

Wenn Mitarbeiter/innen eine Regelung ignorieren oder umgehen, ist das meist ein Zeichen dafür, dass diese nicht mit den Arbeitsabläufen vereinbar ist oder durch die Mitarbeiter/innen nicht umgesetzt werden kann. Beispielsweise ist eine Anweisung, vertrauliche Schreiben nicht unbeaufsichtigt am Drucker liegen zu lassen, unsinnig, wenn zum Drucken nur ein weit entfernter Netzdrucker zur Verfügung steht.

Wenn bei Kontrollen Mängel festgestellt werden, kommt es nicht darauf an, nur die Symptome zu beseitigen. Vielmehr ist es wichtig, die Ursachen für diese Probleme festzustellen und Lösungen aufzuzeigen. Diese können beispielsweise in der Änderung bestehender Regelungen oder in der Hinzunahme technischer Maßnahmen bestehen.

PER 1.11 Geregelte Verfahrensweise bei vermuteten Sicherheitsverletzungen

Relevanz: Management; Umsetzung/Wartung;

Die Vorgehensweise zur Untersuchung angeblicher (bewusster oder versehentlicher) Verletzungen von Sicherheitsvorgaben sowie potentielle Konsequenzen - im Falle interner Mitarbeiter/innen können dies beispielsweise disziplinäre Maßnahmen sein, im Falle externer Mitarbeiter/innen etwa vertraglich abgeleitete Konsequenzen - sollen festgelegt, vom Management verabschiedet und allen Mitarbeiterinnen/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

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

PER 2.1 Regelungen für den kurzfristigen Einsatz von Fremdpersonal

Relevanz: Management; Umsetzung/Wartung;

Kurzfristig oder einmalig zum Einsatz kommendes Fremdpersonal ist wie Besucher/innen zu behandeln, d.h. dass also etwa der Aufenthalt in sicherheitsrelevanten Bereichen nur in Begleitung von Mitarbeiterinnen/Mitarbeitern der Behörde bzw. des Unternehmens erlaubt ist etc. (vgl. dazu etwa INF 1.6 Portierdienst).

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

Relevanz: Umsetzung/Wartung;

Externe Mitarbeiter/innen, die über einen längeren Zeitraum in einer oder für eine Organisation tätig 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.

PER 2.3 Beaufsichtigung oder Begleitung von Fremdpersonen

Relevanz: Umsetzung/Wartung; Anwender/innen;

Fremde (Besucher/innen, Handwerker/innen, Wartungs- und Reinigungspersonal) sollten, außer in Räumen, die ausdrücklich dafür vorgesehen sind, nicht unbeaufsichtigt sein (siehe auch INF 1.4 Zutrittskontrolle und INF 1.6 Portierdienst). Wird es erforderlich, eine/einen Fremde/n allein im

Büro zurückzulassen, sollte man eine/einen Kollegin/Kollegen ins Zimmer oder den/die Besucher/in zu einer/einem Kollegin/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/innen 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. Telearbeit).

Die Notwendigkeit dieser Maßnahmen ist den Mitarbeiterinnen/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/innen über die IT-Sicherheitspolitik

Relevanz: Management; Umsetzung/Wartung;

Externe Mitarbeiter/innen 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

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

PER 3.1 Geregelte Einarbeitung/Einweisung neuer Mitarbeiter/innen

Relevanz: Umsetzung/Wartung;

Neuen Mitarbeiterinnen/Mitarbeitern müssen interne Regelungen, Gepflogenheiten und Verfahrensweisen im IT-Einsatz bekannt gegeben werden. Ohne eine entsprechende Einweisung kennen sie ihre Ansprechpartner/innen 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/innen 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 und Sensibilisierung zu IT-Sicherheitsmaßnahmen),
- Vorstellung aller Ansprechpartner/innen, insbesondere zu IT-Sicherheitsfragen,
- Erläuterung der hausinternen Regelungen und Vorschriften zur IT-Sicherheit und der organisationsweiten IT-Sicherheitspolitik.

PER 3.2 Schulung vor Programmnutzung

Relevanz: Umsetzung/Wartung;

Durch unsachgemäßen Umgang mit IT-Anwendungen hervorgerufene Schäden können vermieden werden, wenn die Benutzer/innen eingehend in die IT-Anwendungen eingewiesen werden. Daher ist es unabdingbar, dass die Benutzer/innen 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 und Sensibilisierung zu IT-Sicherheitsmaßnahmen

Relevanz: Umsetzung/Wartung; Anwender/innen;

Umfassende IT-Sicherheit kann nur dann gewährleistet werden, wenn alle beteiligten und betroffenen Personen einen angemessenen Kenntnisstand über IT-Sicherheit allgemein und insbesondere über die Gefahren und Gegenmaßnahmen in ihrem eigenen Arbeitsgebiet haben. Es liegt in der Verantwortung der Organisationsleitung, durch geeignete Schulungsmaßnahmen hierfür die nötigen Voraussetzungen zu schaffen. Darüber hinaus sollte jede/r Benutzer/in dazu motiviert werden, sich auch in Eigeninitiative Kenntnisse anzueignen.

Angesichts des Umfangs der möglichen Schulungsthemen und der Bedeutung der IT-Sicherheit ist bei der Auswahl der Schulungsinhalte ein koordiniertes Vorgehen erforderlich. Dieses ist in Schulungskonzepten darzulegen und zu dokumentieren.

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

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

- *Sensibilisierung für IT-Sicherheit*
  Die überwiegende Zahl von Schäden im IT-Bereich entsteht durch Nachlässigkeit. Um dies zu verhindern, ist jede/r Einzelne zum sorgfältigen Umgang mit der IT zu motivieren. Zusätzlich sind Verhaltensregeln zu vermitteln, die Verständnis für die IT-Sicherheitsmaßnahmen wecken. Jede/r Mitarbeiter/in 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, im Intranet oder am “Schwarzen Brett”.

- *Die mitarbeiter/innenbezogenen IT-Sicherheitsmaßnahmen*
  Zu diesem Thema sollen die IT-Sicherheitsmaßnahmen vermittelt werden, die in einem IT-Sicherheitskonzept erarbeitet wurden und von den einzelnen Mitarbeiterinnen/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 anwendungsspezifische Daten 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 Mitarbeiterinnen/Mitarbeitern vermittelt werden, wie mit Viren umzugehen ist. Mögliche Inhalte dieser Schulung sind (siehe Kap. Virenschutz):
  - 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, Bürgerkarte ...) 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 und 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. Disaster Recovery und Business Continuity Planung) der Organisation und die von jedem Einzelnen durchzuführenden Datensicherungs-aufgaben. Besonders bedeutend ist dies für den PC-Bereich, in dem jede/r Benutzer/in selbst die Datensicherung verantwortlich durchführen muss.
- *Der geregelte Ablauf eines Datenträgeraustausches*
  Die Festlegung, wann welchen Kommunikationspartnerinnen/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/innen in die Handhabung dieser Verfahren ausreichend einzuarbeiten.
- *Der Umgang mit personenbezogenen Daten*
  An den Umgang mit personenbezogenen Daten sind besondere Anforderungen zu stellen. Mitarbeiter/innen, 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/innen (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.
- *Richtiges Verhalten bei Auftreten von Sicherheitsproblemen (IHP)*
  Die in den Incident Handling-Plänen (IHPs) festgelegten Aufgaben und Verantwortlichkeiten aller Mitarbeiter/innen bei Auftreten sicherheitsrelevanter Ereignisse sind allen betroffenen Mitarbeiterinnen/Mitarbeitern bekannt zu machen, regelmäßige Schulungen und gegebenenfalls praktische Übungen sind vorzusehen (vgl. auch PER 3.5 Aktionen bei Auftreten von Sicherheitsproblemen (Incident Handling Pläne))
- *Vorbeugung gegen Social Engineering*
  Die Mitarbeiter/innen 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/innen regelmäßig darauf hingewiesen werden, die Identität von Gesprächspartnerinnen/Gesprächspartnern zu überprüfen und insbesondere am Telefon keine vertraulichen Informationen weiterzugeben.

PER 3.4 Betreuung und Beratung von IT-Benutzerinnen/IT-Benutzern

Relevanz: Umsetzung/Wartung;

Neben der Schulung, die die IT-Benutzer/innen in die Lage versetzt, die vorhandene Informationstechnik sachgerecht einzusetzen, bedarf es einer Betreuung und Beratung der IT-Benutzer/innen 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/innen zu beauftragen und diese allen Mitarbeiterinnen/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 jede/n Benutzer/in klar ersichtlich sein, an wen sie/er sich in Problemfällen zu wenden hat.

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

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

Die Aufgaben und Verantwortlichkeiten aller Mitarbeiter/innen 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 Mitarbeiterinnen/Mitarbeitern bekannt zu machen.

PER 3.6 Schulung des Wartungs- und Administrationspersonals

Relevanz: Umsetzung/Wartung;

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 Einweisung in die Regelungen der Handhabung von Kommunikationsmedien

Relevanz: Umsetzung/Wartung; Anwender/innen;

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. Alle Mitarbeiter/innen sind daher auf die Besonderheiten der Handhabung von solchen Geräten hinzuweisen und für potentielle Gefahren zu sensibilisieren.

Verständliche Bedienungsanleitungen, Sicherheitshinweise und ggf. auch Dienstanweisungen sind den Mitarbeiterinnen/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 einer/eines Fax-Verantwortlichen, die/der für die Verteilung eingehender Fax-Sendungen zuständig ist und als Ansprechpartner/in in Fax-Problemfällen fungiert,
- Festlegung, wer das Faxgerät benutzen darf,
- Verbot des Versendens von vertraulichen Informationen per Fax (oder besondere technische und organisatorische 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

Relevanz: Umsetzung/Wartung;

Nach der Beschaffung eines Schutzschrankes (Serverschrank oder Datensicherungsschrank - vgl. auch INF 5.7 Beschaffung und Einsatz geeigneter Schutzschränke) sind die Benutzer/innen 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 minimiert werden. Gegebenenfalls ist sporadisch zu kontrollieren, ob im Serverschrank Wasser kondensiert ist.

3 IT-Sicherheitsmanagement

3.1 IT-Sicherheitsmanagement

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

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.

SMG 1.1 Etablierung eines IT-Sicherheitsmanagementprozesses

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

Methodisches Sicherheitsmanagement ist zur Gewährleistung umfassender und angemessener IT-Sicherheit unerlässlich. Der IT-Sicherheitsmanagementprozess ist daher ein integraler Bestandteil der organisationsweiten IT-Sicherheitspolitik (vgl. SMG 1.2 Erarbeitung einer organisationsweiten IT-Sicherheitspolitik, und in dem Zusammenhang auch [IKTB-170902-8]). 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 Informationssicherheits-managements und die eventuell erforderlichen Rückkopplungen zwischen den einzelnen Stufen. In Teil 1 des vorliegenden Handbuches [KIT S01] werden die zur Etablierung eines umfassenden Informationssicherheitsmanagementprozesses erforderlichen Schritte detailliert beschrieben.

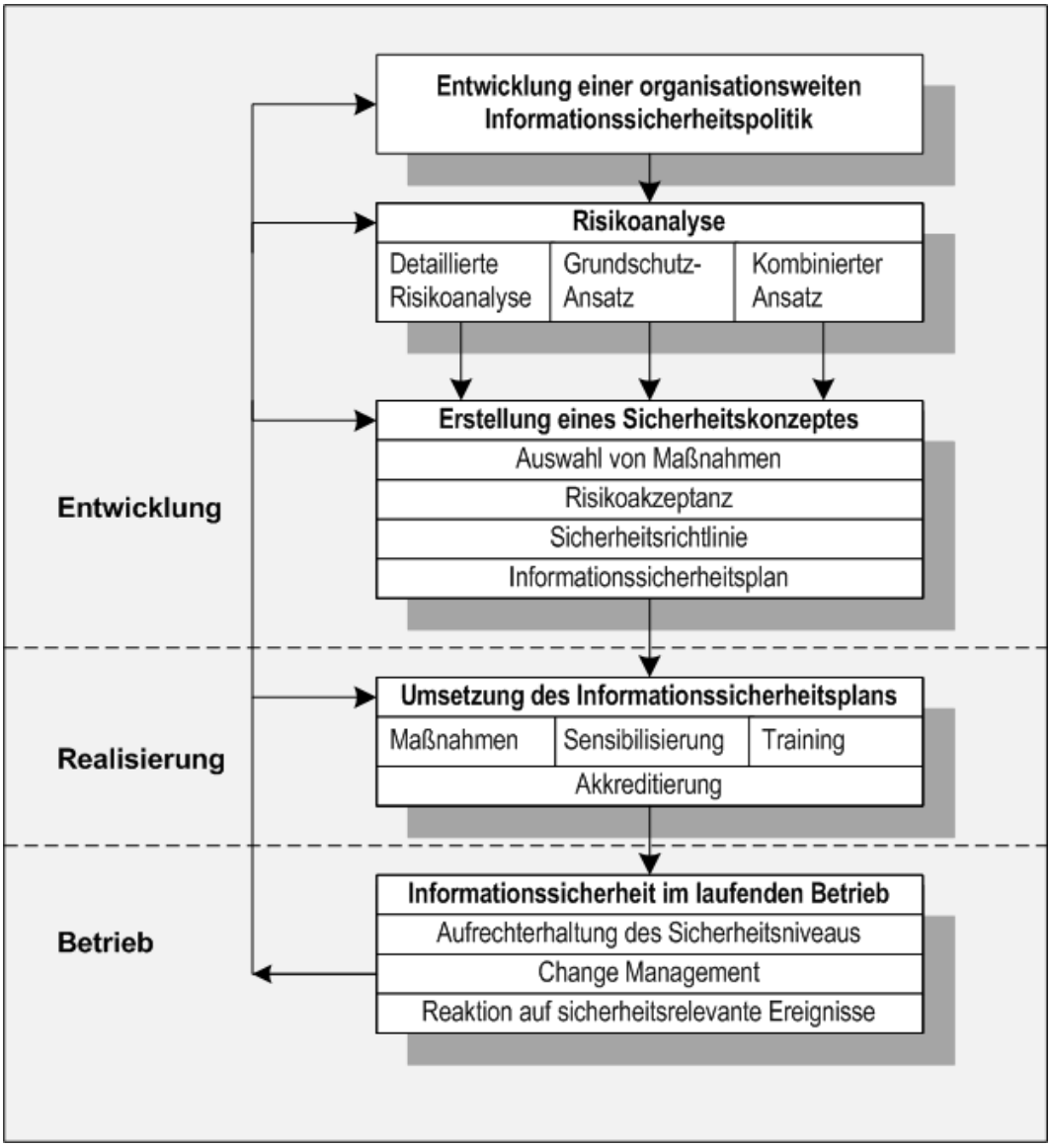

Abbildung 3: Aktivitäten im Rahmen des Informationssicherheitsmanagements

SMG 1.2 Erarbeitung einer organisationsweiten IT-Sicherheitspolitik

Relevanz: Management; Umsetzung/Wartung;

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.

Ressorts in der öffentlichen Verwaltung werden auf Basis des IKT-Board-Beschlusses [IKTB-170902-8] explizit zur Umsetzung einer Sicherheitspolitik angehalten.

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 für alle 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 Risikoakzeptanz
- 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 finden sich in Teil 1, Kapitel 3 [KIT S01] des vorliegenden Handbuches.

Österreichische Sicherheits- und Verteidigungsdoktrin – Teilstrategie IKT-Sicherheit

In diesem Zusammenhang sei auch auf die österreichischen Sicherheits- und Verteidigungsdoktrin – Teilstrategie IKT-Sicherheit [OESVD-IT] hingewiesen.

Darin sind gegliedert in vier Themenbereiche grundlegende Informationen bezüglich der IKT-Sicherheit gegeben, wie:

- *Ist-Analyse:*
  Bietet eine einleitende und allgemeine Darstellung der Ausgangssituation mit der dazu notwendigen Begriffsbildung und Erklärungen zu den rechtlichen und technischen Rahmenbedingungen.
- *Risiko-Analyse:*
  Bietet eine Definition der Risken sowie eine dementsprechende Deklaration von Schutzzielen. Außerdem erfolgt eine Bewertung der aktuellen Entwicklung und Trends auf dem Gebiet der Informationstechnologie als Basis für eine Schlussfolgerung auf zukünftige Bedrohungsszenarien.
- *Strategien:*
  Stellt eine längerfristige Leitlinie für eine adäquate und bestmögliche Sicherheit im Bereich der IKT durch Qualitätssicherung, Notfallvorsorge, Legistik, Organisation, Öffentlichkeits- und Zusammenarbeit.
- *Maßnahmen:*
  Bietet lösungsorientierte Tätigkeiten in Form der Implementierung der anzuwendenden Strategien.

Im Rahmen des IKT-Board Beschlusses vom 18.12.2002 [IKTB-181202-3] wird die Anwendung der Teilstrategie IKT-Sicherheit der österreichischen Sicherheits- und Verteidigungsdoktrin speziell für Organisationen der öffentlichen Verwaltung empfohlen.

SMG 1.3 Erarbeitung von IT-Systemsicherheitspolitiken

Relevanz: Management; Umsetzung/Wartung;

Für jedes IT-System sollte eine IT-Systemsicherheitspolitik erarbeitet werden.

Eine IT-Systemsicherheitspolitik sollte erstellt werden, welche

- 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 Teil 1, Kapitel 5.3 [KIT S01] des vorliegenden Handbuches.

SMG 1.4 Festlegung von Verantwortlichkeiten

Relevanz: Umsetzung/Wartung; Anwender/innen;

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

Diese Festlegung erfolgt zweckmäßig im Rahmen der organisationsweiten IT-Sicherheitspolitik (vgl. SMG 1.2 Erarbeitung einer organisationsweiten IT-Sicherheitspolitik und Teil 1, Kapitel 3 [KIT S01]).

Es empfiehlt sich, darüber hinaus detaillierte Regelungen zu folgenden Bereichen zu treffen:

- 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 Software mit Schadensfunktion (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 Mitarbeiterinnen/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, ungeklärte Zuständigkeiten und Widersprüche zu verhindern.

SMG 1.5 Funktionstrennung

Relevanz: Umsetzung/Wartung;

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

Relevanz: Umsetzung/Wartung;

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.

In Anlehnung an den IKT-Board Beschluss vom 17.09.2002 [IKTB-170902-7] wird die Verwendung und Umsetzung einer sicheren Initialkonfiguration bei der Auslieferung von Systemen im Bundesbereich empfohlen. Dadurch soll das Vertrauen in das Grundsystem gestärkt werden.

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 Benutzerinnen/Benutzern.

IT-Nutzer/innen:

- Bei Gerätewechsel ist keine erneute Einweisung in die IT-Konfiguration erforderlich, Ausfallzeiten werden somit minimiert.
- Bei Fragen zu Hard- und Software können sich Anwender/innen 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/innen werden in dem Umfeld geschult, das sie am Arbeitsplatz vorfinden.

SMG 1.7 Akkreditierung von IT-Systemen

Relevanz: Umsetzung/Wartung;

Für jedes IT-System ist sicherzustellen, dass es den Anforderungen der IT-Systemsicherheitspolitik 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. Security Compliance Checking
- 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 Neuakkreditierung durchzuführen ist, sollten in der IT-Systemsicherheitspolitik festgelegt werden.

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 Sicherheit im gesamten Lebenszyklus eines IT-Systems 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] bzw. der "Common Criteria" [Common Criteria].

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

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

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 [Anmerkung: Dieses wird seit sieben Jahren in vielen europäischen Ländern angewendet und wird laufend von der Bundesrepublik Deutschland gewartet und verbessert.] entwickelt. Es teilt sich in vier Bereiche auf:

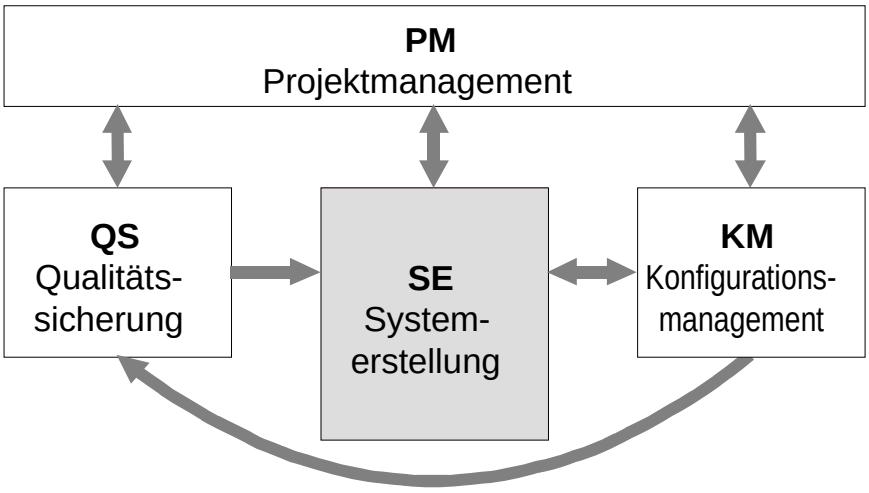

Abbildung 4: Die vier Bereiche (Submodelle) des IT-BVM

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. Kostensteuerung, 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 sich in weitere Elementarphasen (Blöcke im Vordergrund) und diese wiederum in Aktivitäten (nicht abgebildet).

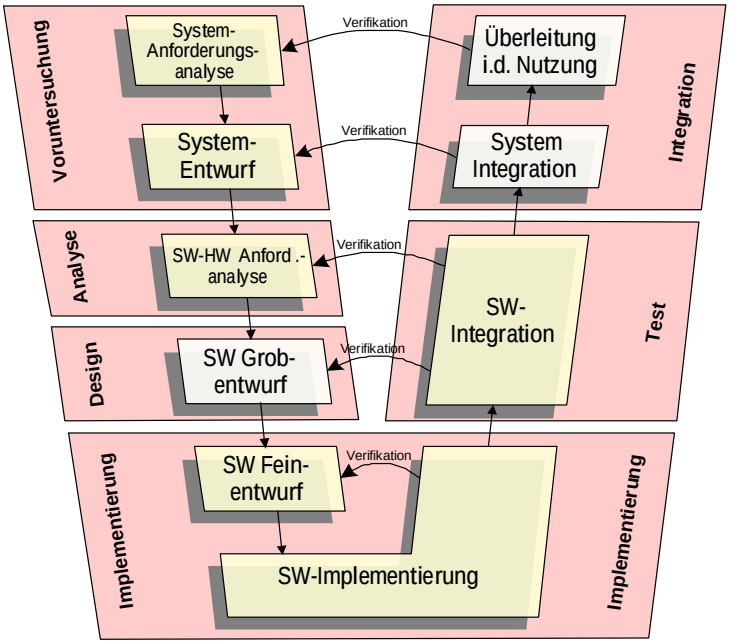

Abbildung 5: Gliederung des Vorgehensmodells

Es folgt eine kurze Beschreibung der Elementarphasen:

- *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 Software 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 Überprüfungen gegenüber dem SW-Feinentwurf werden durchgeführt.
- *SE 7 - SW-Integration*
  Die einzelnen Softwareteile werden zu größeren Softwareeinheiten zusammengefügt und getestet.
- *SE 8 - System integrieren*
  Die Software wird zum Gesamtsystem integriert.
- *SE 9 - Überleitung in die Nutzung*
  Das Gesamtsystem (EDV + Infrastruktur) wird am Bestimmungsort installiert und in Betrieb genommen.

Die Reihenfolge der Aktivitäten erscheint sequentiell. Dies entspricht der Vorstellung vom IT-Systemerstellungsprozess als einem strengen Top-down-Vorgehen. In der Regel sind jedoch Iterationen im Erstellungsprozess üblich. Die nachfolgende Abbildung zeigt eine schematisierte linearisierte Darstellung des logischen Ablaufs der IT-Systemerstellung und deren Einbettung in das organisatorische Umfeld.

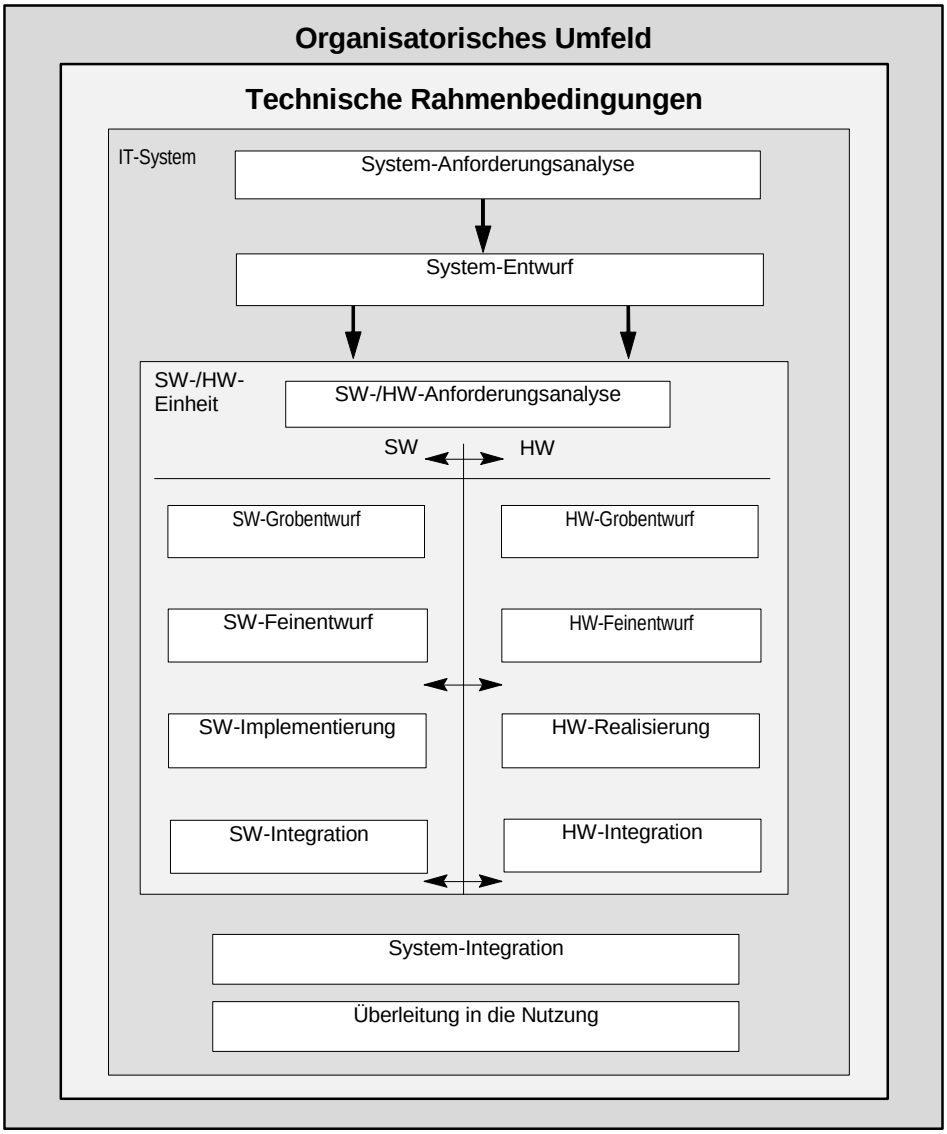

Abbildung 6: Randbedingungen zur IT-Systemerstellung

Das beschriebene Vorgehensmodell dient als Grundlage für die nachfolgenden Maßnahmen. Dabei werden die in den einzelnen Phasen für die IT-Sicherheit relevanten Maßnahmen herausgegriffen. Für weitere Details zum Vorgehensmodell sei auf das Gesamtkonzept ([IT-BVM]) verwiesen.

ENT 1.1 IT-Sicherheit in der System-Anforderungsanalyse

Relevanz: Umsetzung/Wartung;

Die Voruntersuchung besteht aus den Elementarphasen "System-Anforderungsanalyse" und "System-Entwurf", die sich ihrerseits aus unterschiedlichen Aktivitäten zusammensetzen.

In der System-Anforderungsanalyse, der ersten Elementarphase der Phase Voruntersuchung, werden die Anforderungen an das Gesamtsystem erhoben. Unter dem Gesamtsystem versteht man dabei nicht nur das IT-System, sondern auch das fachliche Umfeld, selbst wenn Teile davon später nicht mittels EDV abgedeckt werden.

Der Anforderungskatalog kann etwa Aussagen zu folgenden Punkten enthalten:

- *Funktionale Anforderungen,*
  die das System zur Unterstützung der Aufgabenerfüllung der Fachabteilung erfüllen muss. Die für die Fachaufgabe relevanten Einzelfunktionalitäten sollten hervorgehoben werden.
- *IT-Einsatzumgebung:*
  Diese wird einerseits beschrieben durch die Rahmenbedingungen, die durch die vorhandene oder geplante IT-Einsatzumgebung vorgegeben werden, und andererseits durch die Leistungsanforderungen, die durch das System an die Einsatzumgebung vorgegeben werden.
- *Kompatibilitätsanforderungen*
  zu anderen Programmen oder IT-Systemen, also Migrationsunterstützung und Aufwärts- und Abwärtskompatibilität.
- *Performanceanforderungen:*
  diese beschreiben die erforderlichen Leistungen hinsichtlich Durchsatz und Laufzeitverhalten. Für die geforderten Funktionen sollten möglichst genaue Angaben über die maximal zulässige Bearbeitungszeit getroffen werden.
- *Interoperabilitätsanforderungen,*
  d.h. die Zusammenarbeit mit anderen Produkten bzw. Systemen über Plattformgrenzen hinweg muss möglich sein.
- *Alternativen zu Herstellermonopolen:*
  Alternativen zu entstehenden Herstellermonopolen sind im Rahmen der System-Anforderungsanalyse zu berücksichtigen. Speziell im Hinblick auf Kompatibilität und Austauschbarkeit im Notfall ist dies ein Beitrag zur Systemsicherheit. Als eine der Hauptschwierigkeiten wären beispielsweise proprietäre Protokolle zu identifizieren, die Probleme bei der Suche nach Ersatzsystemen darstellen. Aufgrund des IKT-Board-Beschlusses [IKTB-250602-1] sind derartige Alternativen bei Anschaffungen von Servern im Rahmen der öffentlichen Verwaltung empfohlen. (Vergleiche auch K-Fall-Vorgaben – BCP 2.1)
- *Zuverlässigkeitsanforderungen:*
  Diese betreffen die Stabilität des Systems, also Fehlererkennung und Toleranz sowie Ausfall- und Betriebssicherheit.
- *Konformität zu Standards:*
  Dies können internationale Normen, De-facto-Standards oder auch Hausstandards sein.
- *Einhaltung von internen Regelungen und gesetzlichen Vorschriften,*
  z.B. ausreichender Datenschutz bei der Verarbeitung personenbezogener Daten
- *Anforderungen an die Benutzerfreundlichkeit,*
  insbesondere an die Güte der Benutzeroberfläche sowie die Qualität der Benutzerdokumentation und der Hilfefunktionen.
- Anforderungen an die Wartbarkeit
- *Obergrenze der Kosten:*
  Dabei müssen nicht nur die unmittelbaren Entwicklungs- bzw. Beschaffungskosten für das System selber einbezogen werden, sondern auch Folgekosten, wie z.B. Wartungsaufwände, Personalkosten oder notwendige Schulungen.
- Aus den Anforderungen an die Dokumentation muss hervorgehen, welche Dokumente in welcher Güte (Vollständigkeit, Verständlichkeit) erforderlich sind.
- Bezüglich der Softwarequalität können Anforderungen gestellt werden, die von Herstellererklärungen über die eingesetzten Qualitätssicherungsverfahren, über ISO 9000 Zertifikate bis hin zu unabhängigen Softwareprüfungen nach ISO 12119 reichen.

Zusätzlich zu den operationellen Anforderungen müssen die IT-Sicherheitsziele vorgegeben werden. Dies kann auf zwei Arten erfolgen:
entweder

- durch die Formulierung von Anforderungen an Vertraulichkeit, Integrität oder Verfügbarkeit (vgl. BCP 2.1 von bestimmten operationellen Funktionen oder verarbeiteten Informationen,

oder

- anhand einer bereits vorgegebenen Sicherheitspolitik, die im Gesamtsystem durchgesetzt werden soll.

ENT 1.2 Durchführung einer Risikoanalyse und Festlegung der IT-Sicherheitsanforderungen

Relevanz: Umsetzung/Wartung;

Basierend auf den bereits definierten Anwenderanforderungen und Informationen über die Einsatzumgebung des Systems sind die für das System relevanten Bedrohungen zu ermitteln und die damit verbundenen Risiken zu bewerten.

Zu möglichen Strategien und Vorgehensweisen zur Risikoanalyse s. Teil 1, Kap. 4 [KIT S01] des vorliegenden Sicherheitshandbuches.

Die Ergebnisse der Risikoanalyse bilden die Grundlage für die Formulierung der Anforderungen an die IT-Sicherheit innerhalb der Anwenderforderungen (vgl. ENT 1.1 IT-Sicherheit in der System-Anforderungsanalyse).

Typische *Sicherheitsanforderungen*, die an ein gesamtes IT-System oder auch an eine Einzelkomponente oder ein Produkt möglicherweise gestellt werden, seien im Folgenden kurz erläutert (dabei wird im Folgenden wieder generell von “Systemen” gesprochen). Weitere Ausführungen finden sich in den [ITSEC] und den [Common Criteria].

- *Identifizierung und Authentisierung*
  In vielen Systemen wird es Anforderungen geben, diejenigen Benutzer/innen zu bestimmen und zu überwachen, die Zugriff auf Betriebsmittel haben, die vom System kontrolliert werden. Dazu muss nicht nur die behauptete Identität der/des Benutzerin/Benutzers festgestellt, sondern auch die Tatsache nachgeprüft werden, dass die/der Benutzer/in tatsächlich die Person ist, die sie/er zu sein vorgibt. Dies geschieht, indem die/der Benutzer/in dem System Informationen liefert, die fest mit der/dem betreffenden Benutzer/in verknüpft sind. Dies können entweder personenbezogene oder personengebundene Informationen sein, s. dazu auch Kap. Berechtigungssysteme, Schlüssel- und Passwortverwaltung.
- *Zugriffskontrolle*
  Bei vielen Systemen wird es erforderlich sein, sicherzustellen, dass Benutzer/innen und Prozesse daran gehindert werden, Zugriff auf Informationen oder Betriebsmittel zu erhalten, für die sie kein Zugriffsrecht haben oder für die keine Notwendigkeit zu einem Zugriff besteht. Desgleichen wird es Anforderungen bezüglich der unbefugten Erzeugung, Änderung oder Löschung von Informationen geben.
- *Beweissicherung*
  Bei vielen Systemen wird es erforderlich sein sicherzustellen, dass über Handlungen, die von Benutzerinnen/Benutzern bzw. von Prozessen im Namen solcher Benutzer/innen ausgeführt werden, Informationen aufgezeichnet werden, damit die Folgen solcher Handlungen später der/dem betreffenden Benutzer/in zugeordnet werden können und die/der Benutzer/in für ihre/seine Handlungen verantwortlich gemacht werden kann.

- *Protokollauswertung*
  Bei vielen Systemen wird sicherzustellen sein, dass sowohl über gewöhnliche Vorgänge als auch über außergewöhnliche Vorfälle ausreichend Informationen aufgezeichnet werden, damit durch Nachprüfungen später festgestellt werden kann, ob tatsächlich Sicherheitsverletzungen vorgelegen haben und welche Informationen oder sonstigen Betriebsmittel davon betroffen waren.
- *Unverfälschbarkeit*
  Bei vielen Systemen wird es erforderlich sein, sicherzustellen, dass bestimmte Beziehungen zwischen unterschiedlichen Daten korrekt bleiben und dass Daten zwischen einzelnen Prozessen ohne Änderungen übertragen werden. Daneben müssen auch Funktionen bereitgestellt werden, die es bei der Übertragung von Daten zwischen einzelnen Prozessen, Benutzerinnen/Benutzern und Objekten ermöglichen, Verluste, Ergänzungen oder Veränderungen zu entdecken bzw. zu verhindern, und die es unmöglich machen, die angebliche oder tatsächliche Herkunft bzw. Bestimmung der Datenübertragung zu ändern.
- *Zuverlässigkeit*
  Bei vielen Systemen wird es erforderlich sein, sicherzustellen, dass zeitkritische Aufgaben genau zu dem Zeitpunkt durchgeführt werden, zu dem es erforderlich ist, also nicht früher oder später, und es wird sicherzustellen sein, dass zeitunkritische Aufgaben nicht in zeitkritische umgewandelt werden können. Desgleichen wird es bei vielen Systemen erforderlich sein, sicherzustellen, dass ein Zugriff in dem erforderlichen Moment möglich ist und Betriebsmittel nicht unnötig angefordert oder zurückgehalten werden.
- *Übertragungssicherung*
  Dieser Begriff umfasst alle Funktionen, die für den Schutz der Daten während der Übertragung über Kommunikationskanäle vorgesehen sind:
  - Authentisierung
  - Zugriffskontrolle
  - Datenvertraulichkeit
  - Datenintegrität
  - Sende- und Empfangsnachweis

Über die ITSEC hinaus können weitere Sicherheitsanforderungen bestehen, wie etwa Datensicherung, Verschlüsselung gespeicherter Daten, Funktionen zur Wahrung der Datenintegrität oder datenschutzrechtliche Anforderungen.

Stärke der Mechanismen

Common Criteria [Common Criteria] definiert eine Stärke der Funktion (Strength of Function – SOF). Es handelt sich dabei um eine Charakterisierung von Sicherheitsfunktionen des Produkts, die den geringsten angenommenen Aufwand beschreibt, um die zugrunde liegenden Sicherheitsmechanismen durch einen direkten Angriff außer Kraft zu setzen. Es werden drei Stufen über das Angriffspotential definiert:

niedrig:
Die Stufe bietet angemessenen Schutz gegen zufälliges Brechen der Sicherheit durch Angreifer/innen, die über ein geringes Angriffspotential verfügen.

mittel:
Die Stufe bietet einen angemessenen Schutz gegen nahe liegendes oder absichtliches Brechen durch Angreifer/innen, die über ein mittleres Angriffspotential verfügen.

hoch:
Die Stufe bietet einen geeigneten Schutz gegen geplantes oder organisiertes Brechen der EVG-Sicherheit durch Angreifer/innen, die über ein hohes Angriffspotential verfügen.

Ähnlich werden in ITSEC drei Stufen (niedrig, mittel, hoch) für die Stärke des Mechanismus definiert.

ENT 1.3 IT-Sicherheit in Design und Implementierung

Relevanz: Umsetzung/Wartung;

System-Entwurf:

Diese Elementarphase des Entwicklungsprozesses bezieht sich auf die oberste Stufe der Definition und des Entwurfs eines IT-Systems oder Produktes. Dies erfolgt in Form einer Spezifikation auf hohem Abstraktionsniveau, die die grundlegende Struktur des Systems, seine externen Schnittstellen sowie seine Untergliederung in die wichtigsten Hardware- und Softwarekomponenten identifiziert.

Bereits in dieser Elementarphase, in der die Systemarchitektur und ein Integrationsplan erarbeitet werden, ist auf eine adäquate Berücksichtigung der Sicherheitsanforderungen zu achten.

Aus Sicht der IT-Sicherheit ist es insbesondere wichtig, dass bereits im System-Entwurf eine klare und wirksame Trennung zwischen IT-sicherheitsspezifischen, IT-sicherheitsrelevanten und anderen Komponenten getroffen wird. Eine klare Trennung unterstützt die Sicherstellung der Korrektheit der weiteren Entwicklungsschritte und erleichtert eine eventuelle Evaluierung der Sicherheit des Systems (etwa nach [ITSEC] oder [Common Criteria]).

Dabei bedeuten:
- *IT-sicherheitsspezifische Komponenten:*
  Komponenten, die unmittelbar zur Durchsetzung der IT-Sicherheit beitragen
- *IT-sicherheitsrelevante Komponenten:*
  Komponenten, die nicht unmittelbar zur IT-Sicherheit beitragen, deren Fehlverhalten oder Missbrauch jedoch die Sicherheit gefährden kann.

Die Schnittstellen der IT-Sicherheitsmaßnahmen zu den beteiligten Architekturelementen müssen dokumentiert werden.

SW-Grobentwurf und SW-Feinentwurf:

Diese Elementarphasen des Entwicklungsprozesses beziehen sich auf die Verfeinerung des Systementwurfes bis hin zu einem Detaillierungsgrad, der als Basis für die Programmierung (und/oder Hardwarekonstruktion) verwendet werden kann.

Aus Sicht der IT-Sicherheit sind hier insbesondere
- die Abhängigkeiten der IT-Sicherheitsfunktionen,
- die Wechselwirkungen der IT-Sicherheitsmechanismen, die zur Realisierung der IT-Sicherheitsfunktionen gewählt wurden, und
- die Auswirkungen, die die Realisierung der IT-Sicherheitsfunktionen auf andere SW-Einheiten haben können,

zu untersuchen.

Alle Schnittstellen der IT-sicherheitsspezifischen und der IT-sicherheitsrelevanten SW-Komponenten und -Module müssen mit ihrem Zweck und ihren Parametern beschrieben werden. Die Separierung vom nicht IT-sicherheitsrelevanten Teil muss sichtbar sein.

Weiters ist festzustellen, ob und gegebenenfalls welche IT-sicherheitsspezifischen oder IT-sicherheitsrelevanten Anteile in anderen SW-Komponenten, -Modulen bzw. Datenbanken bei der Realisierung entstehen.

Implementierung und Tests:

Jede Komponente bzw. jeder Modul ist zunächst aus den Spezifikationen zu programmieren oder zu konstruieren. Diese Komponenten und Module müssen dann gegen ihre Spezifikationen geprüft und getestet werden. Anschließend werden einzelne Komponenten und Module zusammen in kontrollierter Form integriert, bis das komplette System vorliegt, das dann als Ganzes gegen die Spezifikation und die Sicherheitsvorgaben geprüft und getestet wird (vgl. dazu [IT-BVM], Kap 7, 8 und 9 (Phasen Implementierung, Test und Integration)). Details dazu siehe auch ENT 1.5 Entwicklung eines Testplans für Standardsoftware und ENT 1.6 Testen von Software.

ENT 1.4 Entwicklungsumgebung

Relevanz: Umsetzung/Wartung;

Zur Entwicklungsumgebung zählen Maßnahmen, Verfahren und Standards, die während der Systemerstellung zum Einsatz kommen.

Zur Gewährleistung der Sicherheit des zu entwickelnden Systems sind auch an die Sicherheit der Entwicklungsumgebung besondere Anforderungen zu stellen. Abhängig von den Sicherheitsanforderungen an das System und den Anforderungen in dessen Vertrauenswürdigkeit können dies etwa sein:

Konfigurationskontrolle:

Die Konfigurationskontrolle soll sicherstellen, dass alle Entwurfsergebnisse und Implementierungen in kontrollierter Form erstellt und geändert werden und dass sie nachweislich den früheren Darstellungen entsprechen.

Es ist wichtig, dass alle Versionen eines Systems eindeutig identifiziert werden können (Versionsnummer). In vielen Fällen wird es sinnvoll sein, den Entwicklungsvorgang durch ein Konfigurationskontrollsystem zu unterstützen. Common Criteria fordert etwa einen Konfigurationsmanagement-Plan ab Evaluationsstufe EAL3, automatisiertes Konfigurations-management ab Evaluationsstufe EAL4.

Sicherheit bei der/dem Entwickler/in:

Es ist sicherzustellen, dass die Entwicklung gegen böswillige Angriffe geschützt ist und die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen gewährleistet sind (vgl. dazu §126a zu Datenbeschädigung (StGB), BGBl. Nr. 60/1974 i.d.g.F.).

Dazu ist eine Reihe von organisatorischen, technischen und personellen Maßnahmen erforderlich, die im Detail in anderen Maßnahmenbeschreibungen in diesem Handbuch nachgelesen werden können.

Grundsätzlich zu beachten sind dabei unter anderem:

- Die physische Sicherheit der Räume und Gebäude, in denen die Entwicklung erfolgt (Zutrittskontrolle, Einbruchs- und Brandschutz, ... vgl. Kapitel Bauliche und infrastrukturelle Maßnahmen).
- *Personelle Sicherheit:* Bei der Entwicklung sicherheitsrelevanter bzw. sicherheitsspezifischer Systeme und Komponenten darf nur vertrauenswürdiges Personal zum Einsatz kommen.
- *Sicherheit bei der Übertragung von Informationen und der Übersendung von Datenträgern:* Abhängig von den Vertraulichkeitsanforderungen sind entsprechende Maßnahmen zum Schutz der Informationen zu treffen.
- Sicherstellung der Verfügbarkeit der Ergebnisse (vgl. Abschnitt Disaster Recovery Planung).

Trennung von Entwicklungs- und Produktionsumgebung:

Es ist eine strikte Trennung der Entwicklungs- von der Produktionsumgebung vorzusehen.

Auch die Produktion ist, wie die Entwicklung gegen Angriffe sowohl von Insiderinnen/Insidern als auch von Außentäterinnen/Außentätern zu schützen.

Es empfiehlt sich, die Anforderungen und Maßnahmen zur Gewährleistung der Sicherheit in der Entwicklungsumgebung in einem eigenen Dokument festzuhalten.

ENT 1.5 Entwicklung eines Testplans für Standardsoftware

Sowohl bei der Eigenentwicklung von IT-Systemen als auch beim Einsatz von Produkten (Standardsoftware) sind ausführliche Tests unumgänglich. Während im Rahmen der Eigenentwicklung Tests den gesamten Entwicklungsprozess begleiten (vgl. Regelwerk SE im [IT-BVM]), muss Standard-SW im Rahmen des Auswahlprozesses ausführlich getestet werden.

Vor der Entscheidung für ein geeignetes Standardsoftwareprodukt müssen die nach der Vorauswahl in die engere Wahl gezogenen Produkte als Testlizenz beschafft und ausreichend getestet werden. Die Ergebnisse dieser Tests liefern dann die Grundlage für die Installationsvorschriften und andere Freigabebedingungen.

Die im nachfolgenden beschriebene Vorgehensweise beim Testen orientiert sich an den Standardwerken [ISO/IEC 12119] (”Softwareerzeugnisse, Qualitätsanforderungen und Prüfbestimmungen”), Vorgehensmodell für die Planung und Durchführung von IT-Vorhaben (V-Modell) und dem Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik ([ITSEM]).

Um sicherzugehen, dass das Produkt die gestellten Anforderungen auch im gewünschten Maße erfüllt, sind systematische Tests zur Überprüfung der Eignung und Zuverlässigkeit auf Grundlage des Anforderungskataloges erforderlich.

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

- Eingangsprüfungen (Prüfung auf Viren, Lauffähigkeit in der gewünschten IT-Einsatzumgebung, ...),
- funktionale Tests (Überprüfung der funktionalen Anforderungen),

- Tests weiterer funktionaler Eigenschaften (Überprüfung von Kompatibilität, Performance, Interoperabilität, Konformität mit Regelungen oder Gesetzen, Benutzerfreundlichkeit, Wartbarkeit, Dokumentation) und
- sicherheitsspezifische Tests (Überprüfung der Sicherheitsanforderungen).

Es ist ein Testplan zu erstellen, der folgende Inhalte umfasst:

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

Anforderungen an die Testumgebung:

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

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

ENT 1.6 Testen von Software

Relevanz: Umsetzung/Wartung;

Das Testen von Software lässt sich in die Abschnitte Vorbereitung, Durchführung und Auswertung unterteilen.

In diesen Abschnitten sind folgende Aufgaben wahrzunehmen:

Testvorbereitung:

- Festlegung der Testmethoden für die Einzeltests (Testarten, -verfahren und -werkzeuge)
- Generierung von Testdaten und Testfällen
- Aufbau der benötigten Testumgebung

Testdurchführung:

- Eingangsprüfungen
- Funktionale Tests
- Tests weiterer funktionaler Eigenschaften
- Sicherheitsspezifische Tests
- Pilotanwendung (Einsatz unter Echtbedingungen), falls erforderlich

Testauswertung:

- Bewertung der Testergebnisse anhand festgelegter Entscheidungskriterien
- Zusammenführung der Ergebnisse
- Dokumentation

Sicherheitsspezifische Tests

Aus Sicht der IT-Sicherheit sind insbesondere auch folgende Aspekte zu untersuchen:

- Wirksamkeit und Korrektheit der Sicherheitsfunktionen,
- Stärke der Sicherheitsmechanismen und
- Unumgänglichkeit und Zwangsläufigkeit der Sicherheitsmechanismen.

Als Grundlage für eine Sicherheitsuntersuchung könnte beispielsweise das Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik ([ITSEM]) herangezogen werden, in dem viele der nachfolgend aufgezeigten Vorgehensweisen beschrieben sind. Die weiteren Ausführungen dienen zur Orientierung und zur Einführung in die Thematik.

Zu Beginn muss durch funktionale Tests zunächst nachgewiesen werden, dass das Produkt die erforderlichen Sicherheitsfunktionen bereitstellt.

Anschließend ist zu überprüfen, ob alle erforderlichen Sicherheitsmechanismen im Anforderungskatalog genannt wurden, ggf. ist dieser zu ergänzen.

Zum Testen von Anwendungen die auf die Bürgerkarten-Funktionalität zugreifen, soll auf nicht real existente Testpersonen, die im ZMR für diesen Zweck formell eingerichtet wurden, zurückgegriffen werden [IKTB-220905-01].

Um die Mindeststärke der Mechanismen zu bestätigen oder zu verwerfen, sind Penetrationstests durchzuführen. Diese sind nach allen anderen Tests durchzuführen, da sich aus diesen Tests Hinweise auf potentielle Schwachstellen ergeben können. Durch Penetrationstests kann das Testobjekt oder die Testumgebung beschädigt oder beeinträchtigt werden. Damit solche Schäden keine Auswirkungen haben, sollten vor der Durchführung von Penetrationstests Datensicherungen gemacht werden.

Penetrationstests können durch die Verwendung von Sicherheitskonfigurations- und Protokollierungstools unterstützt werden. Diese Tools untersuchen eine Systemkonfiguration und suchen nach gemeinsamen Schwachstellen wie etwa allgemein lesbaren Dateien und fehlenden Passwörtern.

Mit Penetrationstests soll das Produkt auf Konstruktionsschwachstellen untersucht werden, indem dieselben Methoden angewandt werden, die auch eine/ein potentielle/r Angreifer/in zur Ausnutzung von Schwachstellen benutzen würde, wie z.B.

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

Weiters ist die Stärke der Mechanismen zu überprüfen (vgl. dazu ENT 1.2 Durchführung einer Risikoanalyse).

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

ENT 1.7 Abnahme und Freigabe von Software

Relevanz: Umsetzung/Wartung;

Sowohl Standardsoftware als auch selbst- oder im Auftrag entwickelte Programme müssen einer geregelten Abnahme und Freigabe unterzogen werden (vgl. dazu auch Kap. 9 (Phase Integration) des Regelwerks SE des IT-BVM [IT-BVM]).

In der *Abnahme* sollte überprüft werden, ob die Software

- die erforderliche Funktionalität zuverlässig bereitstellt,
- keine nicht dokumentierten Funktionen enthält,
- frei von Viren ist (insbesondere bei Standardsoftwareprodukten),
- kompatibel zu den anderen eingesetzten Produkten ist,
- in der angestrebten Betriebsumgebung lauffähig ist und welche Parameter zu setzen sind.

Im Falle von Standardsoftware ist darüber hinaus zu prüfen, ob diese komplett einschließlich der erforderlichen Handbücher/Dokumentationen ausgeliefert wurde, für Eigenentwicklungen ist die Vollständigkeit und Korrektheit der Dokumentation zu prüfen. Näheres zu den Anforderungen an die Dokumentation s. ENT 2.1 Dokumentation von Software.

Abnahmeplan:

Üblicherweise werden hierzu Testfälle und die erwarteten Ergebnisse für die Software erarbeitet. Anhand dieser Testfälle wird die Software getestet und der Abgleich zwischen berechnetem und erwartetem Ergebnis wird als Indiz für die Korrektheit der Software benutzt.

Zur Entwicklung der Testfälle und zur Durchführung der Tests ist folgendes zu beachten:

- Die Testfälle werden von der fachlich zuständigen Stelle entwickelt.
- Für Testfälle werden keine Daten des Echtbetriebs benutzt.
- Testdaten, insbesondere wenn sie durch Kopieren der Echtdaten erstellt werden, dürfen keine vertraulichen Informationen beinhalten; personenbezogene Daten sind zu anonymisieren oder zu simulieren.
- Die Durchführung der Tests darf keine Auswirkungen auf den Echtbetrieb haben. Nach Möglichkeit sollte ein logisch oder physikalisch isolierter Testrechner benutzt werden.

Eine Abnahme ist zu verweigern, wenn

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

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

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

Freigabe:

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

Die Freigabeerklärung sollte umfassen:

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

Falls IT-technisch möglich, muss verhindert werden, dass Software nach der Freigabe verändert oder manipuliert werden kann (s. ENT 1.9 Sicherstellen der Integrität von Software). Andernfalls ist dies durch eine Regelung festzulegen.

Auch nach intensiven Abnahmetests kann es vorkommen, dass im laufenden Einsatz Fehler in der Software festgestellt werden. Für diesen Fall sind detaillierte Verfahrensweisen festzulegen (Ansprechpartner/in, Fehlerbeseitigungsablauf, Beteiligung der fachlich zuständigen Stelle, Wiederholung der Abnahme und Freigabe, Versionskontrolle).

ENT 1.8 Installation und Konfiguration von Software

Relevanz: Umsetzung/Wartung; Anwender/innen;

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

Abweichungen von der Installationsanweisung bedürfen der Zustimmung der Freigabeinstanz.

Wenn die Benutzer/innen die Software selbst installieren sollen, muss ihnen eine Installationsanweisung zur Verfügung gestellt werden, die eine selbständige Installation ermöglicht. Mindestens die Pilot-Installation durch eine/einen ausgewählte/n typische/n Benutzer/in sollte durch die IT-Abteilung begleitet werden, um die Verständlichkeit der Installationsanweisung zu überprüfen.

Sowohl vor als auch nach der Installation von Software sollte eine vollständige Datensicherung durchgeführt werden. Die erste Datensicherung kann bei nachfolgenden Problemen während der Installation zur Wiederherstellung eines konsolidierten Aufsetzpunktes verwendet werden. Nach der erfolgreichen Installation sollte erneut eine vollständige Datensicherung durchgeführt werden, damit bei späteren Problemen wieder auf den Zustand nach der erfolgreichen Installation des Produktes aufgesetzt werden kann.

Die erfolgreiche Installation wird schriftlich an die für die Aufnahme des Produktionsbetriebes zuständige Stelle gemeldet.

ENT 1.9 Sicherstellen der Integrität von Software

Relevanz: Umsetzung/Wartung;

Es ist sicherzustellen, dass die freigegebene Software nur unverändert installiert werden kann. Damit soll verhindert werden, dass zwischenzeitlich gewollte oder ungewollte Veränderungen vorgenommen werden können, z.B. durch Viren, Bit-Fehler aufgrund technischer Fehler oder Manipulationen in Konfigurationsdateien.

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

Von den Originaldatenträgern sollten, falls der Datenumfang es zulässt, Sicherungskopien angefertigt werden. Originaldatenträger und alle Kopien müssen vor unberechtigtem Zugriff geschützt aufbewahrt werden. Die angefertigten Kopien sollten nummeriert und in Bestandsverzeichnisse aufgenommen werden. Kopien, die nicht mehr benötigt werden, sind zu löschen.

Vor der Installation muss eine Virenprüfung durchgeführt werden.

Optional kann über die Originaldatenträger oder über eine während des Tests installierte Referenzversion eine Checksumme (vgl. Kap. Kryptographische Maßnahmen) gebildet werden, anhand derer vor der Installation die Integrität der dafür eingesetzten Datenträger bzw. der in lokalen Netzen hinterlegten Versionen überprüft werden kann. Darüber hinaus können installierte Programme zum Schutz vor unberechtigten Veränderungen der freigegebenen Konfiguration zusätzlich mit Checksummen versehen werden. Dies ermöglicht es auch, Infektionen mit bisher unbekannten Viren zu erkennen und festzustellen, ob eine Vireninfektion vor oder nach der Installation stattgefunden hat.

ENT 1.10 Lizenzverwaltung und Versionskontrolle von Standardsoftware

Relevanz: Umsetzung/Wartung; Anwender/innen;

Ohne eine geeignete Versionskontrolle und Lizenzkontrolle kommt es erfahrungsgemäß schnell zur Verwendung verschiedenster Versionen auf einem IT-System oder innerhalb einer Organisationseinheit, von denen evtl. einige ohne Lizenz benutzt werden.

Auf allen IT-Systemen einer Institution darf ausschließlich lizenzierte Software eingesetzt werden. Diese Regelung muss allen Mitarbeiterinnen/Mitarbeitern bekannt gemacht werden, die Administratoren der verschiedenen IT-Systeme müssen sicherstellen, dass nur lizenzierte Software eingesetzt wird. Dafür müssen sie mit geeigneten Werkzeugen zur Lizenzkontrolle ausgestattet werden.

Häufig werden in einer Institution verschiedene Versionen einer Standardsoftware eingesetzt. Im Rahmen der Lizenzkontrolle muss es auch möglich sein, einen Überblick über alle eingesetzten Versionen zu erhalten. Damit kann gewährleistet werden, dass alte Versionen durch neuere ersetzt werden, sobald dies notwendig ist, und dass bei der Rückgabe von Lizenzen alle Versionen gelöscht werden.

ENT 1.11 Deinstallation von Software

Relevanz: Umsetzung/Wartung; Anwender/innen;

Bei der Deinstallation von Software müssen alle Dateien entfernt werden, die für den Betrieb der Software auf dem IT-System angelegt worden sind, und alle Einträge in Systemdateien, die bezüglich dieser Software vorgenommen wurden, gelöscht werden. Bei vielen Softwareprodukten werden während der Installation in diversen Verzeichnissen auf dem IT-System Dateien angelegt oder bestehende Dateien verändert.

Um eine vollständige Deinstallation durchführen zu können, ist es daher hilfreich, die bei der Installation durchgeführten Systemänderungen festzuhalten, entweder manuell oder mit Hilfe von speziellen Tools. Wird dies nicht vorgenommen, kommt es erfahrungsgemäß dazu, dass eine

Deinstallation nur rudimentär stattfindet oder dass sie unterlassen wird aus Furcht, wichtige Dateien bei der Deinstallation zu löschen.

Weiters sollte sichergestellt werden, dass bei einer Deinstallation auch alle Vorgängerversionen vollständig deinstalliert werden.

4.2 Dokumentation

Relevanz: Umsetzung/Wartung;

Die im Folgenden angeführten Maßnahmen geben grobe Richtlinien zu den Anforderungen an die Dokumentation. Dabei wird insbesondere auf die sicherheitsspezifischen Fragen im Rahmen der Dokumentation eingegangen. Die Ausführungen orientieren sich an den [AVB-IT], den [IT-BVM] sowie den [ITSEC]. In den genannten Dokumenten finden sich auch weitere Details.

ENT 2.1 Dokumentation von Software

Relevanz: Umsetzung/Wartung;

Für jede Softwarekomponente ist die Verfügbarkeit der zu ihrer Nutzung erforderlichen und/oder zweckmäßigen Dokumentation sicherzustellen.

Dabei ist zu achten auf:

- die Vollständigkeit und Korrektheit der gelieferten Dokumentation und
- die laufende Aktualisierung der Dokumentation während der gesamten Nutzungsdauer der Software.

Die Dokumentation muss zumindest beinhalten:

- Benutzerdokumentation
- Dokumentation für Installation und Administration

Darüber hinaus können je nach Bedarf folgende Anforderungen bestehen:

- technische Dokumentation
- Entwicklungsdokumentation

Benutzerdokumentation:

Bei der Benutzerdokumentation (in den [IT-BVM] als "Anwendungshandbuch" bezeichnet) handelt es sich um Information über die Software, die die/der Entwickler/in der/dem Benutzer/in zur Verwendung bereitstellt.

Die Benutzerdokumentation hat alle für die laufende Arbeit notwendigen Abläufe so zu beschreiben, dass sie für eine eingeschulte Person verständlich sind. Daneben hat die Dokumentation typische und vorhersehbare Fehlersituationen und deren Behebung zu beschreiben.

Aus sicherheitstechnischer Sicht soll die Benutzerdokumentation der/dem Endbenutzer/in helfen,

- die Sicherheitseigenschaften der Software sowie
- den Beitrag der/des Endbenutzerin/Endbenutzers zur Gewährleistung der Sicherheit bei der Verwendung der Software

zu verstehen.

Die Benutzerdokumentation sollte in deutscher Sprache vorliegen. Dies kann und sollte auch vertraglich festgelegt werden (vgl. etwa AVB-IT [AVB-IT]).

Ebenso empfiehlt sich eine Vereinbarung über die Lieferung der Dokumentation zusätzlich in maschinenlesbarer Form, so dass diese an definierten Arbeitsplätzen während der Arbeit abgerufen werden kann.

Dokumentation für Installation und Administration:

Bei dieser Dokumentation handelt es sich um Information über die erforderlichen Maßnahmen zur Aufnahme des Betriebs, zur Durchführung und Überwachung des Betriebs und zur Unterbrechung und Beendigung des Betriebs. Sie soll Administratoren helfen, die Software in einer sicheren Art und Weise zu installieren, zu konfigurieren und zu bedienen.

Die Dokumentation für die Installation und Administration (im Folgenden kurz als "Administratordokumentation", in den [IT-BVM] als "Betriebshandbuch" bezeichnet) hat alle für die Installation und die laufende Verwaltung des Systems notwendigen Abläufe so zu beschreiben, dass sie für eine eingeschulte Person verständlich sind. Daneben hat die Dokumentation typische und vorhersehbare Fehlersituationen und deren Behebung zu beschreiben.

Aus sicherheitstechnischer Sicht muss die Administratordokumentation die sicherheitsspezifischen Funktionen darlegen, die für Administratoren von Bedeutung sind. Darüber hinaus muss sie Richtlinien zur konsistenten und wirksamen Nutzung der Sicherheitseigenschaften der Software enthalten und darlegen, wie solche Eigenschaften zusammenwirken.

Technische Dokumentation:

Diese muss den zum Zeitpunkt der Installation der Software üblichen Standards entsprechen und so gestaltet sein, dass sie für eine/einen mit ähnlichen Komponenten vertraute/n Expertin/Experten verständlich und verwertbar ist.

ENT 2.2 Sourcecodehinterlegung

Relevanz: Umsetzung/Wartung;

Im Falle einer Lieferung von Software, bei der der Sourcecode nicht mitgeliefert wird, sollte nach Möglichkeit - insbesondere bei der Entwicklung von Individualsoftware - Sourcecodehinterlegung vereinbart werden.

Diese soll die Möglichkeit einer weiteren Fehlerbehebung, Änderung und Wartung von Software für den Fall der Handlungsunfähigkeit des Softwareherstellers und den Fall der Einstellung der Weiterentwicklung oder Wartung sicherstellen.

Durchführung:

Die/Der Auftragnehmer/in (SW-Hersteller) stellt die Software auf einem Datenträger, der auf dem System der/des Auftraggeberin/Auftraggebers gelesen werden kann, in der Quellensprache bereit, übersetzt sie in Maschinencode und nimmt die Installation auf dem System vor.

Nach der Installation wird der Datenträger mit dem Quellencode samt der dazugehörigen Dokumentation (Inhalt und Aufbau des Datenträgers, Programm und Datenflusspläne, Testverfahren, Testprogramme, Fehlerbehandlung usw.) von der/dem Auftragnehmer/in versiegelt und bei der/dem Auftraggeber/in oder einer/einem vertrauenswürdigen Dritten (z.B. Notar/in) hinterlegt.

Tritt beim Hersteller Handlungsunfähigkeit (etwa Liquidation, Eröffnung eines Konkursverfahrens, ...) ein oder stellt sie/er entgegen anders lautenden Vereinbarungen die Weiterentwicklung und/oder Wartung der Software ein, so ist die/der Auftraggeber/in berechtigt, die hinterlegten Datenträger zu entnehmen und entweder ein sachkundiges Unternehmen mit den erforderlichen weiteren Arbeiten (Wartung, Fehlerbehebung, ...) zu beauftragen oder diese selbst durchzuführen.

Dabei ist zu beachten:

- Der Datenträger muss die Software in den ursprünglichen Programmiersprachen zum Zeitpunkt der Installation einschließlich aller seitherigen Änderungen enthalten.
- Der Datenträger muss die in maschinenlesbarer Form vorliegende Dokumentation enthalten.
- Es ist eine Aufstellung der versiegelt hinterlegten Gegenstände sowie eine Anweisung über die Handhabung des Datenträgers und die Installation der Software beizulegen.
- Die Hinterlegung muss bei jeder Lieferung einer neuen Version wiederholt werden, auf die Aktualität aller Komponenten sowie der Dokumentation ist zu achten.

Ein Vorschlag zur Formulierung einer entsprechenden vertraglichen Vereinbarung findet sich in den AVB-IT [AVB-IT] (s. Anhang B: Referenzdokumente und Anhang C.1 Sourcecode-hinterlegung (Muster, aus AVB-IT)).

ENT 2.3 Dokumentation der Systemkonfiguration

Relevanz: Umsetzung/Wartung;

Planung, Steuerung, Kontrolle und Notfallvorsorge des IT-Einsatzes basieren auf einer aktuellen Dokumentation des vorhandenen IT-Systems. Nur eine aktuelle Dokumentation der Systemkonfiguration ermöglicht im Notfall einen geordneten Wiederanlauf des IT-Systems.

Bei einem Netzbetrieb sind sowohl die physikalische Netzstruktur (vgl. ENT 2.4 Dokumentation und Kennzeichnung der Verkabelung) als auch die logische Netzkonfiguration zu dokumentieren. Dazu gehören auch die Zugriffsrechte der einzelnen Benutzer/innen (siehe SYS 1.3 Einrichtung und Dokumentation der zugelassenen Benutzer/innen und Rechteprofile) und der Stand der Datensicherung.

Dabei ist zu beachten:

- Die Dokumentation muss aktuell und verständlich sein, damit auch eine/ein Vertreter/in die Administration jederzeit weiterführen kann. Dies gilt insbesondere für Änderungen an Systemverzeichnissen und -dateien.
- Bei Installation neuer Betriebssysteme oder bei Updates sind die vorgenommenen Änderungen besonders sorgfältig zu dokumentieren. Möglicherweise kann durch die Aktivierung neuer oder durch die Änderung bestehender Systemparameter das Verhalten des IT-Systems (insbesondere auch von Sicherheitsfunktionen) maßgeblich verändert werden.
- Um das Vertrauen in Betriebssysteme zu sichern, ist generell eine so genannte Vertrauenseinstellung im Zuge der Neuinstallation/-konfiguration vorzunehmen. Speziell im Bundesbereich ist gemäß [IKTB-170902-7] eine definierte sichere Initialkonfiguration zu verwenden. Deren Anwendung ist allerdings auch generell zu empfehlen. Eine entsprechend dokumentierte Initialkonfiguration wird im Rahmen des Online-Angebotes des Chief Information Office des Bundes zur Verfügung stehen. In diesem Zusammenhang: siehe auch SYS 5.8 Sichere Initialkonfiguration und Zertifikatsgrundeinstellung.
- Die Unterlagen sind gesichert aufzubewahren, so dass ihre Verfügbarkeit im Bedarfsfall gewährleistet ist.

ENT 2.4 Dokumentation und Kennzeichnung der Verkabelung

Relevanz: Umsetzung/Wartung;

Für Wartung, Fehlersuche, Instandsetzung und für erfolgreiche Überprüfung der Verkabelung ist eine gute Dokumentation und eindeutige Kennzeichnung aller Kabel erforderlich. Die Güte dieser Revisionsdokumentation ist abhängig von der Vollständigkeit, der Aktualität und der Lesbarkeit.

In dieser Dokumentation (auch Bestandsplan genannt) sind *alle* das Netz betreffenden Sachverhalte aufzunehmen:

- genauer Kabeltyp,
- nutzungsorientierte Kabelkennzeichnung,
- Standorte von Zentralen und Verteilern mit genauen Bezeichnungen,
- genaue Führung von Kabeln und Trassen in der Liegenschaft (Einzeichnung in bemaßte Grundriss- und Lagepläne),
- Trassendimensionierung und -belegung,
- Belegungspläne aller Rangierungen und Verteiler,
- Nutzung aller Leitungen, Nennung der daran angeschlossenen Netzteilnehmer/innen,
- technische Daten von Anschlusspunkten,
- Gefahrenpunkte,
- vorhandene und zu prüfende Schutzmaßnahmen.

Es muss möglich sein, sich anhand dieser Dokumentation einfach und schnell ein genaues Bild über die Verkabelung zu machen.

Da es mit zunehmender Größe eines Netzes nicht möglich ist, alle Informationen in einem Plan unterzubringen, ist eine Aufteilung der Informationen sinnvoll. Tatsächliche Lageinformationen sind immer in maßstäbliche Pläne einzuzeichnen, andere Informationen können in Tabellenform geführt werden. Wichtig dabei ist eine eindeutige Zuordnung aller Angaben untereinander.

Um die Aktualität der Dokumentation zu gewährleisten, ist sicherzustellen, dass alle Arbeiten am Netz rechtzeitig und vollständig derjenigen/demjenigen bekannt werden, die/der die Dokumentation führt. Es ist z.B. denkbar, die Ausgabe von Material, die Vergabe von Fremdaufträgen oder die Freigabe gesicherter Bereiche von der Mitzeichnung dieser Person abhängig zu machen.

Da diese Dokumentation schutzwürdige Informationen beinhaltet, ist sie sicher aufzubewahren und der Zugriff darauf zu regeln.

Vgl. dazu auch INF 4.1 Lagepläne der Versorgungsleitungen

ENT 2.5 Neutrale Dokumentation in den Verteilern

Relevanz: Umsetzung/Wartung;

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

Es ist auf Aktualität, Vollständigkeit und Korrektheit dieser Information zu achten.

ENT 2.6 Dokumentation der Datensicherung

Relevanz: Umsetzung/Wartung;

In einem Datensicherungskonzept muss festgelegt werden, wie die Dokumentation der Datensicherung zu erfolgen hat (vgl. Kap. Datensicherung).

Zur Gewährleistung einer ordnungsgemäßen und funktionierenden Datensicherung ist eine Dokumentation erforderlich, die für jedes IT-System zumindest folgendes umfassen soll:

- das Datum der Datensicherung,
- der Datensicherungsumfang (welche Dateien/Verzeichnisse wurden gesichert),
- der Datenträger, auf dem die Daten im operativen Betrieb gespeichert sind,
- der Datenträger, auf dem die Daten gesichert wurden,
- die für die Datensicherung eingesetzte Hard- und Software (mit Versionsnummer) und
- die bei der Datensicherung gewählten Parameter (Art der Datensicherung usw.).

Darüber hinaus bedarf es einer Beschreibung der Vorgehensweise, die einer/einem sachverständigen Dritten eine Wiederherstellung eines Datensicherungsbestandes erlaubt. Auch hier muss eine Beschreibung der erforderlichen Hard- und Software, der benötigten Parameter und der Vorgehensweise, nach der die Datenrekonstruktion zu erfolgen hat, erstellt werden.

4.3 Evaluierung und Zertifizierung

Relevanz: Management; Umsetzung/Wartung;

ENT 3.1 Beachtung des Beitrags der Zertifizierung für die Beschaffung

Relevanz: Management; Umsetzung/Wartung;

Die Benutzer/innen von IT-Systemen müssen sich auf die Sicherheit des von ihnen verwendeten Systems verlassen können. Sie benötigen auch einen Maßstab für den Vergleich der Sicherheitseigenschaften von IT-Produkten, deren Anschaffung sie in Betracht ziehen. Neben der Durchführung eigener eingehender Tests oder dem Vertrauen in die Aussagen des Herstellers bzw. Vertreibers wird zunehmend auf die Möglichkeit einer Prüfung und Bewertung durch eine neutrale, vertrauenswürdige Instanz zurückgegriffen. Insbesondere bei einem hohen oder sehr hohen Schutzbedarf kann die Vertrauenswürdigkeit der Produkte in Hinblick auf IT-Sicherheit nur dadurch gewährleistet werden, dass unabhängige Prüfstellen die Produkte untersuchen und bewerten.

Eine solche Evaluation von Systemen oder Produkten erfordert objektive und genau definierte Kriterien für die Bewertung der Sicherheit und das Vorhandensein einer Zertifizierungsstelle, die bestätigen kann, dass die Evaluation ordnungsgemäß durchgeführt wurde.

Eine allgemein anerkannte Grundlage dieser Evaluierungen bilden die europaweit harmonisierten "Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC)" [ITSEC] und das zugehörige Evaluationshandbuch [ITSEM] sowie die weltweit abgestimmten "Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik" (Common Criteria 2.0) [Common Criteria].

Aus einem nach der Evaluierung erstellten Zertifizierungsreport geht hervor, welche Funktionalität mit welcher Prüftiefe untersucht wurde und welche Bewertung vorgenommen wurde. Zusätzlich wird die geprüfte Mechanismenstärke der Implementation der Sicherheitsfunktionen angegeben, die ein Maß darstellt für den Aufwand, den man zum Überwinden der Sicherheitsfunktionen aufbringen muss.

[ITSEC] kennt etwa die Evaluationsstufen E1 (geringste Prüftiefe) bis E6 (höchste Prüftiefe) und unterscheidet die Mechanismenstärken niedrig, mittel und hoch. Die Common Criteria 2.0 [Common Criteria] unterscheiden sieben Vertrauenswürdigkeitsstufen (EAL1 bis EAL7), wobei EAL1 unter E1 anzusetzen ist, um den Zugang zur Evaluation zu erleichtern.

Darüber hinaus werden Hinweise gegeben, welche Randbedingungen beim Einsatz eines Produktes beachtet werden müssen.

In Österreich wurde gemäß dem IKT-Board-Beschluss vom 25.06.2002 [IKTB-250602-2] das so genannte *österreichische E-Government-Gütesiegel* geschaffen, damit Anwender/innen mit dessen Hilfe einfach und schnell erkennen können, ob ein Produkt, eine Webseite oder eine Transaktion hinreichend sicher und qualitativ hochwertig gemäß den Richtlinien des Gütesiegels ist.

Das Gütesiegel wird an Behörden und Organisationen vergeben, deren Online-Verfahren den technischen E-Government-Kriterien entsprechen und an Produkte, die diese erfüllen. Träger/innen

des Gütesiegels müssen sich verpflichten, ihre ausgezeichneten Verfahren und Produkte auch in Zukunft an die jeweils gültigen technischen Kriterien und Qualitätsmerkmale anzupassen.

Für die Vergabe des E-Government-Gütesiegel sind die notwendigen Voraussetzungen zu überprüfen. Diese werden regelmäßig in den IKT-Board-Beschlüssen den aktuellen Anforderungen angepasst [IKTB-090204-01].

Stehen bei der IT-Beschaffung mehrere Produkte mit angemessenem Preis-/Leistungsverhältnis zur Auswahl, so kann ein eventuell vorhandenes Sicherheitszertifikat bzw. Gütesiegel als Auswahlkriterium positiv berücksichtigt werden [IKTB-090204-02].

5 Systemsicherheit

5.1 Berechtigungssysteme, Schlüssel- und Passwortverwaltung

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

Durch organisatorische und technische Vorkehrungen ist sicherzustellen, dass der Zugriff zu IT-Systemen, Netzwerken, Programmen und Daten nur berechtigten Personen oder Prozessen und nur im Rahmen der festgelegten Regeln möglich ist.

SYS 1.1 Grundsätzliche Festlegungen zur Rechteverwaltung

Relevanz: Umsetzung/Wartung;

Folgende grundsätzliche Festlegungen zur Rechteverwaltung in einem IT-System sollten - vorzugsweise im Rahmen der IT-Systemsicherheitspolitik - getroffen werden (”Zugriffskontroll-politik”):

- welche Subjekte (z.B. Personen, Programme, Prozesse, ...) und welche Objekte (z.B. IT-Anwendungen, Daten, ...) unterliegen der Rechteverwaltung,
- welche Arten von Rechten (z.B. Lesen, Schreiben, Ausführen, ...) können zwischen Subjekten und Objekten existieren,
- wer darf Rechte einsehen, vergeben bzw. ändern,
- welche Regeln müssen bei Vergabe bzw. Änderung eingehalten werden (Authentisierung, ev. 4-Augen-Prinzip),
- welche Rollen müssen durch die Rechteverwaltung definiert werden (z.B. Administrator, Revision, Benutzer/innen,..),
- welche Rollen sind miteinander unvereinbar (z.B. Benutzer/in und Revision, Administrator und Auditor,..),
- wie erfolgen Identifikation und Authentisierung.

Die Rechteverwaltung muss vollständig, widerspruchsfrei und überschaubar sein.

Umgesetzt werden die Zugriffsrechte durch die Rechteverwaltung des IT-Systems.

Definition von Rollen:

Viele IT-Systeme lassen es zu, Rollen zu definieren, denen bestimmte Rechte zugeordnet werden. Solche Rollen können etwa sein: Administrator, Datensicherer/in, Datenerfasser/in oder Sachbearbeiter/innen.

SYS 1.2 Vergabe und Verwaltung von Zugriffsrechten

Relevanz: Umsetzung/Wartung; Anwender/innen;

Die Vergabe und Verwaltung von Zugriffsrechten wird in hohem Maße vom spezifischen IT-System, den darauf durchgeführten Aufgaben sowie der betroffenen Organisation abhängig sein.

Es gibt jedoch einige Grundregeln, deren Einhaltung generell empfohlen wird:

- Die Rechteverwaltung darf nur durch eine/n Berechtigte/n und nur im Rahmen der in der Zugriffskontrollpolitik festgelegten Regeln durchgeführt werden.
- Grundsätzlich sollten immer nur so viele Zugriffsrechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist (”Need-to-know-Prinzip”).
- Jede/r Benutzer/in soll ihre/seine Rechte innerhalb einer Anwendung einsehen können, ebenso jede/r Verantwortliche für seinen Bereich.
- Personelle und aufgabenbezogene Änderungen müssen innerhalb der Rechteverwaltung unverzüglich berücksichtigt werden.
- Es muss ein geregeltes Verfahren für den temporären Entzug von Zugriffsrechten (z.B. bei Urlaub, Karenz, ...) bestehen.
- Bei Ausscheiden einer Mitarbeiterin bzw. eines Mitarbeiters sind deren/dessen Kennung und die zugehörigen Rechte unverzüglich zu deaktivieren bzw. zu löschen.
- Nicht mehr aktive Benutzerkennungen dürfen nicht für Nachfolger/innen reaktiviert werden.
- Zusätzlich sollte in definierten Abständen eine Suche nach “toten Benutzerkennungen”, also Kennungen, die seit einem längeren, systembezogen zu definierenden Zeitraum nicht benutzt wurden, vorgesehen sein.

SYS 1.3 Einrichtung und Dokumentation der zugelassenen Benutzer/innen und Rechteprofile

Relevanz: Umsetzung/Wartung;

Regelungen für die Einrichtung von Benutzer/innen bzw. Benutzergruppen bilden die Voraussetzung für eine angemessene Vergabe von Zugriffsrechten und für die Sicherstellung eines geordneten und überwachbaren Betriebsablaufs.

Es sollte ein Formblatt existieren, um von jedem/jeder Benutzer/in bzw. für jede Benutzergruppe zunächst die erforderlichen Daten zu erfassen, z.B.:

- Name, Vorname, eindeutige Identifikation zumindest des jeweiligen Berechtigungssystems
- Vorschlag für die Benutzer/innen- bzw. Gruppenkennung, wenn diese nicht durch Konventionen vorgegeben sind,
- Organisationseinheit,
- Erreichbarkeit (z.B. Telefon, Raum),
- ggf. Projekt,
- ggf. Angaben über die geplante Tätigkeit im System und die dazu erforderlichen Rechte sowie die Dauer der Tätigkeit,
- ggf. Restriktionen auf Zeiten, Endgeräte, Plattenvolumen, Zugriffsberechtigungen (für bestimmte Verzeichnisse, Remote-Zugriffe, etc.), eingeschränkte Benutzerumgebung,
- ggf. Zustimmung von Vorgesetzten.

Ein Passwort, das einem/einer neuen Benutzer/in für die erstmalige Systemnutzung mitgeteilt wird, muss danach gewechselt werden (s. auch SYS 1.5 Regelungen des Passwortgebrauches). Dies sollte vom System initiiert werden.

Es ist sinnvoll, Namenskonventionen für Benutzer- und Gruppennamen festzulegen, wie zum Beispiel eine Kombination aus Vor- und Nachnamen (z.B. vorname.nachname) oder eigene Benutzer-IDs (z.B. Kürzel Organisationseinheit plus lfd. Nummer).

Anonymisierte bzw. generische Benutzerkennungen sind nur bei unbedenklichen Inhalten, die jedoch nicht öffentlich, sondern einem eingeschränkten Benutzerkreis zugänglich sein sollen, zulässig.

Für sensible IT-Systeme bzw. Anwendungen, bei denen personenbezogene Zugriffssicherheit erforderlich ist, muss jedem/jeder Benutzer/in eine eigene Benutzerkennung zugeordnet sein, es dürfen nicht mehrere Benutzer/innen unter derselben Kennung arbeiten.

Dokumentation:

Die Dokumentation dient der Übersicht über die zugelassenen Benutzer/innen, Benutzergruppen und Rechteprofile und ist Voraussetzung für Kontrollen.

Dokumentiert werden sollen insbesondere

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

Bei all diesen Aufzeichnungen ist auf Aktualität und Vollständigkeit zu achten.

SYS 1.4 Wahl geeigneter Mittel zur Authentisierung

Relevanz: Management; Umsetzung/Wartung;

Während unter Identifikation die Bestimmung der Identität eines Subjektes bzw. Objektes zu verstehen ist (meist durch Angabe eines Namens oder einer User-ID), versteht man unter Authentisierung den Nachweis der angegebenen Identität.

Die Wahl eines geeigneten Authentisierungsverfahrens ist von entscheidender Bedeutung für die Sicherheit des Gesamtsystems und muss daher den Sicherheitsanforderungen und den technischen Möglichkeiten gemäß getroffen werden.

Grundsätzlich gibt es 3 Arten der Authentisierung:

- Authentisierung durch Wissen: etwa durch Eingabe von Passwörtern, Codes, kryptographischen Schlüsseln
- Authentisierung durch Besitz: beispielsweise von Schlüsseln oder Karten
- Authentisierung durch Eigenschaften oder Verhaltensmerkmale (biometrische Verfahren): z.B. Unterschriftendynamik, Stimmerkennung, Fingerabdruck, ...

Die Sicherheit der einzelnen Authentisierungsverfahren ist sehr unterschiedlich und im Einzelfall immer zu hinterfragen. In vielen Fällen kommen Kombinationen der drei angeführten Prinzipien (etwa Authentisierung durch Wissen und Besitz) zur Anwendung.

Im Bereich der öffentlichen Verwaltung wird die Verwendung von so genannten Dienstkarten, gemäß der Empfehlung des IKT-Boards [IKTB-140102-1], zur Identifikation bzw. Authentisierung vorzusehen sein.

Darüber hinaus ist generell zu prüfen, ob bei Verfahren der öffentlichen Verwaltung, das gemäß dem IKT-Board Beschluss festgelegte Konzept Bürgerkarte zur Authentisierung von Benutzerinnen/Benutzern anzuwenden ist. Weiters besteht die Möglichkeit, in Verbindung mit der Bürgerkarte so genannte Single Sign-On Funktionalitäten zu realisieren.

Für die Signatur und die Identifikation wird empfohlen die Module für Onlineverfahren (MOA-ID, MOA-SS/SP) zu verwenden [IKTB-161203-01]. Diese Module stehen auch der Wirtschaft frei zur Verfügung [IKTB-110504-1]. Gemäß dem IKT-Board Beschluss [IKTB-260701-1] soll sogar anstelle eines konventionellen Sigle-Sign-On die Identifikation mit der Bürgerkarte, unter Verwendung geeigneter Basisdienste, treten.

Nach der Auswahl eines geeigneten Authentisierungsverfahrens sind Regelungen über die Handhabung der Authentifikationsmitteln zu treffen (vgl. dazu auch SYS 1.5 „Regelungen des Passwortgebrauches“ und SYS 1.6 „Regelungen des Gebrauchs von Chipkarten“).

Biometrie:

In der Diskussion um Mittel der Authentifikation rückt auch Biometrie zunehmend in den Mittelpunkt. Biometrie kann allerdings noch nicht in allen Bereichen der Identifikation und Authentifikation – im Speziellen im Sinne eines authentischen Identitätsnachweises - als technisches Mittel der Wahl angesehen werden.

Die Stabsstelle IKT-Strategie des Bundes hat im Rahmen des IKT-Board Beschlusses [IKTB-110903-10], besonders im Hinblick auf den Einsatz der Biometrie in Bereichen der öffentlichen Verwaltung, die folgenden allgemeinen Umsetzungsrichtlinien beschlossen:

- Eine hohe Funktionsstärke (SOF high) ist derzeit und in absehbarer Zukunft nicht erreichbar, daher ist vorerst nur limitierter Einsatz der Biometrie möglich.
- Standards für biometrische Merkmale, die eine dauerhafte (etwa 10-jährige) Sicherheit gewährleisten, sind noch nicht vorhanden, daher können zentrale Datenbanken nicht sinnvoll eingesetzt werden.
- Die Identifikationsanwendung außerhalb der erkennungsdienstlichen Aufgaben ist noch nicht technologisch rechtfertigbar.
- Anwendungen können im Bereich der Verifikation und der Komfortsteigerung einen wesentlichen Beitrag leisten. Verifikationsanwendungen mit biometrischen Daten unter Kontrolle des Inhabers/der Inhaberin und mit amtlicher Bestätigung (Signatur) zur breiten Anwendung sind derzeit möglich und können eingesetzt werden. Dies gilt auch für Anwendungen mit Identifikationszuordnung in beschränkten Gruppen (im Normalfall etwa bis zu 100 Personen).
- Anwendungen müssen zurzeit in kontrollierter Umgebung ablaufen. Der Machtgeber für das Identifikationsobjekt (z.B. Computer, Daten, etc.) muss die Möglichkeit der Kontrolle des Verifikationsprozesses haben.

Derzeit praktikable Anwendungen für Biometrie sind z.B.:

- Personendokumente mit biometrischen Daten auf dem Dokument, die durch die Behörde bestätigt (signiert) sind.
- Zuordnung von Chipkarten zu Personen (dies ist vom Willensakt der Auslösung einer Funktion zu trennen, da Wachzustand und Bewusstsein zurzeit in biometrischen Systemen nicht mit vertretbarem Aufwand technisch kontrollierbar sind).
- Zutrittskontrolle zu Anlagen und Räumen vor allem über Sekundärmechanismen (z.B. biometrisches Merkmal und Karte als Träger der Referenzdaten) oder in beschränkten Populationen.

SYS 1.5 Regelungen des Passwortgebrauches

Relevanz: Umsetzung/Wartung; Anwender/innen;

Erfolgt die Authentisierung in einem IT-System über Passwörter, so ist die Sicherheit der Zugriffsrechteverwaltung des Systems entscheidend davon abhängig, dass das Passwort korrekt gewählt und verwendet wird. Dafür ist es empfehlenswert, eine Regelung zum Passwortgebrauch einzuführen, die Benutzer/innen diesbezüglich zu unterweisen und die Einhaltung zu kontrollieren.

Regelungen zum Passwortgebrauch sind in hohem Maße abhängig vom betroffenen IT-System, dem Schutzbedarf der darauf laufenden Anwendungen bzw. der gespeicherten Daten sowie den auf dem System realisierten technischen Möglichkeiten.

Im Folgenden werden jedoch einige Grundregeln gegeben, die eine Art *Mindeststandard für die Wahl und die Handhabung von Passwörtern* darstellen. Für Benutzer/innen mit umfangreichen Rechten, wie etwa Administratoren, bzw. in Bereichen, in denen mit streng vertraulichen Informationen gearbeitet wird, werden die Anforderungen im Allgemeinen höher liegen.

- Das Passwort sollte mindestens 6 Zeichen lang sein.
- Es ist zu prüfen, ob das Berechtigungssystem alle Stellen des Passwortes oder nur Teile davon überprüft.
- Innerhalb des Passwortes sollte mindestens ein Zeichen verwendet werden, das kein Buchstabe ist (Sonderzeichen oder Zahl).
- Passwörter mit spezieller, von Außenstehenden leicht zu erratender Bedeutung, wie Namen, Geburtsdaten, Firmen- oder Abteilungsbezeichnungen, Kfz-Kennzeichen, etc. sind ebenso zu vermeiden wie Standardausdrücke wie TEST, SYSTEM und Tastatur- und Zeichenmuster, wie ABCDEF, QWERTZ, 123456, etc.
- Voreingestellte Passwörter (z.B. des Herstellers bei Auslieferung von Systemen) müssen umgehend durch individuelle Passwörter ersetzt werden. Der Hersteller bzw. Lieferant sollte dazu nach allen voreingestellten Benutzerkennungen und Passwörtern befragt werden.
- Passwörter dürfen nicht auf programmierbaren Funktionstasten gespeichert werden.
- Die Eingabe des Passwortes sollte unbeobachtet stattfinden.
- Bei der Eingabe darf das Passwort nicht auf dem Bildschirm angezeigt werden.
- Das Passwort muss geheim gehalten werden und sollte nur dem/der Benutzer/in persönlich bekannt sein.
- Das Passwort sollte nach Möglichkeit nicht schriftlich fixiert werden. Wird es doch aufgeschrieben, so ist für die Sicherheit dieser Aufzeichnungen besonders Sorge zu tragen.
- Das Passwort muss regelmäßig gewechselt werden, z.B. alle 90 Tage.

- Ist das Passwort unautorisierten Personen bekannt geworden, so ist ein sofortiger Passwortwechsel durchzuführen.

Falls IT-technisch möglich, sollten folgende Randbedingungen eingehalten werden:

- Die Wahl von Trivialpasswörtern (s.o.) sollte mit technischen Mitteln verhindert werden (”Stopwortliste”).
- Jede/r Benutzer/in muss sein eigenes Passwort jederzeit ändern können.
- Für die Erstanmeldung neuer Benutzer/innen sollten Einmalpasswörter vergeben werden, also Passwörter, die nach einmaligem Gebrauch gewechselt werden müssen.
- Nach einer vorgegebenen Anzahl von Fehlversuchen (meist 3) ist eine vordefinierte Aktion zu setzen. Eine solche Aktion kann etwa eine Sperre der Benutzer-ID sein, die nur vom Systemadministrator aufgehoben werden kann, aber auch eine Sperre des Gerätes oder ein Timeout, eine Warnmeldung oder Ähnliches.
- Bei der Authentisierung in vernetzten Systemen sollten Passwörter verschlüsselt übertragen werden.
- Die Passwörter sollten im System zugriffssicher und nicht im Klartext gespeichert werden, z.B. mittels Einwegverschlüsselung.
- Der Passwortwechsel sollte vom System regelmäßig initiiert werden.
- Die Wiederholung alter Passwörter beim Passwortwechsel sollte vom IT-System verhindert werden. Dazu sollten alle alten Passwörter bzw. eine größere Anzahl zum Vergleich herangezogen werden (Passwort Historie).

SYS 1.6 Regelungen des Gebrauchs von Chipkarten

Relevanz: Umsetzung/Wartung; Anwender/innen;

Für Anwendungen im Sicherheitsbereich kommen intelligente Speicherkarten (Karten mit fest verdrahteter Sicherheitslogik) sowie Mikroprozessor-Karten (Karten mit Speicher und CPU, ev. auch mit Co-Prozessor) zum Einsatz.

Chipkarten haben unter Sicherheitsaspekten im Wesentlichen zwei Funktionen zu erfüllen. Sie dienen

- als Trägermedium für vertrauliche Daten z.B. Chiffrierschlüssel, Signaturschlüssel zur Generierung elektronischer Unterschriften (vgl. Kapitel Kryptographische Maßnahmen), Zugangscodes (etwa zu IT-Systemen), persönliche Daten (medizinische Daten, Prüfungsergebnisse, etc.)
- als Security Modul (zur Durchführung von Sicherheitsfunktionen) z.B. zur Chiffrierung, Authentisierung, Generierung von elektronischen Signaturen, Generierung von Sessionkeys oder zur Durchführung von Transaktionen).

Entscheidender Vorteil der Chipkarte gegenüber anderen Medien ist, dass die Speicherung der vertraulichen Daten und die Durchführung von sicherheitskritischen Funktionen innerhalb der Karte - also in einem geschützten Bereich - erfolgen kann. Angriffe gegen diesen geschützten Bereich erfordern einen sehr hohen technologischen Aufwand. Ist mit solchen Angriffen zu rechnen, so sind eine Reihe von kryptographischen und systemtechnischen Gegenmaßnahmen zu setzen (etwa Schlüsseldiversifizierung, Verwendung kartenspezifischer Schlüssel und geeignete Implementierung von kryptographischen Algorithmen). Für Details zur Sicherheit von Chipkarten

sei auf die Literatur verwiesen - im Folgenden wird der Einsatz von Chipkarten in sicherheitsrelevanten Applikationen behandelt.

Der Zugriff auf Daten und Funktionen von Chipkarten ist heute im Allgemeinen durch sog. PINs (Personal Identification Number) geschützt. Denkbar ist auch eine Multifaktor-Authentisierung, wo eine PIN zusammen mit biometrischen Merkmalen herangezogen wird. Dadurch kann die PIN zur leichteren Handhabe verkürzt werden.

Neben der Qualität der Karte selbst kommt auch der Wahl und der Handhabung der PIN entscheidende Bedeutung für die Sicherheit des Gesamtsystems zu. Diese sind in hohem Maße abhängig vom Schutzbedarf des betroffenen Systems und der Art der Anwendung. Im Folgenden werden einige Grundregeln gegeben, die eine Art *Mindeststandard für die Handhabung von Karten und PINs in sicherheitsrelevanten Anwendungen* (etwa Zutritts- oder Zugriffskontrolle, Signatur, ...) darstellen.

- Keine unautorisierte Weitergabe der Karte: Chipkarten stellen in der Regel ein persönliches Sicherheitsmedium dar und sollten daher sicher verwahrt und keinesfalls an andere Personen weitergegeben werden. Wenn erforderlich, sind die Mitarbeiter/innen in entsprechenden Verpflichtungserklärungen zur Einhaltung dieser Regelungen zu verpflichten. Die Chipkarten sollten immer mit dem Namen der Trägerin bzw. des Trägers versehen werden. Übertragbare Chipkarten ohne Namen sollten gar nicht oder nur in sicherheitstechnisch belanglosen Bereichen eingesetzt werden.
- Die PIN muss geheim gehalten werden und darf nur dem/der Benutzer/in persönlich bekannt sein.
- Ein Aufbewahren der PIN gemeinsam mit der Karte oder gar ein Notieren der PIN auf der Karte ist unbedingt zu vermeiden.
- Die Länge der PIN hängt von Art und Schutzbedarf der Anwendung ab und liegt im Allgemeinen zwischen 4 und 8 Stellen. Die Wahl von Trivial-PINs ist zu vermeiden.
- Da sich Chipkarten in der Regel nach einer festgelegten Anzahl von PIN-Falscheingaben (meist 3) selbst sperren - dies stellt eines der wichtigsten Sicherheitsfeatures der Karte dar -, ist eine Möglichkeit des Entsperrens vorzusehen. Dies erfolgt durch eine von der PIN unterschiedliche (und meist deutlich längere) Geheimzahl (”Supervisor PIN”, “Personal Unblocking Key” (PUK)), die entweder dem/der Benutzer/in selbst oder einer/einem Sicherheitsverantwortlichen bekannt sein kann.
- PINs dürfen nicht auf programmierbaren Funktionstasten gespeichert werden.
- Die Eingabe der PIN sollte unbeobachtet stattfinden.
- Bei der Eingabe darf die PIN nicht auf einem Bildschirm oder Display angezeigt werden.
- Es ist zu prüfen, ob eine Übertragung der PIN zwischen Tastatur und Karte im Klartext aus Sicherheitsgründen vertretbar ist. Für Anwendungen mit hohem Sicherheitsbedarf in ungeschützten bzw. unkontrollierbaren Umgebungen sollten sog. “Secure PIN-Pads” zum Einsatz kommen, bei denen die Übertragung der PIN technisch oder mittels kryptographischer Verfahren geschützt wird.

Zusätzlich ergibt sich bei der Wahl der einzusetzenden Chipkarte, dass speziell in Verbindung mit Anwendungen der öffentlichen Verwaltung, diese den Security Layer unterstützen (vgl. [IKTB-040901-1]).

SYS 1.7 Organisatorische Regelungen für Zugriffsmöglichkeiten in Vertretungs- bzw. Notfällen

Relevanz: Umsetzung/Wartung; Anwender/innen;

Es sind Vorkehrungen zu treffen, die in Notfällen bei Abwesenheit einer Mitarbeiterin bzw. eines Mitarbeiters (z.B. im Urlaubs- oder Krankheitsfall) ihrer/seiner Vertretung, Zugriff auf das IT-System bzw. die Daten ermöglichen.

Generell sollte in Applikationen und IT-Systemen eine Stellvertreterregelung schon eingebaut sein, damit keine Weitergabe von Passwörtern in Abwesenheitsfällen benötigt wird.

Ist es in Einzelfällen doch notwendig, ein Passwort zu hinterlegen, so ist dieses an einem geeigneten, geschützten Ort (z.B. in einem Tresor) zu deponieren und bei jeder Änderung des Passwortes zu aktualisieren (regelmäßige Prüfung auf Aktualität erforderlich!). Wird es notwendig, dieses hinterlegte Passwort zu nutzen, so sollte dies nach dem Vier-Augen-Prinzip, d. h. von zwei Personen gleichzeitig, geschehen.

Ist vom System technisch kein Vier-Augen-Prinzip vorgesehen, so lässt sich dieses auch organisatorisch nachbilden, indem Passwörter in mehrere Teile zerlegt werden, wobei jede/r im Notfall Zugriffsberechtigte nur einen Teil besitzt.

Nach der Rückkehr der Benutzerin bzw. des Benutzers ist diese/r über die Weitergabe des Passworts in Kenntnis zu setzen und ein neues Passwort von ihr/ihm zu vergeben. Außerdem ist die Weitergabe des Passworts und deren Dauer zu dokumentieren.

Je nach den technischen Möglichkeiten können auch “Einmalpasswörter” oder Passwörter mit begrenzter Benutzungsdauer vergeben werden.

Beim Einsatz von Chipkarten zur Authentisierung sind Vorkehrungen zu treffen, die es erlauben, bei momentaner Inoperabilität bzw. Nichtverfügbarkeit der Chipkarte einer/einem Berechtigten den Zugang zum System zu ermöglichen. Abhängig von den Personalisierungsmöglichkeiten vor Ort ist dafür Sorge zu tragen, dass eine zeitgerechte Neuausstellung der Karte oder eine Ausstellung einer temporär gültigen Karte möglich ist oder aber Ersatzkarten zur Verfügung stehen.

SYS 1.8 Bildschirmsperre

Relevanz: Umsetzung/Wartung; Anwender/innen;

Unter einer Bildschirmsperre versteht man die Möglichkeit, die auf dem Bildschirm aktuell vorhandenen Informationen zu verbergen. Die Aktivierung der Bildschirmsperre sollte erfolgen, wenn der/die Benutzer/in den Arbeitsplatz für eine nur kurze Zeit verlässt. Als weiteres Leistungsmerkmal sollte die Bildschirmsperre eine automatische Aktivierung bei längerer Pausenzeit aufweisen. Verfügt das Softwareprodukt außerdem über eine Passwort-Abfrage, wird bei der Abwesenheit der Benutzerin bzw. des Benutzers zusätzlich ein Zugriffsschutz für das IT-System gewährleistet.

Beim Einsatz von Chipkarten ist die Bildschirmsperre nur mittels Chipkarte und PIN wieder aufzuheben. Beim Entfernen der Chipkarte ist entweder die Bildschirmsperre zu aktivieren, oder der/die Benutzer/in auszuloggen.

SYS 1.9 Richtlinien beim Datenaustausch mit Dritten

Relevanz: Umsetzung/Wartung; Anwender/innen;

Beim regelmäßigen Datenaustausch mit Dritten ist die Festlegung von Richtlinien bzw. der Abschluss von Vereinbarungen mit allen Beteiligten sinnvoll. Dabei spielt es keine Rolle, wie der Datenaustausch selbst erfolgt (Datenträgeraustausch, E-Mail, etc.).

In einer derartigen Vereinbarung können Angaben zu folgenden Punkten enthalten sein:

- Bestimmung der Verantwortlichen
- Benennung von Ansprechpartnerinnen bzw. Ansprechpartnern (in technischen, organisatorischen und sicherheitstechnischen Belangen)
- existiert ein Non-Disclosure-Agreement (NDA)
- Festlegung der Datennutzung
- welche Anwendungen und Datenformate sind zu verwenden
- wie und wo erfolgt die Prüfung auf Virenfreiheit
- wann dürfen Daten gelöscht werden
- Regelung des Schlüsselmanagements, falls erforderlich
- Einhaltung einschlägiger Gesetze (bspw. DSG 2000, BGBl. I Nr. 165/1999 i.d.g.F. etc.)

5.2 Betriebsmittel und Datenträger

Relevanz: Umsetzung/Wartung; Anwender/innen;

In diesem Kapitel werden generelle Richtlinien zum Umgang mit Betriebsmitteln und Datenträgern gegeben. Der Umgang mit Datenträgern und den darauf gespeicherten Informationen ist in der "Informationssicherheitspolitik" einer Organisation festzulegen (vgl. dazu Teil 1 des Informations-sicherheitshandbuches, Kapitel 3.2.5 "Klassifikation von Daten" [KIT S01]). Diese Klassifikation und die damit verbundene Festlegung der Verantwortlichkeiten und Vorgehensweisen stellen eine wesentliche Grundlage für die IT-Sicherheit einer Organisation dar.

Insbesondere sei darauf hingewiesen, dass einerseits die Klassifizierung der Daten national durch das Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999 i.d.g.F. sowie durch das Informationssicherheitsgesetz (InfoSiG), BGBl. I Nr. 23/2002 i.d.g.F. geregelt wird. International bzw. im EU-Raum ist der "Beschluss des Rates vom 19. März 2001 über die Annahme der Sicherheitsvorschriften des Rates", EU 5775/01 i.d.g.F. einzuhalten, der die Verbindung zwischen den nationalen Klassifizierungen und Richtlinien darstellt. Dies ist gegebenenfalls in der Informationssicherheitspolitik zu berücksichtigen.

SYS 2.1 Betriebsmittelverwaltung

Relevanz: Umsetzung/Wartung;

Betriebsmittel für den IT-Einsatz sind alle erforderlichen Mittel wie Hardwarekomponenten (Rechner, Tastatur, Drucker, ...), Software (Systemsoftware, Individualprogramme, Standardsoftware u.ä.), Verbrauchsmaterial (Papier, Toner, Druckerpatronen), Datenträger (Magnetbänder, Disketten, Streamertapes, Festplatten, Wechselplatten, CD-ROMs u.ä.).

Die Betriebsmittelverwaltung umfasst folgende Aufgaben:

- Beschaffung,
- Prüfung vor Einsatz,
- Kennzeichnung,
- Bestandsführung und
- Außerbetriebnahme.

Beschaffung:

Neben reinen Wirtschaftlichkeitsaspekten kann durch ein geregeltes Beschaffungsverfahren auch die Neu- und Weiterentwicklung im Bereich der Informationstechnik stärker berücksichtigt werden. Eine zentrale Beschaffung sichert auch die Einführung und Einhaltung eines "Hausstandards" und vereinfacht damit die Schulung der Mitarbeiter/innen und die Wartung.

Prüfverfahren vor Einsatz:

Mit einem geregelten Prüfverfahren vor Einsatz der Betriebsmittel lassen sich unterschiedliche Gefährdungen abwenden.

Beispiele dafür sind:

- Überprüfung der Vollständigkeit von Lieferungen (z.B. Handbücher), um die Verfügbarkeit aller Lieferteile zu gewährleisten,
- Test neuer PC-Software sowie neuer vorformatierter Datenträger mit einem Virensuchprogramm,
- Testläufe neuer Software auf speziellen Testsystemen,
- Überprüfung der Kompatibilität neuer Hardware- und Softwarekomponenten mit den vorhandenen.

Bestandsführung:

Alle wesentlichen Betriebsmittel sollten mit eindeutigen Identifizierungsmerkmalen gekennzeichnet werden. Zusätzlich sollten die Seriennummern vorhandener Geräte wie Bildschirm, Drucker, Festplatten etc. dokumentiert werden, damit sie nach einem Diebstahl identifiziert werden können.

Für die Bestandsführung müssen die Betriebsmittel in Bestandsverzeichnissen aufgelistet werden. Ein solches Bestandsverzeichnis muss Auskunft geben können über Identifizierungsmerkmale, Beschaffungsquellen, Lieferzeiten, Verbleib der Betriebsmittel, Lagerhaltung, Aushändigungsvorschriften, Wartungsverträge und Wartungsintervalle.

Eine ordnungsgemäße Bestandsführung erleichtert nicht nur die Verbrauchsermittlung und Veranlassung von Nachbestellungen, sondern ermöglicht auch Vollständigkeitskontrollen, die Überprüfung des Einsatzes von nicht genehmigter Software oder die Feststellung der Entwendung von Betriebsmitteln.

Im Bundesbereich gibt es Vorschriften über die Bestandsführung, die "Richtlinien für die Inventar- und Materialverwaltung (RIM)". Die dort vorgesehenen Aufzeichnungen reichen für einen sicheren EDV-Betrieb nicht aus. Die für den sicheren Betrieb zuständige Organisationseinheit muss daher eigene, entsprechend erweiterte Aufzeichnungen führen.

SYS 2.2 Datenträgerverwaltung

Relevanz: Umsetzung/Wartung; Anwender/innen;

Die Datenträgerverwaltung stellt einen Teil der Betriebsmittelverwaltung dar. Ihre Aufgabe ist es, den Zugriff auf Datenträger im erforderlichen Umfang und in angemessener Zeit zu gewährleisten.

Neben den in SYS 2.1 „Betriebsmittelverwaltung“ angeführten Maßnahmen ist für die Verwaltung von Datenträgern zusätzlich zu beachten:

- Die äußerliche Kennzeichnung von Datenträgern soll deren schnelle Identifizierung ermöglichen, jedoch für Unbefugte keine Rückschlüsse auf den Inhalt erlauben (z.B. die Kennzeichnung eines Datenträgers mit dem Stichwort “Gehaltsdaten”), um einen Missbrauch zu erschweren. Eine festgelegte Struktur von Kennzeichnungsmerkmalen (z.B. Datum, Ablagestruktur, lfd. Nummer) erleichtert die Zuordnung in Bestandsverzeichnissen.
- Für eine sachgerechte Behandlung von Datenträgern sind die Herstellerangaben zu beachten.
- Hinsichtlich der Aufbewahrung von Datenträgern sind einerseits Maßnahmen zur Lagerung (magnetfeld-/staubgeschützt, klimagerecht) und andererseits Maßnahmen zur Verhinderung des unbefugten Zugriffs (geeignete Behältnisse, Schränke, Räume) zu treffen.
- Versand und Transport: Die Verpackung des Datenträgers ist an seiner Schutzbedürftigkeit auszurichten. Hier sind die in der Informationssicherheitspolitik festzulegenden Regeln umzusetzen (etwa Versand nur in verschlossenen/versiegelten Behältnissen, durch Kurierdienst, in chiffrierter Form, etc.).
- Der Datenträger darf über die zu versendenden Daten hinaus keine “Restdaten” enthalten. Dies kann durch physikalisches Löschen erreicht werden (s. auch unten “Wiederaufbereitung”).
- Vor Versand oder Weitergabe wichtiger Datenträger sollte eine Sicherungskopie erstellt werden. Das Anfertigen von Kopien ist zu dokumentieren und die Kopien sind als solche zu kennzeichnen.
- *Wiederaufbereitung:* Eine geregelte Vorgehensweise für die Löschung bzw. Wiederaufbereitung von Datenträgern verhindert den Missbrauch der gespeicherten Daten. Vor der Wiederverwendung von Datenträgern, die schutzwürdige Daten enthalten haben, müssen diese Daten in irreversibler Form gelöscht werden.
- Außerbetriebnahme, Reparaturtausch: Datenträger, die schutzwürdige Daten enthalten und außer Betrieb genommen oder im Zuge einer Reparatur ausgetauscht werden sollen, sind mechanisch zu zerstören (vgl. dazu auch ÖNORM S 2109 „Akten- und Datenvernichtung“ sowie Kap. 6.1 „Wartung“).

Für den Fall, dass von Dritten erhaltene Datenträger eingesetzt werden, sind Regelungen über deren Behandlung vor dem Einsatz zu treffen. Werden zum Beispiel Daten für PCs übermittelt, sollte generell ein Viren-Check des Datenträgers erfolgen. Dies gilt entsprechend auch vor dem erstmaligen Einsatz neuer Datenträger. Es ist empfehlenswert, nicht nur beim Empfang, sondern auch vor dem Versenden von Datenträgern diese auf Viren zu überprüfen. Vgl. dazu auch Kap. „Virenschutz“.

SYS 2.3 Datenträgeraustausch

Relevanz: Umsetzung/Wartung; Anwender/innen;

Kennzeichnung der Datenträger beim Versand

Neben den in Maßnahme SYS 2.2 „Datenträgerverwaltung“ dargestellten Umsetzungshinweisen ist bei einer ausreichenden Kennzeichnung von auszutauschenden Datenträgern darauf zu achten, dass Absender/in und (alle) Empfänger/innen unmittelbar zu identifizieren sind. Die Kennzeichnung muss den Inhalt des Datenträgers eindeutig für den/die Empfänger/in erkennbar machen. Es ist jedoch bei schützenswerten Informationen wichtig, dass diese Kennzeichnung für Unbefugte nicht interpretierbar ist.

Darüber hinaus sollten die Datenträger mit den für das Auslesen notwendigen Parametern gekennzeichnet werden. Das Versanddatum, eventuelle Versionsnummern oder Ordnungsmerkmale können gegebenenfalls nützlich sein.

Regelung des Datenträgeraustausches

Sollen zwischen zwei oder mehreren Kommunikationspartnern Datenträger ausgetauscht werden, so sind zum ordnungsgemäßen Austausch einige Punkte zu beachten.

Zum Beispiel:

- Die Adressierung muss eindeutig erfolgen, um eine fehlerhafte Zustellung zu vermeiden. So sollte neben dem Namen der Empfängerin bzw. des Empfängers auch die Organisationseinheit und die genaue Bezeichnung der Behörde/des Unternehmens angegeben sein. Entsprechendes gilt für die Adresse der Absenderin oder des Absenders.
- Dem Datenträger sollte (optional) ein Datenträgerbegleitzettel beigelegt werden, der Absender/in, Empfänger/in, Art des Datenträgers, Seriennummer, Identifikationsmerkmale für den Inhalt des Datenträgers, Datum des Versandes, ggf. Datum bis wann der Datenträger spätestens den/die Empfänger/in erreicht haben muss, sowie Parameter, die zum Lesen der Informationen benötigt werden (z.B. Bandgeschwindigkeit) enthält.
- Bei regelmäßigem Austausch von Datenträgern zwischen den gleichen Partnern empfiehlt es sich, dafür stets die gleichen Datenträger zu verwenden, so dass bei einem ev. Fehler bei der Wiederaufbereitung (vgl. SYS 2.2 „Datenträgerverwaltung“) die potentiellen Auswirkungen möglichst gering gehalten werden.
- Abhängig von den Regelungen der Informationssicherheitspolitik sind Datenträger, die Daten hoher Vertraulichkeitsstufen enthalten, beim Transport durch Dritte entweder zu verschlüsseln, oder in entsprechend versperrten Behältnissen zu transportieren

Nicht vermerkt werden sollte,

- welches Passwort für die eventuell geschützten Informationen vergeben wurde,
- welche Schlüssel ggf. für eine Verschlüsselung der Informationen verwendet wurde,
- welchen Inhalt der Datenträger hat.

Der Versand des Datenträgers kann (optional) dokumentiert werden. Für jede stattgefundene Übermittlung ist dann in einem Protokoll festzuhalten, wer wann welche Informationen erhalten hat. Je nach Schutzbedarf beziehungsweise Wichtigkeit der übermittelten Informationen ist der Empfang zu quittieren und ein Quittungsvermerk dem erwähnten Protokoll beizufügen.

Es sind jeweils Verantwortliche für den Versand und für den Empfang zu benennen.

5.3 Einsatz von Software

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

SYS 3.1 Nutzungsverbot nicht-freigegebener Software

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

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

Dabei ist zu beachten:

- Das Nutzungsverbot nicht-freigegebener Software sollte schriftlich fixiert werden, alle Mitarbeiter/innen sind darüber zu unterrichten.
- Ausnahmeregelungen sollten einen Erlaubnisvorbehalt vorsehen.
- Das unautorisierte Einspielen und/oder Nutzen von Software ist soweit möglich mit technischen Mitteln zu verhindern.
- Es ist zu dokumentieren, welche Versionen ausführbarer Dateien freigegeben wurden; dabei sind insbesondere Erstellungsdatum und Dateigröße festzuhalten.
- Die freigegebenen Programme sind regelmäßig auf Veränderungen zu überprüfen.

SYS 3.2 Nutzungsverbot privater Hard- und Software-Komponenten

Relevanz: Umsetzung/Wartung; Anwender/innen;

Im Allgemeinen sollte ein Nutzungsverbot privater Software (vgl. auch SYS 3.1 Nutzungsverbot nicht-freigegebener Software), Hardware (Disketten, Wechselplatte, PC, Notebook) und Daten ausgesprochen werden.

Besonders bei RAS-Zugängen (remote access service; Fernzugänge) ist das Verwendungsverbot privater HW und SW zu beachten (vgl. Kap. Remote Access).

Ausnahmeregelungen sollten einen Erlaubnisvorbehalt vorsehen.

SYS 3.3 Überprüfung des Software-Bestandes

Relevanz: Umsetzung/Wartung;

Um Verstöße gegen das Verbot der Nutzung nicht-freigegebener Software feststellen zu können, ist eine regelmäßige Überprüfung des Software-Bestandes notwendig. Ist die Zahl der IT-Systeme sehr groß, kann eine stichprobenartige Überprüfung durchgeführt werden. Die Ergebnisse der Überprüfung sind zu dokumentieren, um auch Wiederholungsfälle feststellen zu können.

Dabei ist zu beachten:

- Sollte bei der Überprüfung nicht-freigegebene Software gefunden werden, so ist die Legalisierung oder Entfernung zu veranlassen. Es muss festgelegt sein, was mit allfälligen Daten zu geschehen hat, welche mittels illegaler Software verarbeitet bzw. gespeichert wurden.
- Um diese Überprüfung durchführen zu können, muss der überprüfenden Instanz die entsprechende Befugnis durch die Unternehmens- bzw. Behördenleitung verliehen werden.
- Der prüfenden Instanz muss bekannt sein, welche Software auf welchem IT-System freigegeben ist (Software-Bestandsverzeichnis).
- Es ist festzulegen, wie bei Feststellung eines Verstoßes verfahren wird.

SYS 3.4 Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen

Relevanz: Umsetzung/Wartung; Anwender/innen;

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

Im Folgenden seien einige dieser Funktionen kurz erläutert:

- *Passwortschutz bei Programmaufruf:*
  Das Programm kann nur gestartet werden, wenn vorher ein Passwort korrekt eingegeben wurde. Dies verhindert die unberechtigte Nutzung des Programms.
- *Zugriffsschutz zu einzelnen Dateien:*
  Das Programm kann nur dann auf eine geschützte Datei zugreifen, wenn das mit dieser Datei verknüpfte Passwort korrekt eingegeben wird. Dies verhindert den unerlaubten Zugriff mittels des Programms auf bestimmte Dateien.
- *Automatische Speicherung von Zwischenergebnissen:*
  Das Programm nimmt eine automatische Speicherung von Zwischenergebnissen vor, so dass ein Stromausfall nur noch die Datenänderungen betrifft, die nach dieser automatischen Speicherung eingetreten sind. Gegebenenfalls ist jedoch zu überprüfen, ob die zwischengespeicherten Daten nach dem regulären Programmende wieder gelöscht wurden (vgl. SYS 3.6 „Verifizieren der zu übertragenden Daten vor Weitergabe“).
- *Automatische Sicherung der Vorgängerdatei:*
  Wird eine Datei gespeichert, zu der im angegebenen Pfad eine Datei gleichen Namens existiert, so wird die zweite Datei nicht gelöscht, sondern mit einer anderen Kennung versehen. Damit wird verhindert, dass versehentlich eine Datei gleichen Namens gelöscht wird.

- *Verschlüsselung von Dateien:*
  Das Programm ist in der Lage, eine Datei verschlüsselt abzuspeichern, so dass eine unbefugte Kenntnisnahme verhindert werden kann. Die Inhalte der Datei sind damit nur denjenigen zugänglich, die über den verwendeten geheimen Chiffrierschlüssel verfügen.
- *Automatisches Anzeigen von Makros in Dateien:*
  Diese Funktion soll das unbeabsichtigte Ausführen von Makros verhindern und damit Schutz vor Makro-Viren bieten (vgl. Kap. Virenschutz).

Je nach eingesetzter Software und damit vorhandenen Zusatzsicherheitsfunktionen kann der Einsatz dieser Funktionen sinnvoll sein. Für mobil eingesetzte IT-Systeme bieten sich insbesondere die Nutzung des Passwortschutzes bei Programmaufruf und die automatische Speicherung an.

SYS 3.5 Update von Software

Relevanz: Umsetzung/Wartung;

Durch ein Update von Software können Schwachstellen beseitigt oder Funktionen erweitert werden.

Ein Update ist insbesondere dann erforderlich, wenn Schwachstellen bekannt werden, die Auswirkungen auf den sicheren Betrieb des Systems haben, wenn Fehlfunktionen wiederholt auftauchen oder eine funktionale Erweiterung aus sicherheitstechnischen oder fachlichen Erfordernissen notwendig wird.

Vor einem Update sind die Funktionalität, die Interoperabilität und die Zuverlässigkeit der neuen Komponenten genau zu prüfen. Dies geschieht am sinnvollsten auf einem eigenen Testsystem, bevor das Update in den produktiven Einsatz übernommen wird.

Insbesondere ist darauf Bedacht zu nehmen, dass in der Vorgängerversion explizit behobene Sicherheitsmängel nicht wieder neu auftauchen, bzw. getroffene Parametrisierungen nachgezogen werden.

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

SYS 3.6 Verifizieren der zu übertragenden Daten vor Weitergabe

Relevanz: Anwender/innen;

Vor dem Versenden einer Datei per E-Mail oder Datenträgeraustausch bzw. vor dem Veröffentlichen einer Datei auf einem WWW-Server sollte diese daraufhin überprüft werden, ob sie Restinformationen enthält, die nicht zur Veröffentlichung bestimmt sind. Solche Restinformationen können verschiedenen Ursprungs sein und dementsprechend unterschiedlich können auch die Aktionen sein, die dagegen zu unternehmen sind. Die häufigsten Ursachen für solche Restinformationen sind im Folgenden beschrieben.

Generell sollte Standardsoftware wie z.B. für Textverarbeitung oder Tabellenkalkulation darauf überprüft werden, welche Zusatzinformationen in damit erstellten Dateien gespeichert werden. Dabei werden einige dieser Informationen mit, andere ohne Wissen der Benutzerin bzw. des Benutzers gespeichert.

Vor der Weitergabe von Dateien sollten diese zumindest stichprobenartig auf unerwünschte Zusatzinformationen überprüft werden. Dazu sollte ein anderer Editor benutzt werden als der, mit dem die Datei erstellt wurde. Dabei ist darauf zu achten, dass nicht alle Restinformationen einfach gelöscht werden können, ohne das Dateiformat zu zerstören. Wenn z.B. aus einer Textverarbeitungsdatei einige Bytes gelöscht werden, erkennt das Textverarbeitungsprogramm unter Umständen das Dateiformat nicht mehr.

- Um Restinformationen zu beseitigen, kann die Datei in einem anderen Dateiformat abgespeichert werden, z.B. als “Nur-Text” oder als HTML,
- können die Nutzdaten in eine zweite Instanz derselben Standardsoftware kopiert werden, wobei auf dem IT-System keine andere Applikation laufen sollte. Dies empfiehlt sich insbesondere bei Dateien mit einer größeren Änderungshistorie.

Verborgener Text / Kommentare

Eine Datei kann Textpassagen enthalten, die als “versteckt” oder “verborgen” formatiert sind. Einige Programme bieten auch die Möglichkeit an, Kommentare hinzuzufügen, die auf dem Ausdruck und oft auch am Bildschirm ausgeblendet sind. Solche Textpassagen können Bemerkungen enthalten, die nicht für den/die Empfänger/in bestimmt sind. Daher müssen in Dateien, bevor sie an Externe weitergegeben werden, solche Zusatzinformationen gelöscht werden.

Änderungsmarkierungen

Bei der Bearbeitung von Dateien kann es sinnvoll sein, hierbei Änderungsmarkierungen zu verwenden. Da diese auf dem Ausdruck und am Bildschirm ausgeblendet werden können, muss vor der Weitergabe von Dateien ebenfalls überprüft werden, ob diese Änderungsmarkierungen enthalten.

Versionsführung

Bei einer Vielzahl von Anwendungen gibt es die Möglichkeit, verschiedene Versionen eines Dokumentes in *einer* Datei zu speichern. Dies dient dazu, um bei Bedarf auf frühere Überarbeitungsstände zurückgreifen zu können. Dies kann aber sehr schnell zu riesigen Dateien führen, z.B. wenn Graphiken mitgeführt werden. Es ist darauf zu achten, dass keine Optionen, die sämtliche Vorgängerversionen automatisch abspeichern, in den Grundeinstellungen der Anwendung ausgewählt werden.

Dateieigenschaften

Als Dateieigenschaften oder Datei-Info werden in der Datei Informationen gespeichert, die bei späteren Suchen helfen sollen, Dateien wieder zu finden. Dabei können je nach Applikation Informationen wie Titel, Verzeichnisstrukturen, Versionsstände, Bearbeiter/innen (nicht nur die/der Unterschreibende), Kommentare, Bearbeitungszeit, letztes Druckdatum, Dokumentnamen und -beschreibungen enthalten sein. Einige dieser Informationen werden von den Programmen selber angelegt und können nicht durch den/die Bearbeiter/in beeinflusst werden. Andere Informationen

müssen manuell eingegeben werden. Vor der Weitergabe einer Datei an Externe ist zu überprüfen, welche zusätzlichen Informationen dieser Art die Datei enthält.

Schnellspeicherung

Textverarbeitungsprogramme nutzen die Option der Schnellspeicherung, um nur die Veränderungen seit der letzten Sicherung und nicht das gesamte Dokument speichern zu müssen. Dieser Vorgang nimmt somit weniger Zeit in Anspruch als ein vollständiger Speichervorgang. Der entscheidende Nachteil ist jedoch, dass die Datei unter Umständen Textfragmente enthalten kann, die durch die Überarbeitung hätten beseitigt werden sollen. Grundsätzlich sollten daher Schnellspeicherungs-optionen abgeschaltet werden.

Entscheidet sich der/die Benutzer/in trotzdem für die Schnellspeicheroption, sollte er/sie bei folgenden Situationen immer einen vollständigen Speichervorgang durchführen:

- wenn die Bearbeitung eines Dokuments abgeschlossen ist,
- bevor der Dokumenttext in eine andere Anwendung übertragen wird,
- bevor das Dokument in ein anderes Dateiformat konvertiert wird und
- bevor das Dokument per E-Mail oder Datenträgeraustausch versandt wird.

SYS 3.7 Datenformate

Relevanz: Umsetzung/Wartung; Anwender/innen;

Durch die Vielzahl von Anwendungsprogrammen ist auch eine Vielzahl von Datenformaten in Verwendung. Bei gleichartigen Anwendungen verschiedener Hersteller, aber auch bei den verschiedenen Versionen ein und desselben Programms eines Herstellers können die gebräuchlichen Datenformate variieren.

Bei der Anschaffung von Software muss daher auf die damit zu verwendenden beabsichtigten Datenformate geachtet werden. Sollen Datenbestände mit Dritten ausgetauscht werden, so ist umso mehr auf die Kompatibilität der durch eine Anwendung unterstützten Formate zu achten.

Für die Lebensdauer von Datenbeständen muss gewährleistet werden, dass für den Zugriff auf gesicherte Daten auch in Zukunft Anwendungen existieren, welche die entsprechenden Datenformate bearbeiten können. In diesem Zusammenhang ist im Rahmen der Datensicherung und –pflege ggf. eine Umformatierung vorzusehen.

5.4 Virenschutz

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

Computer-Viren (im Rahmen dieses Handbuches der Einfachheit halber als Viren bezeichnet) gehören zu den "Programmen mit Schadensfunktionen" ("maliziöse Software"). Dies sind Programme, die verdeckte Funktionen enthalten und damit durch Löschen, Überschreiben oder sonstige Veränderungen unkontrollierbare Schäden an Programmen und Daten bewirken können. Damit verursachen sie zusätzliche Arbeit und Kosten und haben einen negativen Einfluss auf die Vertraulichkeit, Integrität und/oder Verfügbarkeit von Daten oder Programmen.

Zu den Programmen mit Schadensfunktionen gehören:

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

Trojanische Pferde:
Selbständige Programme mit verdeckter Schadensfunktion, ohne Selbstreproduktion. Trojanische Pferde dienen vor allem dazu, Computer auszuspionieren.

Logische Bomben:
Programme, deren Schadensfunktion von einer logischen Bedingung gesteuert wird, beispielsweise dem Datum oder einer bestimmten Eingabe.

Würmer:
Selbständige, selbstreproduzierende Programme, die sich in einem System (vor allem in Netzen) ausbreiten.

Verbreitung:
Während früher Viren meist durch den Austausch verseuchter Datenträger verbreitet wurden, wird heute zunehmend die Verbreitung über Internet bzw. E-Mail zum Problem. Bei den meisten über E-Mail verbreiteten "Viren" handelt es sich eigentlich um Würmer, die - unabhängig von der eigentlichen Schadensfunktion - schon durch ihr massenhaftes Auftreten und ihre rasante Verbreitung großes Aufsehen erregen und zu hohen Schäden führen. (vgl. dazu auch [NSA-EEC1])

Das nachfolgende Kapitel beschäftigt sich vorwiegend mit dem Schutz gegen Viren und Würmer, die zur Vereinfachung im Folgenden generell als "Viren" bezeichnet werden. Die angeführten Maßnahmen sind großteils auch gegen andere Arten von Software mit Schadensfunktion, wie z.B. Trojanische Pferde anwendbar.

SYS 4.1 Erstellung eines Virenschutzkonzepts

Relevanz: Umsetzung/Wartung;

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

Schutzmaßnahmen sind zu treffen:

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

Neben den technischen Schutzmaßnahmen sind auch organisatorische und personelle Maßnahmen erforderlich, um einem Virenbefall soweit wie möglich vorzubeugen, bzw. im Falle eines Virenbefalls den Schaden möglichst zu begrenzen.

Die nachfolgenden Maßnahmen geben eine Reihe von generellen Empfehlungen zum Virenschutz, die an die Erfordernisse der betroffenen Institution anzupassen sind. Je mehr bzw. je exakter die Empfehlungen umgesetzt werden, desto geringer wird das allgemeine Risiko. Allerdings können ggf. bestimmte (auch notwendige / vorgesehene) Funktionen nicht mehr oder zumindest weniger produktiv durchgeführt werden. Die anzuwendenden Maßnahmen sind daher vor dem Hintergrund des Gesamtsystems und der jeweils gültigen Policy vorzuschreiben. Für die Effizienz des Virenschutzkonzeptes sind dabei nicht nur die ausgewählten Maßnahmen selbst von Bedeutung, sondern auch die Abstimmung dieser Maßnahmen aufeinander.

SYS 4.2 Generelle Maßnahmen zur Vorbeugung gegen Virenbefall

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

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

- Regelmäßige Durchführung einer Datensicherung (vgl. BCP 1.1).
- Sichere Aufbewahrung der Sicherheitskopien von Datenträgern (vgl. BCP 1.5).
- Setzen des Schreibschutzes bei allen Disketten, auf die nicht geschrieben werden muss (gilt insbesondere für die meisten Programmdisketten) und bei allen ausgehenden Datenträgern.
- Überprüfung aller ein- und ausgehenden Datenträger (vgl. auch SYS 2.3 Datenträgeraustausch).
- Überprüfung aller vorinstallierten Neugeräte und gewarteten Geräte.
- Überprüfung aller ein- und ausgehenden Dateien über externe Netzwerke (E-Mails, Internet) (s.u.).
- Als vorbeugende Maßnahme gegen Virenbefall empfiehlt es sich, die Boot-Reihenfolge auf C: A: einzustellen oder das Booten von Diskette ganz zu unterbinden.
- Die Unterteilung der Festplatte in mehrere Partitionen kann die Rekonstruktion von Daten nach einem Virus-Schaden erleichtern (Anmerkung: Dies gilt auch bei einem Headcrash).
- Es sollten nur vertrauenswürdige Programme zugelassen sein, die auch über entsprechende Sicherheitsfunktionen verfügen. Dies gilt in besonderem Maße für E-Mail-Programme. “Private” Insel-Lösungen auf einzelnen Arbeitsplatz-Rechnern sollten nicht zugelassen werden, um die Sicherheit des Gesamtsystems nicht zu gefährden.
- Für Probleme sollte ein zentraler Ansprechpartner (E-Mail-Adresse, Telefon- und Fax-Nummer) benannt werden.

SYS 4.3 Empfohlene Virenschutzmaßnahmen auf Firewall-Ebene

Relevanz: Umsetzung/Wartung;

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

Gateways bieten meist auch Möglichkeiten ohne teure Zusatzprodukte Maßnahmen zu setzen, die der Verbreitung von Schadprogrammen entgegenwirken. Dabei können Dateitypen (z.B. *.VBS, *.WSH, *.BAT, *.EXE), die im täglichen Arbeitsablauf nicht als Anhänge von E-Mails vorkommen, gleich zentral abgeblockt werden.

Der Einsatz spezieller Rechner, die den Verkehr auf Viren und auch den Content der Mails scannen können, ist in Form einer erweiterten Gatewayfunktionalität oder der Einbindung über eigene Protokolle (z.B. Content Vectoring Protocol) möglich. Dabei kann Mail mittels Virenscanner verschiedener Hersteller überprüft werden und - sogar vor dem Vorliegen der neuen Virensignaturen - durch das Filtern entsprechender Textbegriffe die Ausbreitung neuer Schadsoftware gestoppt werden.

Sollten Informationen geblockt werden, empfiehlt es sich, dem/der Absender/in einer solchen E-Mail eine automatisierte Nachricht zukommen zu lassen, dass seine/ihre Mail nicht zugestellt werden konnte.

SYS 4.4 Empfohlene Virenschutzmaßnahmen auf Server-Ebene

Relevanz: Umsetzung/Wartung;

Auf E-Mail-Servern sollten Virenschutzprogramme zur zentralen Überprüfung des E-Mail-Verkehrs installiert werden (vgl. dazu auch SYS 4.8 „Auswahl und Einsatz von Virenschutzprogrammen“).

Dabei ist auf eine regelmäßige Aktualisierung der eingesetzten Programme zu achten.

SYS 4.5 Empfohlene Virenschutzmaßnahmen auf Client-Ebene und Einzelplatzrechnern

Relevanz: Umsetzung/Wartung; Anwender/innen;

- Aktivierung aller vorhandenen Sicherheitsfunktionen des Rechners (Passwort-Schutz, Bildschirmschoner mit Passwort, etc.), damit während der Abwesenheit der berechtigten Benutzerin bzw. des berechtigten Benutzers Unbefugte keine Möglichkeit haben, durch unbedachte oder gewollte Handlungen den Rechner zu gefährden.
- Einsatz eines aktuellen Virenschutzprogrammes mit aktuellen Signatur-Dateien, das im Hintergrund läuft (resident) und bei bekannten Viren Alarm schlägt. (Auch wenn am Mail-Server bereits ein Virenschutzprogramm zum Einsatz kommt, empfiehlt sich die Installation dezentraler Virenschutzprogramme, um beispielsweise auch Schutz bei verschlüsselter Kommunikation zu erreichen.)
- Aktivierung der Anzeige aller Dateitypen im Browser bzw. Mailprogramm.
- Aktivierung des Makro-Virenschutzes von Anwendungsprogrammen (MS Word, Excel, Powerpoint, etc.) und Beachtung von Warnmeldungen.
- Sofern möglich: Wahl der höchsten Stufen in den Sicherheitseinstellungen von Internet-Browsern (Deaktivieren von aktiven Inhalten (ActiveX, Java, JavaScript) und Skript-Sprachen (z.B. Visual Basic Script, VBS), etc.).
- Keine Nutzung von Applikationsverknüpfung für Anwendungen mit potentiell aktivem Code (MS-Office) im Browser, keine Aktivierung von Anwendungen über Internet.
- Die Ausführung von aktiven Inhalten in E-Mail-Programmen immer unterbinden (entsprechende Optionen setzen).
- Durch den Einsatz eines Firewall-Produkts auf den Einzelplatzrechnern (Personal Firewalls), die regeln, welche Programme auf das Internet zugreifen dürfen, kann der Schadsoftware ebenfalls gezielt entgegen gewirkt werden. Dadurch wird die zentrale Firewall, die keine Informationen über die aufrufenden Programme hat, wirkungsvoll ergänzt (vgl. SYS 8.4).

SYS 4.6 Vermeidung bzw. Erkennung von Viren durch den/die Benutzer/in

Relevanz: Umsetzung/Wartung; Anwender/innen;

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

Erkennen potentieller Gefahren bei eingehender E-Mail und Abwehrmaßnahmen:

- Bei E-Mail auch von vermeintlich bekannten bzw. vertrauenswürdigen Absenderinnen bzw. Absendern prüfen, ob der Text der Nachricht auch zum/zur Absender/in passt (englischer Text von deutscher Partnerin bzw. deutschem Partner, zweifelhafter Text oder fehlender Bezug zu konkreten Vorgängen etc.) und ob die Anlage (Attachment) auch erwartet wurde.
- Vorsicht bei mehreren E-Mails mit gleichlautendem Betreff.
- Kein “Doppelklick” bei ausführbaren Programmen (*.COM, *.EXE) oder Script-Sprachen (*.VBS, *.BAT, etc.), (sofern sie nicht bereits auf Firewall-Ebene gefiltert wurden),
- Vorsicht auch bei Office-Dateien (*.DOC, *.XLS, *.PPT, etc.) sowie Bildschirmschonern (*.SCR).
- Auch eine E-Mail im HTML-Format kann aktive Inhalte mit Schadensfunktion enthalten.
- Nur vertrauenswürdige E-Mail-Attachments öffnen (z.B. in letzter Konsequenz sogar nach telefonischer Absprache). Es ist zu beachten, dass die Art des Datei-Anhangs (Attachment) bei Sabotageangriffen oft getarnt ist und über ein Icon nicht sicher erkannt werden kann.
- Die Konfiguration der E-Mail-Clients sollte so eingestellt sein, dass Attachments nicht automatisch geöffnet werden. Außerdem sollten als E-Mail-Editor keine Programme mit der Funktionalität von Makro-Sprachen (z.B. MS Word) oder Scripts eingesetzt werden. Bei der Verwendung des HTML-Formates ist ebenfalls Vorsicht geboten.

Empfohlene Verhaltensregeln im Verdachtsfall:

Verdächtige E-Mails bzw. deren Attachments sollten auf keinen Fall von dem/der Endanwender/in geöffnet werden.

Im Privatbereich und ev. auch in Teilen des kommerziellen Bereiches wird ein sofortiges Löschen von offensichtlich unsinnigen oder sonst wie verdächtigen Mails empfehlenswert sein, um der Gefahr einer Vireninfektion zu begegnen. In Bereichen, wo dies entweder aufgrund gesetzlicher Vorschriften oder kommerzieller Überlegungen nicht möglich ist, ist dafür zu sorgen, dass verdächtige E-Mails in entsprechend sicherer Umgebung geöffnet und analysiert werden können. Dazu sind sog. “Quarantänebereiche” einzurichten, in denen die Mails von Spezialistinnen bzw. Spezialisten untersucht und weiterbehandelt werden können. Benutzer/innen müssen wissen, wie sie diese Spezialistinnen bzw. Spezialisten erreichen oder Mails an solche Bereiche weiterleiten können.

Maßnahmen bei ausgehender E-Mail:

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

- Vermeidung aktiver Inhalte in E-Mails.
- Keine unnötigen E-Mails mit Scherz-Programmen und ähnlichem versenden, da diese evtl. einen Computer-Virus enthalten können.
- Keinen Aufforderungen zur Weiterleitung von Warnungen, Mails oder Anhängen an Freundinnen bzw. Freunde, Bekannte oder Kolleginnen/Kollegen folgen, sondern direkt nur an die/den IT-Sicherheitsbeauftragte/n senden. Es handelt sich nämlich meist um irritierende und belästigende Mails mit Falschmeldungen (Hoax oder "elektronische Ente", Kettenbrief).
- Gelegentlich prüfen, ob E-Mails im Ausgangs-Postkorb stehen, die nicht von dem/der Benutzer/in selbst verfasst wurden.

Verhalten bei Downloads aus dem Internet:

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

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

SYS 4.7 Erstellung von Notfallplänen im Fall von Vireninfektionen

Relevanz: Umsetzung/Wartung;

- Die Informationswege für Notfälle sind zu planen, die zuständigen Funktionen oder Personen zu definieren, Ausweichwege für die Kommunikation und Vertretungsregeln festzulegen.
- Je nach vorliegendem Schadprogramm sind Verfahren zur differenzierten E-Mail-Filterung (z.B. Größenbeschränkung, keine Attachments, nur Post-Eingang, Filterung von bestimmten Betreffs) vorzubereiten und auch zu testen. Da E-Mail mittlerweile das zentrale Informationsmedium geworden ist, dürfen diese Systeme allenfalls kurzzeitig deaktiviert werden, damit nach wie vor Warnungen möglich sind.
- Es muss sichergestellt sein, dass bei Vorliegen eines neuen Virus die Updates der Virenschutzprogramme möglichst rasch auf Servern, Gateways und Clients eingestellt werden. Die entsprechenden Verteilwege und Maßnahmen sind vorzubereiten und selbstverständlich auch regelmäßig zu testen.

- Sollten durch einen neuen Virus die üblichen Informationswege nicht verfügbar sein, sind alternative Verfahren zur zeitnahen Warnung vorzusehen (z. B. notfalls auch durch Fax, SMS, Lautsprecherdurchsagen).
- Für den Notfall sind Backup- und Restore-Strategien zu erarbeiten, die festlegen, welche Rechner in welcher Reihenfolge in betriebsbereiten Zustand zu bringen sind, damit in kürzester Zeit eine, wenn auch eingeschränkte, Funktionsfähigkeit hergestellt werden kann.

SYS 4.8 Auswahl und Einsatz von Virenschutzprogrammen

Relevanz: Umsetzung/Wartung;

Zum Schutz vor Viren können unterschiedliche Wirkprinzipien genutzt werden.

Programme, die Speichermedien nach bekannten Viren durchsuchen, haben sich in der Vergangenheit als effektivstes und wirksamstes Mittel in der Viren-Bekämpfung erwiesen. Von Vorteil ist, dass neu erhaltene Software oder Datenträger schon vor dem ersten Einsatz geprüft werden können. Man kann daher eine Infektion mit bekannten Viren grundsätzlich vermeiden. Ein weiterer Vorteil ist, dass man durch das Virenschutzprogramm eine genauere Information über den jeweils entdeckten Virus erhält. Die bekannten Viren sind durch Spezialistinnen bzw. Spezialisten analysiert worden, so dass man weiß, ob und welche Schadensfunktionen vorhanden sind. Ein gutes Virenschutzprogramm muss daher nicht nur in der Lage sein, viele Viren zu finden, sondern sie auch möglichst exakt identifizieren. Zahlreiche Programme bieten auch die Möglichkeit einer Entfernung gefundener Viren an. Hierbei ist zu beachten, dass die Qualität dieser Entfernungsroutinen sehr unterschiedlich ist. Wenn immer möglich, sollten mit der Entfernung Spezialistinnen bzw. Spezialisten betraut werden.

Zu beachten ist, dass Virenschutzprogramme mit der Zeit ihre Wirksamkeit verlieren, da sie nur die zu ihrem Erstellungszeitpunkt bekannten Viren berücksichtigen, neu hinzugekommene jedoch meist nicht erkennen können. Daher ist eine regelmäßige Aktualisierung des Virenschutzprogramms erforderlich.

Ebenso wie andere Programme können sie durch Aufruf (transient) oder im Hintergrund (resident) genutzt werden. Die Betriebsart des Virenschutzprogramms hat entscheidenden Einfluss auf die Akzeptanz bei den Anwenderinnen/Anwendern und damit auf die tatsächlich erreichte Schutzfunktion.

Beim transienten Betrieb wird das Programm aufgerufen, durchsucht die eingestellten Teile des Computers, beendet seine Arbeit danach und macht den Speicher wieder frei. Meist löst der/die Anwender/in den Aufruf aus.

Beim residenten Betrieb wird das Virenschutzprogramm beim Start des Rechners in den Speicher geladen und verbleibt dort aktiv bis zum Ausschalten. Es verrichtet seine Tätigkeit, ohne dass der/die Anwender/in dabei mitwirkt, er/sie kann inzwischen seine/ihre eigentliche Arbeit, z.B. das Schreiben von Texten, ausführen.

Eine weitere präventive Maßnahme ist der Einsatz von *Checksummen-Prüfprogrammen*. Hierbei werden zum Schutz vor Veränderung von den zu prüfenden Dateien oder Systembereichen (z.B. Boot- und Partition-Sektor) Prüfsummen berechnet, die regelmäßig kontrolliert werden. Auf diese Weise können nicht nur Verseuchungen mit bisher unbekannten Viren erkannt werden, sondern auch andere unberechtigte Veränderungen an Dateien.

Im Wesentlichen sollte ein Virenschutzprogramm folgende Eigenschaften erfüllen:

- Der Umfang der erkannten Viren sollte möglichst groß sein und dem aktuell bekannten Bestand entsprechen, insbesondere müssen alle sehr stark verbreiteten Viren erkannt werden.
- Eine ständige Aktualisierung bezüglich neuer Viren muss vom Hersteller sichergestellt sein.
- Das Programm sollte Viren auch in komprimierter Form finden, wobei gängige Komprimierungsfunktionen wie PKZIP unterstützt werden sollten.
- Gefundene Viren müssen mit einer vollständigen Pfad-Angabe angezeigt werden.
- Das Programm muss seine eigene Virenfreiheit feststellen, bevor die Suchfunktion ausgeführt wird.
- Nach Möglichkeit muss das Produkt als residentes Programm eine permanente Virenkontrolle ermöglichen.
- Sinnvoll ist eine Funktionalität, die es erlaubt, erkannte Viren zu entfernen, ohne weitere Schäden an Programmen oder Daten zu verursachen.
- Das Programm sollte über eine Protokollierungsfunktion verfügen, die folgende Daten festhält:
  - Versionsstand des Programms,
  - Datum und Uhrzeit der Überprüfung,
  - Angabe aller benutzten Parameter,
  - Prüfergebnis mit Prüfumfang,
  - Anzahl und Identifikation der Dateien und Objekte, die nicht geprüft werden konnten.
- Das Programm sollte eine Warnung ausgeben, wenn es feststellt, dass es offensichtlich nicht aktualisiert wurde.
- Das Programm sollte eine Liste der erkennbaren Viren und ihre Beschreibung beinhalten. Darüber hinaus sind jeweils Beschreibungen von Sofortmaßnahmen und Maßnahmen zum Entfernen des Virus anzugeben.

SYS 4.9 Verhaltensregeln bei Auftreten eines Virus

Relevanz: Umsetzung/Wartung; Anwender/innen;

Gibt es Anzeichen, dass ein Rechner von einem Virus befallen ist (z.B. Programmdateien werden länger, unerklärliches Systemverhalten, nicht auffindbare Dateien, veränderte Dateiinhalte, ständige Verringerung des freien Speicherplatzes, ohne dass etwas abgespeichert wurde), so sind zur Feststellung des Virus und zur anschließenden Beseitigung folgende Schritte durchzuführen.

Grundregel: Falls möglich, sollten fachkundige Betreuer/innen (Administrator, Bereichs-IT-Sicherheitsverantwortliche/r, Helpdesk) zu Hilfe geholt werden.

Falls dies nicht möglich ist, sollten folgende Schritte durchgeführt werden:

- Beenden der laufenden Programme und Abschalten des Rechners.
- Einlegen einer einwandfreien, schreibgeschützten System-Diskette (”Notfall-Diskette”) in Laufwerk A:.
- Booten des Rechners von dieser Diskette (evtl. vorher Boot-Reihenfolge im BIOS-Setup ändern, siehe SYS 4.2 „Generelle Maßnahmen zur Vorbeugung gegen Virenbefall“).
- Überprüfen des Rechners mit einem aktuellen Virenschutzprogramm um festzustellen, ob tatsächlich ein Virus aufgetreten ist und um welchen Virus es sich ggf. handelt.
- Entfernen des Virus abhängig vom jeweiligen Virustyp.

- Erneute Überprüfung der Festplatte mit dem Viren-Suchprogramm.
- Untersuchung aller anderen Datenträger (Disketten, Wechselplatten) auf Virenbefall und Entfernung eventuell vorhandener Viren.
- Es sollte versucht werden, die Quelle der Vireninfektion festzustellen. Ist die Quelle auf Original-Datenträger zurückzuführen, dann sollte der Hersteller informiert werden. Liegt die Quelle in Dateien oder E-Mail, so ist der/die Ersteller/in der Datei zu unterrichten.
- Warnung an andere IT-Benutzer/innen, wenn ein Datenaustausch vom infizierten Rechner erfolgte.

Sollte der Virus Daten gelöscht oder verändert haben, so muss versucht werden, die Daten aus den Datensicherungen und die Programme aus den Sicherungskopien der Programme (vgl. BCP 1.6 „Sicherungskopie der eingesetzten Software“) zu rekonstruieren.

Anschließend ist nochmals Schritt 7 zu wiederholen.

SYS 4.10 Warnsystem für Computerviren – Aktualisierung von Virenschutzprogrammen

Relevanz: Umsetzung/Wartung; Anwender/innen;

Im Zusammenhang mit Computerviren ist die permanente Aktualität des verwendeten Virenschutzprogrammes von größter Wichtigkeit. Bereits bei der Beschaffung von Virenschutzprogrammen ist daher für die Aktualisierbarkeit und die Versorgung von entsprechenden Updates durch den Hersteller Sorge zu tragen. Darüber hinaus sind die Verantwortlichkeiten für die regelmäßig durchzuführenden Aktualisierungen innerhalb der Organisation zu definieren.

Neben der Aktualisierung der eingesetzten Software ist auch die Information über neue Computerviren, sowie Informationen über empfohlene aktive und passive Gegenmaßnahmen, besonders wichtig. Dabei genügt es oft nicht, sich nur auf die periodischen Updates des Virenschutzprogramm-Herstellers zu verlassen. Im Bereich der öffentlichen Verwaltung wird ein eigenes Viren- und Incident-Warnsystem (CIRCA - Computer Incident Response Coordination Austria) eingerichtet (vgl. IKT-Board-Beschluss [IKTB-170902-3] vom 17.09.2002). Dieses wird in der ersten Phase durch das Krisenmanagement des Bundeskanzleramts (BKA) betrieben. Mit einem Warnsystem für Computerviren und sonstigen schädigenden Inhalten soll eine Informationsbasis und ein Verteilsystem für derartige Informationen geschaffen werden, welches den geeigneten Stellen der öffentlichen Verwaltung und der Wirtschaft zur Verfügung steht.

5.5 Arbeitsplatz-IT-Systeme

Relevanz: Umsetzung/Wartung; Anwender/innen;

SYS 5.1 Herausgabe einer PC-Richtlinie

Relevanz: Umsetzung/Wartung; Anwender/innen;

Um einen sicheren und ordnungsgemäßen Einsatz von Personalcomputern in größeren Organisationen zu gewährleisten, sollte eine PC-Richtlinie erstellt werden, in der verbindlich vorgeschrieben wird, welche Randbedingungen eingehalten werden müssen und welche IT-Sicherheitsmaßnahmen zu ergreifen sind. Diese PC-Richtlinie soll zumindest den Einsatz von unvernetzten PCs regeln; werden PCs vernetzt betrieben oder als intelligente Terminals genutzt, ist die Richtlinie um diese Punkte zu erweitern. Im Folgenden wird grob umrissen, welche Inhalte für eine solche PC-Richtlinie sinnvoll sind.

Möglicher inhaltlicher Aufbau einer PC-Richtlinie:

- *Zielsetzung und Begriffsdefinitionen:*
  Dieser erste Teil der PC-Richtlinie soll dazu dienen, die PC-Anwender/innen für IT-Sicherheit zu sensibilisieren und zu motivieren. Gleichzeitig werden die für das gemeinsame Verständnis notwendigen Begriffe definiert und eine einheitliche Sprachregelung geschaffen.
- *Geltungsbereich:*
  In diesem Teil muss verbindlich festgelegt werden, für welche Teile des Unternehmens bzw. der Behörde die PC-Richtlinie gilt.
- *Rechtsvorschriften und interne Regelungen:*
  Hier wird auf wichtige Rechtsvorschriften (z.B. das Datenschutzgesetz 2000 (DSG2000), BGBl. I Nr. 165/1999 i.d.g.F. und das Urheberrechtsgesetz, BGBl. Nr. 111/1936 i.d.g.F.) hingewiesen. Darüber hinaus kann diese Stelle genutzt werden, um alle relevanten betriebsinternen Regelungen aufzuführen.
- *Verantwortungsverteilung:*
  In diesem Teil wird definiert, wer im Zusammenhang mit dem PC-Einsatz welche Verantwortung trägt. Dabei sind insbesondere die Funktionen IT-Benutzer/innen, Vorgesetzte, PC-Administratoren, Datenschutz-/IT-Sicherheitsbeauftragte, Bereichs-IT-Sicherheitsbeauftragte und Applikations-/Projektverantwortliche zu unterscheiden.
- *Umzusetzende und einzuhaltende IT-Sicherheitsmaßnahmen:*
  Im letzten Teil der PC-Richtlinie ist festzulegen, welche IT-Sicherheitsmaßnahmen von dem/der IT-Benutzer/in einzuhalten bzw. umzusetzen sind. Es kann je nach Schutzbedarf auch über die IT-Grundschutzmaßnahmen hinausgehen.

Die PC-Richtlinie muss regelmäßig - insbesondere im Hinblick auf die IT-Sicherheitsmaßnahmen - aktualisiert werden.

Es ist dafür Sorge zu tragen, dass jede/r PC-Benutzer/in ein Exemplar dieser Richtlinie besitzt und dass die Einhaltung regelmäßig überprüft wird.

Sind Telearbeiter/innen im Unternehmen bzw. in der Behörde beschäftigt, sollte die PC-Richtlinie um die dafür spezifischen Regelungen ergänzt werden. Vgl. dazu Kapitel „Telearbeit“.

SYS 5.2 Einführung eines PC-Checkheftes

Relevanz: Umsetzung/Wartung; Anwender/innen;

Um die durchgeführten IT-Sicherheitsmaßnahmen am PC zu dokumentieren, kann ein PC-Checkheft eingeführt werden, in dem der/die PC-Nutzer/in die wichtigsten Angaben zum Gerät dokumentiert. Diese Maßnahme bietet sich in erster Linie für kleine und mittlere Organisationen an, große Organisationen führen und verwalten diese Dokumentationen im Allgemeinen zentral.

Kommt ein PC-Checkheft zum Einsatz, so sollte es folgende Informationen enthalten:

- Name der PC-Benutzerin bzw. des PC-Benutzers,
- Aufstellungsort des PC,
- Beschreibung der Konfiguration,
- Zugangsmittel,
- eingesetzte Hard- und Software,
- planmäßige Zeitpunkte für die Datensicherungen,
- durchgeführte Wartungen und Reparaturen,
- durchgeführte Viren-Kontrollen,
- Zeitpunkt von Passwort-Änderungen,
- zur Verfügung stehendes Zubehör,
- durchgeführte Revisionen,
- Ansprechpartner für Problemfälle und
- Zeitpunkte der durchgeführten Datensicherungen.

Das Führen eines solchen PC-Checkheftes erleichtert Kontrolltätigkeiten und unterstützt eine notwendige Selbstkontrolle der PC-Benutzerin bzw. des PC-Benutzers, damit sie/er regelmäßig Datensicherungen, Passwort-Änderungen und Viren-Checks durchführt (sofern dies nicht zentral erfolgt (s.o.)).

SYS 5.3 Sicherung von Wechselmedien

Relevanz: Umsetzung/Wartung; Anwender/innen;

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

Als derartige Risiken wären unter anderem zu nennen:

- unkontrolliertes Booten von Geräten etwa von Diskette oder CD-ROM,
- unautorisierte Installation von Software und
- unberechtigte Kopien von Daten auf Wechselmedien (Verlust der Vertraulichkeit).

Zur Verringerung dieser Bedrohungen stehen - abhängig von der Art der Wechselmedien und dem zugrunde liegenden Betriebssystem - eine Reihe von Möglichkeiten zur Verfügung, die unten beispielhaft angeführt werden. Es ist aber zu betonen, dass in vielen Fällen eine völlige Sperre der Wechselmedien entweder technisch nicht möglich oder aber aus betrieblichen Gründen nicht durchsetzbar ist. Hier sind zusätzliche personelle (Anweisungen, Verbote, ...) und organisatorische Maßnahmen (Kontrollen, ...) erforderlich.

Maßnahmen zur Sicherung von Wechselmedien:

- Verzicht auf Disketten-, CD-ROM-, ...Laufwerke (bzw. ihr nachträglicher Ausbau)
- (Physischer) Verschluss von Laufwerken (z.B. durch Einsatz von Diskettenschlössern).
- *(Logische) Sperre von Schnittstellen:* Viele Betriebssysteme bieten die Möglichkeit, Schnittstellen zu sperren. Dabei ist allerdings zu beachten, dass dies nicht immer technisch möglich (z.B. SCSI-Schnittstellen) und oft auch aus betrieblichen Gründen nicht durchführbar ist (z.B. ist die parallele Schnittstelle oft für den Anschluss eines Druckers offen zu halten).
- *Verblenden und Verplomben von Schnittstellen* Nach Anschluss aller erforderlichen Schnittstellen wird die Rückseite des Gerätes mit einer speziellen Abdeckung verblendet. Diese wird verplombt, so dass etwaige Manipulationen ersichtlich sind. Diese Vorgehensweise bietet einen relativ hohen Grad an Sicherheit (insbesondere an nachträglichen Nachweismöglichkeiten), es ist aber zu bedenken, dass damit die Flexibilität der Systeme stark eingeschränkt wird. Häufige Übersiedlungen, Konfigurationsänderungen etc. können die Akzeptanz dieser Maßnahme bei Benutzerinnen bzw. Benutzern und Systemverantwortlichen stark reduzieren.

Es ist auch zu bedenken, dass bei IT-Systemen im Netzwerk ein Laden von Treibern etc. etwa über das Internet oder mittels Attachments von Mails möglich ist. Hier sind entsprechende Vorkehrungen zu treffen (s. auch Kap. „Remote Access“)

SYS 5.4 Nutzung der BIOS-Sicherheitsmechanismen

Relevanz: Umsetzung/Wartung;

Moderne BIOS-Varianten bieten eine Vielzahl von Sicherheitsmechanismen an, mit denen sich die Benutzer/innen oder die Systemadministration vertraut machen sollten. Auf keinen Fall sollten aber ungeschulte Benutzer/innen BIOS-Einträge verändern, da hierdurch schwerwiegende Schäden verursacht werden können.

- *Passwortschutz:*
  Bei den meisten BIOS-Varianten kann ein Passwortschutz aktiviert werden. Dieser kann verhältnismäßig einfach überwunden werden, sollte aber auf jeden Fall benutzt werden, wenn keine anderen Zugriffsschutzmechanismen zur Verfügung stehen. Meist kann ausgewählt werden, ob das Passwort vor jedem Rechnerstart oder nur vor Zugriffen auf die BIOS-Einstellungen überprüft werden soll. Teilweise können sogar verschiedene Passwörter für diese Prüfungen benutzt werden. Um zu verhindern, dass Unbefugte die BIOS-Einstellungen ändern, sollte das Setup- oder Administrator-Passwort immer aktiviert werden. Mit einigen (leider wenigen) BIOS-Varianten kann zusätzlich der Zugriff auf die Diskettenlaufwerke durch ein Passwort geschützt werden. Dies sollte benutzt werden, um das unbefugte Einspielen von Software oder das unbemerkte Kopieren von Daten zu verhindern.

- *Boot-Reihenfolge:*
  Die Boot-Reihenfolge sollte so eingestellt sein, dass immer als Erstes von der Festplatte gebootet wird. Beispielsweise sollte also _C,A_ eingestellt werden. Dies schützt vor der Infektion mit Boot-Viren, falls versehentlich eine Diskette im Laufwerksschacht vergessen wird, spart Zeit und schont das Diskettenlaufwerk. Je nach verwendetem BIOS und Betriebssystem muss auch das Booten von anderen austauschbaren Datenträgern wie CD-ROMs verhindert werden. Ohne eine Umstellung der Boot-Reihenfolge können auch weitere Sicherheitsmaßnahmen wie etwa Zugriffsschutzmechanismen umgangen werden. Ein Beispiel hierfür ist das Starten eines anderen Betriebssystems, so dass gesetzte Sicherheitsattribute ignoriert werden. Generell sollte die Wirksamkeit der Umstellung der Boot-Reihenfolge durch einen Boot-Versuch geprüft werden, da einige Controller die interne Reihenfolge außer Betrieb nehmen und eine getrennte Einstellung erfordern.
- *Virenschutz, Virus-Warnfunktion:*
  Wird diese Funktion aktiviert, verlangt der Rechner vor einer Veränderung des Bootsektors bzw. des MBR (Master Boot Record) eine Bestätigung, ob diese durchgeführt werden darf.

SYS 5.5 Einsatz eines Verschlüsselungsproduktes für Arbeitsplatzsysteme

Relevanz: Umsetzung/Wartung; Anwender/innen;

Sind auf einem Arbeitsplatzsystem besonders schutzwürdige Daten gespeichert und wird dieses System in einer nicht oder nur unzureichend geschützten Umgebung betrieben oder aufbewahrt, so ist der Einsatz eines Verschlüsselungsproduktes zu erwägen. Dies gilt in besonderem Maße - aber nicht ausschließlich - für mobile IT-Geräte (Notebooks etc., vgl. auch INF 5.1 „Geeignete Aufstellung eines Arbeitsplatz-IT-Systems“ und INF 5.4 „Nutzung und Aufbewahrung mobiler IT-Geräte“).

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

Von zentraler Bedeutung für die Sicherheit der Verschlüsselung sind dabei die folgenden Punkte:

- Der verwendete Verschlüsselungsalgorithmus muss so konstruiert sein, dass es ohne Kenntnis des verwendeten Schlüssels praktisch nicht möglich ist, den Klartext aus dem verschlüsselten Text zu rekonstruieren. Praktisch nicht möglich bedeutet dabei, dass der erforderliche Aufwand zum Brechen des Algorithmus bzw. zum Entschlüsseln deutlich höher ist als der dadurch erzielbare Informationsgewinn.
- Der Schlüssel ist geeignet zu wählen. Nach Möglichkeit sollte ein Schlüssel zufällig erzeugt werden. Wenn es möglich ist, einen Schlüssel wie ein Passwort zu wählen, sollten die diesbezüglichen Regeln aus SYS 1.5 „Regelungen des Passwortgebrauches“ beachtet werden.
- Der verschlüsselte Text und die Schlüssel dürfen nicht zusammen auf einem Datenträger gespeichert werden. Es bietet sich an, den Schlüssel und die zugehörige Passphrase getrennt und geschützt zu halten. Ein hohes Maß an Sicherheit wird erreicht, wenn der Schlüssel auf einer Chipkarte gehalten wird.

Eine Verschlüsselung kann online oder offline vorgenommen werden. Online bedeutet, dass sämtliche Daten der Festplatte (bzw. einer Partition) verschlüsselt werden, ohne dass die Benutzer/innen dies aktiv veranlassen müssen. Eine Offline-Verschlüsselung wird explizit von dem/der Benutzer/in initiiert. Sie/er muss dann auch entscheiden, welche Dateien verschlüsselt werden sollen.

Die Benutzer/innen sind im Umgang mit dem Verschlüsselungsprogramm zu schulen.

SYS 5.6 Verhinderung der unautorisierten Nutzung von Rechnermikrofonen und Videokameras

Relevanz: Umsetzung/Wartung;

Das Mikrofon bzw. die Videokamera eines vernetzten Rechners kann von denjenigen benutzt werden, die Zugriffsrechte auf die entsprechende Gerätedatei haben. Der Zugriff auf die Gerätedatei sollte nur möglich sein, solange jemand an dem IT-System arbeitet. Wenn die Benutzung eines vorhandenen Mikrofons oder einer Kamera generell verhindert werden soll, müssen diese - wenn möglich - ausgeschaltet oder physikalisch vom Gerät getrennt werden.

Falls das Mikrofon bzw. die Kamera in den Rechner (bzw. den Bildschirm) integriert ist und nur durch Software ein- und ausgeschaltet werden kann, müssen die Zugriffsrechte so gesetzt sein, dass es keine Unbefugten benutzen können.

Es ist zu prüfen, ob Zugriffsrechte und Eigentümer bei einem Zugriff auf die Gerätedatei verändert werden. Falls dies der Fall ist oder falls gewünscht ist, dass jede/r Benutzer/in das Mikrofon bzw. die Kamera benutzen kann (und nicht nur in Einzelfällen eine Freigabe durch den Systemadministrator erfolgen soll), muss die Systemadministration ein Kommando zur Verfügung stellen, das

- nur aktiviert werden kann, wenn jemand an dem IT-System angemeldet ist,
- nur durch diese/n Benutzer/in aktiviert werden kann und
- die Zugriffsberechtigungen dem/der Benutzer/in nach dem Abmelden wieder entzieht.

Wünschenswert wäre es auch, Mikrofon und Kamera nach einer voreingestellten Zeitspanne ohne Aktivität automatisch abzuschalten (Timeout).

SYS 5.7 Software-Reinstallation bei Arbeitsplatzrechnern

Relevanz: Umsetzung/Wartung;

Bei Arbeitsplatzrechnern kann es häufiger zu Problemen mit dem Betriebssystem oder den Anwendungen kommen, die nur durch den Benutzersupport wieder behoben werden können. Dies kann z.B. durch Softwarefehler, Konfigurationsänderungen, Aufspielen neuer Software oder durch Viren verursacht werden.

Damit die Administratoren bei den oben beschriebenen Problemen auf den Benutzerrechnern nicht zeitaufwendig nach Fehlern suchen müssen, sollte eine Software-Reinstallation der Standardkonfiguration vorgenommen werden.

Dafür muss zunächst der Rechner eindeutig identifiziert werden und dann über eine entsprechende Dokumentation oder ein Programm anhand dieser Identifikation genau ermittelt werden, welche Software in welcher Konfiguration auf genau diesem Rechner installiert werden muss. Dabei ist es hilfreich, wenn sich die Systeme weitestgehend gleichen, zumindest in Bereichen mit ähnlicher Aufgabenstellung.

Es empfiehlt sich, die Festplatte des Arbeitsplatzrechners neu zu formatieren und anschließend die erforderliche Software und Daten neu aufzuspielen.

Eine Software-Reinstallation kann auf verschiedene Weise durchgeführt werden, so gibt es z.B. spezielle Programme, die eine vorgegebene Konfiguration von einem Server auf den neu zu installierenden Arbeitsplatzrechner überspielen. Hierbei ist zu beachten, dass solche Arbeiten meist in zweierlei Hinsicht zeitkritisch sind: Die Neueinrichtung sollte möglichst schnell erfolgen können, damit das IT-System wieder verfügbar ist, und das Netz sollte möglichst wenig belastet werden. Dies ist insbesondere bei Schulungsrechnern oder PC-Pools wichtig.

Natürlich kann eine Reinstallation auch “von Hand” vorgenommen werden. Zu diesem Zweck sollte als erstes eine Standardinstallation vorgenommen werden. Im Anschluss daran werden die Besonderheiten der einzelnen Rechner kopiert, wie spezielle Gerätetreiber, andere Konfigurationsdateien oder spezielle Software. Dafür müssen diese allerdings vorkonfiguriert verfügbar sein, z.B. auf dem Netz oder auf mobilen Datenträgern. Ein aktuelles Virensuchprogramm muss anschließend zum Einsatz kommen.

SYS 5.8 Sichere Initialkonfiguration und Zertifikatsgrundeinstellung

Relevanz: Umsetzung/Wartung;

Bei Neuinstallationen von Betriebssystemen und Software berücksichtigen die standardmäßigen und herstellerseitigen Grundeinstellungen kaum sicherheitstechnische Aspekte. Somit werden im Zuge von Standardkonfigurationen zur Verfügung stehende Sicherheitsmechanismen oft nicht aktiviert, bzw. bieten grundsätzliche Fehlkonfigurationen potentielle Sicherheitsrisken.

Um dem Entgegenzuwirken ist die Verwendung von geprüften Initialkonfigurationen zu bevorzugen. Derartige Konfigurationen sollten sowohl für das Betriebssystem (vorrangig) aber auch für die verwendete Software von der Administration zur Verfügung gestellt werden.

Im Bundesbereich ist gemäß dem IKT-Board Beschluss [IKTB-170902-7] eine definierte sichere Initialkonfiguration zu verwenden. Eine entsprechend dokumentierte Initialkonfiguration wird im Rahmen des Online-Angebotes des Chief Information Office des Bundes zur Verfügung stehen.

Zertifikatsgrundeinstellung

Voreingestellt in Betriebssystemen bzw. in Internet-Programmen (zum Beispiel Browsern) ist eine Vielzahl von „vertrauenswürdigen“ Zertifizierungsstellen, deren Zertifikaten dadurch explizit vertraut wird. Dies stellt ein Sicherheitsrisiko dar, denn der/die Anwender/in hat in der Regel keine Informationen über die Vertrauenswürdigkeit der Zertifizierungsstellen bzw. ob deren Zertifikate zwischenzeitlich bereits kompromittiert wurden. Demnach sollten in der Initialkonfiguration alle im Zertifikatsspeicher vorkonfigurierten Wurzelzertifikate (vertrauenswürdige Stammzertifikate) entfernt werden, bzw. durch einen definierten Satz an als vertrauenswürdig anerkannten Zertifikaten ersetzt werden.

Nach IKT-Board-Beschluss [IKTB-040402-2] sind alle in der Bundesverwaltung auszuliefernden Arbeitsstationen initial so auszuliefern, dass keinem Zertifizierungsdienst automatisch vertraut wird. Das implizite Vertrauen kann allen Zertifizierungsdiensten und den zugeordneten Diensten, die der EU Signaturrichtlinie ([EU 1999/93/EG] i.d.g.F. Art. 5.1) genügen, explizit ausgesprochen werden, wenn in den Arbeitsstationen die Mechanismen des Widerrufs hinreichend umgesetzt sind. Anderen Zertifizierungsdiensten kann im bereichs-/ressortübergreifenden Datenverkehr nur dann dass Vertrauen im System implizit gegeben werden, wenn dies in der allgemeinen Strategie explizit festgehalten ist.

SYS 5.9 Systemdateien

Relevanz: Umsetzung/Wartung;

Das unbeabsichtigte und unkundige Ändern bzw. Löschen von Systemdateien kann verheerende Auswirkungen auf die Stabilität und Zuverlässigkeit des IT-Systems haben. Eine strikte Rechtevergabe bei diesen Dateien ist daher besonders zu empfehlen.

Im Allgemeinen sollte nur Administratoren der Zugriff auf diese Dateien gewährt werden. Darüber hinaus ist eine regelmäßige Verifizierung der Integrität von Systemdateien sinnvoll (vgl. BET 2.5). Für diesen Zweck stellen viele Betriebssysteme bereits eigene Tools zur Verfügung.

5.6 System-/Netzwerkadministration

Relevanz: Umsetzung/Wartung; Anwender/innen;

Zur Unterstützung der System-/Netzwerkadministration ist der Einsatz von entsprechenden Tools (z.B. CAD-Programmen, speziellen Tools für Netzpläne, Kabelmanagementtools im Zusammenhang mit Systemmanagementtools o.ä.) empfehlenswert. Eine konsequente Aktualisierung aller Informationen bei Umbauten oder Erweiterungen ist ebenso zu gewährleisten wie eine eindeutige und nachvollziehbare Dokumentation (vgl. auch INF 4.1 „Lagepläne der Versorgungsleitungen“ und ENT 2.4 „Dokumentation und Kennzeichnung der Verkabelung“).

Gerade im Zusammenhang mit dem Absichern von Netzwerken gibt es eine Reihe weiterführender Literatur. Exemplarisch sei an dieser Stelle „The 60 Minute Network Security Guide“ der NSA [NSA-SD7] genannt.

SYS 6.1 Sicherstellung einer konsistenten Systemverwaltung

Relevanz: Umsetzung/Wartung; Anwender/innen;

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

Um Fehler zu vermeiden, soll unter dem Super-User-Login nur gearbeitet werden, wenn es notwendig ist. Andere Arbeiten soll auch der Administrator nicht unter der Administrator-Kennung erledigen. Insbesondere dürfen keine Programme anderer Benutzer/innen unter der Administrator-Kennung aufgerufen werden. Ferner sollte die routinemäßige Systemverwaltung (z.B. Backup, Einrichten einer/eines neuen Benutzers/Benutzerin) nur menügesteuert durchgeführt werden können.

Für alle Administratoren sind zusätzliche Benutzerkennungen einzurichten, die nur über die eingeschränkten Rechte verfügen, die die Administratoren zur Aufgabenerfüllung außerhalb der Administration benötigen. Für Arbeiten, die nicht der Administration dienen, sollen die Administratoren ausschließlich diese zusätzlichen Benutzerkennungen verwenden.

Falls das Betriebssystem erlaubt, sollte der Administrator grundsätzlich nicht als Superuser, sondern unter seiner persönlichen Benutzerkennung einsteigen und erst dann in die Superuser-Rolle wechseln.

Bekannte Kennungen, wie etwa root, guest oder administrator, sind zu löschen, stillzulegen oder nach Bedarf zu modifizieren. Bekannte Passwörter (Firmenkennungen und Firmen-Passwörter) sind zu löschen bzw. zu ändern, insbesondere bei Netzwerkkomponenten (Router, Switches, ...).

Alle durchgeführten Änderungen sollten dokumentiert werden, um diese nachvollziehbar zu machen und die Aufgabenteilung zu erleichtern.

SYS 6.2 Sorgfältige Durchführung von Konfigurationsänderungen

Relevanz: Umsetzung/Wartung;

Die Durchführung von Änderungen an einem IT-System im Echtbetrieb ist immer als kritisch einzustufen und entsprechend sorgfältig muss hierbei vorgegangen werden.

Insbesondere für mittlere und große Organisationen ist es unerlässlich, jede Konfigurationsänderung in einem Referenzsystem vorzubereiten und zu testen.

Bevor mit Änderungen am System begonnen wird, muss als Erstes die alte Konfiguration gesichert werden, so dass sie schnell verfügbar ist, wenn Probleme mit der neuen Konfiguration auftreten.

Bei vernetzten IT-Systemen müssen die Benutzer/innen rechtzeitig über die Durchführung von Wartungsarbeiten informiert werden, damit sie zum einen ihre Planung auf eine zeitweise Systemabschaltung einrichten können, und damit sie zum anderen nach Änderungen auftretende Probleme richtig zuordnen können.

Die Konfigurationsänderungen sollten immer nur schrittweise durchgeführt werden. Zwischendurch sollte immer wieder überprüft werden, ob die Änderungen korrekt durchgeführt wurden und das IT-System sowie die betroffenen Applikationen noch lauffähig sind.

Bei Änderungen an Systemdateien ist anschließend ein Neustart durchzuführen, um zu überprüfen, ob sich das IT-System korrekt starten lässt. Für Problemfälle sind alle für einen Notstart benötigten Datenträger vorrätig zu halten, z.B. Boot-Disketten, Start-CD-ROM.

Komplexere Konfigurationsänderungen sollten möglichst nicht in den Originaldateien vorgenommen werden, sondern in Kopien. Alle durchgeführten Änderungen sollten von einem Kollegen überprüft werden, bevor sie in den Echtbetrieb übernommen werden.

Bei IT-Systemen mit hohen Verfügbarkeitsanforderungen ist auf Ersatzsysteme zurück zu greifen bzw. zumindest ein eingeschränkter IT-Betrieb zu gewährleisten. Das Vorgehen kann sich dabei idealerweise nach dem Disaster Recovery Handbuch (vgl. Kap. Disaster Recovery und Business Continuity Planung) richten.

Die durchgeführten Konfigurationsänderungen sollten Schritt für Schritt notiert werden, so dass bei auftretenden Problemen das IT-System durch sukzessive Rücknahme der Änderungen wieder in einen lauffähigen Zustand gebracht werden kann.

SYS 6.3 Ist-Aufnahme der aktuellen Netzsituation

Relevanz: Umsetzung/Wartung;

Die Bestandsaufnahme der aktuellen Netzsituation ist Voraussetzung für

- eine gezielte Sicherheitsanalyse des bestehenden Netzes sowie für
- die Erweiterung eines bestehenden Netzes.

Hierzu ist eine Ist-Aufnahme mit einhergehender Dokumentation der folgenden Aspekte, die z.T. aufeinander aufbauen, notwendig:

- Netztopographie,
- Netztopologie,
- verwendete Netzprotokolle,
- Kommunikationsübergänge im LAN und zum WAN sowie
- Netzperformance und Verkehrsfluss.

Unter der Topographie eines Netzes wird die rein physikalische Struktur eines Netzes in Form der Kabelführung verstanden. Im Gegensatz dazu handelt es sich bei der Netztopologie um die logische Struktur eines Netzes. Die Topographie und Topologie eines Netzes sind nicht notwendig identisch.

SYS 6.4 Analyse der aktuellen Netzsituation

Relevanz: Umsetzung/Wartung;

Diese Maßnahme baut auf den Ergebnissen der Ist-Aufnahme nach SYS 6.3 „Ist-Aufnahme der aktuellen Netzsituation“ auf und erfordert spezielle Kenntnisse im Bereich der Netztopologie, der Netztopographie und von netzspezifischen Schwachstellen. Darüber hinaus ist Erfahrung bei der Beurteilung der eingesetzten individuellen IT-Anwendungen hinsichtlich Vertraulichkeit, Integrität bzw. Verfügbarkeit notwendig.

Eine Analyse der aktuellen Netzsituation besteht im Wesentlichen aus einer Strukturanalyse, einer Schutzbedarfsfeststellung und einer Schwachstellenanalyse.

Strukturanalyse

Diese besteht aus einer Analyse der nach SYS 6.3 „Ist-Aufnahme der aktuellen Netzsituation“ angelegten Dokumentationen. Die Strukturanalyse muss von einem Analyseteam durchgeführt werden, das in der Lage ist, alle möglichen Kommunikationsbeziehungen nachzuvollziehen oder auch herleiten zu können.

Als Ergebnis muss das Analyseteam die Funktionsweise des Netzes verstanden haben und über die prinzipiellen Kommunikationsmöglichkeiten informiert sein. Häufig lassen sich bei der Strukturanalyse bereits konzeptionelle Schwächen des Netzes identifizieren.

Detaillierte Schutzbedarfsfeststellung

Bei besonders schutzwürdigen Applikationen sind in einer detaillierten Schutzbedarfsfeststellung zusätzlich die Anforderungen an Vertraulichkeit, Verfügbarkeit und Integrität in einzelnen Netzbereichen bzw. Segmenten zu berücksichtigen.

Hierzu ist es notwendig festzustellen, welche Anforderungen auf Grund der verschiedenen IT-Verfahren bestehen und wie diese auf die gegebene Netzsegmentierung Einfluss nehmen. Als Ergebnis muss erkenntlich sein, in welchen Netzsegmenten besondere Sicherheitsanforderungen bestehen.

Analyse von Schwachstellen im Netz

Basierend auf den bisher vorliegenden Ergebnissen erfolgt eine Analyse der Schwachpunkte des Netzes.

Hierzu gehört insbesondere bei entsprechenden Verfügbarkeitsanforderungen die Identifizierung von nicht redundant ausgelegten Netzkomponenten (Single-Point-of-Failures). Weiterhin müssen die Bereiche benannt werden, in denen die Anforderungen an Verfügbarkeit, Vertraulichkeit oder Integrität nicht eingehalten werden können bzw. besonderer Aufmerksamkeit bedürfen. Zudem ist festzustellen, ob die gewählte Segmentierung hinsichtlich Bandbreite und Performance geeignet ist.

Es ist zu beachten, dass diese Maßnahme insbesondere in der Designphase für ein neues Netz oder einen neuen Netzteil sinnvoll ist, Änderungen in bestehenden Netzen können aus wirtschaftlichen Aspekten oft sehr schwierig sein.

SYS 6.5 Entwicklung eines Netzkonzeptes

Relevanz: Umsetzung/Wartung;

Um den Anforderungen bezüglich Verfügbarkeit (auch Bandbreite und Performance), Vertraulichkeit und Integrität zu genügen, muss der Aufbau, die Änderung bzw. die Erweiterung eines Netzes sorgfältig geplant werden. Hierzu dient die Erstellung eines Netzkonzeptes.

Die Entwicklung eines Netzkonzeptes unterteilt sich in einen analytischen und einen konzeptionellen Teil:

Analyse

Zunächst ist zu unterscheiden, ob ein bestehendes Netz zu erweitern bzw. zu verändern ist oder ob das Netz vollständig neu aufgebaut werden soll.

Im ersten Fall sind vorab die Maßnahmen SYS 6.3 „Ist-Aufnahme der aktuellen Netzsituation“ und SYS 6.4 „Analyse der aktuellen Netzsituation“ zu bearbeiten. Im zweiten Fall entfallen diese Maßnahmen. Stattdessen sind die Anforderungen an die Netzkommunikation zu ermitteln sowie eine Schutzbedarfsfeststellung des zukünftigen Netzes durchzuführen.

Zur Ermittlung der Kommunikationsanforderungen ist der zukünftig zu erwartende Daten- und Verkehrsfluss zwischen logischen oder organisatorischen Einheiten festzustellen, da die zu erwartende Last die Segmentierung des zukünftigen Netzes beeinflussen muss. Die notwendigen logischen bzw. physikalischen Kommunikationsbeziehungen (dienste-, anwender-, gruppenbezogen) sind ebenfalls zu eruieren und die Kommunikationsübergänge zur LAN/LAN-Kopplung oder über ein WAN zu ermitteln.

Die Schutzbedarfsanforderungen des Netzes werden aus denen der geplanten oder bereits bestehenden IT-Verfahren abgeleitet. Daraus werden physikalische und logische Segmentstrukturen gefolgert, so dass diesen Anforderungen (z.B. hinsichtlich Vertraulichkeit) durch eine Realisierung des Netzes Rechnung getragen werden kann. Zum Beispiel bestimmt der Schutzbedarf einer IT-Anwendung die zukünftige Segmentierung des Netzes.

Schließlich muss versucht werden, die abgeleiteten Kommunikationsbeziehungen mit den Schutzbedarfsanforderungen zu harmonisieren. Unter Umständen sind hierzu Kommunikationsbeziehungen einzuschränken, um dem festgestellten Schutzbedarf gerecht zu werden.

Abschließend sind die verfügbaren Ressourcen zu ermitteln. Hierzu gehören sowohl Personalressourcen, die erforderlich sind, um ein Konzept zu erstellen und umzusetzen bzw. um das Netz zu betreiben, als auch die hierfür notwendigen finanziellen Ressourcen.

Die Ergebnisse sind entsprechend zu dokumentieren.

Konzeption

Im nächsten Schritt sind die Netzstruktur und die zu beachtenden Randbedingungen zu entwickeln. Dabei sind neben den oben genannten Gesichtspunkten auch die künftig zu erwartenden Anforderungen (z.B. hinsichtlich Bandbreite) sowie die örtlichen Gegebenheiten zu berücksichtigen.

Die Erstellung eines Netzkonzeptes erfolgt analog SYS 6.3 „Ist-Aufnahme der aktuellen Netzsituation“ und besteht danach prinzipiell aus den folgenden Schritten, wobei diese Schritte nicht in jedem Fall streng aufeinander folgend ausgeführt werden können. In einigen Teilen beeinflussen sich die Ergebnisse der Schritte gegenseitig, so dass eine regelmäßige Überprüfung und Konsolidierung der Teilergebnisse vorgenommen werden muss.

Konzeption der Netztopographie und der Netztopologie, der physikalischen und logischen Segmentierung

Konzeption der verwendeten Netzprotokolle

Konzeption von Kommunikationsübergängen im LAN und WAN

SYS 6.6 Entwicklung eines Netzmanagementkonzeptes

Relevanz: Umsetzung/Wartung;

Netzmanagement umfasst die Gesamtheit der Vorkehrungen und Aktivitäten zur Sicherstellung des effektiven Einsatzes eines Netzes. Hierzu gehört beispielsweise die Überwachung der Netzkomponenten auf ihre korrekte Funktion, das Monitoring der Netzperformance und die zentrale Konfiguration der Netzkomponenten.

Netzmanagement ist in erster Linie eine organisatorische Problemstellung, deren Lösung mit technischen Mitteln - einem Netzmanagementsystem - lediglich unterstützt werden kann. Abzugrenzen vom Netzmanagement ist das Systemmanagement, welches sich in erster Linie mit dem Management verteilter Systeme befasst. Hierzu gehören beispielsweise eine zentrale Verwaltung der Benutzer/innen, Softwareverteilung, Management der Anwendungen usw. In einigen Bereichen, wie z.B. dem Konfigurationsmanagement (dem Überwachen und Konsolidieren von Konfigurationen eines Systems oder einer Netzkomponente) sind Netz- und Systemmanagement nicht klar zu trennen. In der ISO/IEC-Norm 7498-4 bzw. als X.700 der ITU-T [ITU-T] ist ein Netz- und Systemmanagement-Framework definiert.

Vor der Beschaffung und dem Betrieb eines solchen Netzmanagementsystems ist im ersten Schritt ein Konzept zu erstellen, in dem alle Sicherheitsanforderungen an das Netzmanagement formuliert und angemessene Maßnahmen für den Fehler- oder Alarmfall vorgeschlagen werden. Dabei sind insbesondere die folgenden Bestandteile eines Netzmanagementkonzeptes bei der Erstellung zu berücksichtigen und in einem Gesamtzusammenhang darzustellen:

- Performancemessungen zur Netzanalyse (siehe SYS 6.4 „Analyse der aktuellen Netzsituation“),
- Reaktionen auf Fehlermeldungen der überwachten Netzkomponenten,
- Fernwartung / Remote-Control, insbesondere der aktiven Netzkomponenten,
- Generierung von Trouble-Tickets und Eskalation bei Netzproblemen,
- Protokollierung und Audit (Online und/oder Offline),
- Einbindung eventuell vorhandener proprietärer Systeme bzw. von Systemen mit unterschiedlichen Managementprotokollen (z.B. im Telekommunikationsbereich),
- Konfigurationsmanagement aller im Einsatz befindlichen IT-Systeme,
- Verteilter Zugriff auf die Netzmanagementfunktionalitäten. (Für die Administration oder für das Audit kann ein Remotezugriff auf die Netzmanagementfunktionalitäten notwendig sein. Hier ist insbesondere eine sorgfältige Definition und Vergabe der Zugriffsrechte notwendig.)

SYS 6.7 Sicherer Betrieb eines Netzmanagementsystems

Relevanz: Umsetzung/Wartung;

Für den sicheren Betrieb eines Netzmanagementtools oder eines komplexen Netzmanagementsystems, welches beispielsweise aus mehreren verschiedenen Netzmanagementtools zusammengesetzt sein kann, ist die sichere Konfiguration aller beteiligten Komponenten zu überprüfen und sicherzustellen. Hierzu gehören die Betriebssysteme, auf denen das oder die Netzmanagementsysteme betrieben werden, die zumeist notwendigen externen Datenbanken für ein Netzmanagementsystem, das verwendete Protokoll und die aktiven Netzkomponenten selbst. Vor dem Betrieb eines Netzmanagementsystems muss die Ermittlung der Anforderungen an den Betrieb und die Erstellung eines Netzmanagementkonzeptes stehen (siehe SYS 6.6 „Entwicklung eines Netzmanagementkonzeptes“).

Für den sicheren Betrieb eines Netzmanagementsystems sind folgende Daten relevant:

- Konfigurationsdaten des Netzmanagementsystems, die sich in entsprechend geschützten Verzeichnissen befinden müssen.
- Konfigurationsdaten der Netzkomponenten (Metakonfigurationsdateien), die sich ebenfalls in entsprechend geschützten Verzeichnissen befinden müssen.
- Passwortdateien für das Netzmanagementsystem. Hierbei ist beispielsweise auf die Güte des Passwortes und die Möglichkeit einer verschlüsselten Speicherung des Passwortes zu achten.
- Eine Administration der aktiven Netzkomponenten über das Netz sollte dann eingeschränkt werden und eine Administration über die lokalen Schnittstellen erfolgen, wenn die Erfüllung der Anforderungen an Vertraulichkeit und Integrität der Netzmanagementinformationen nicht gewährleistet werden kann. In diesem Fall ist auf ein zentrales Netzmanagement zu verzichten.

SYS 6.8 Sichere Konfiguration der aktiven Netzkomponenten

Relevanz: Umsetzung/Wartung;

Neben der Sicherheit von Serversystemen und Endgeräten wird die eigentliche Netzinfrastruktur mit den aktiven Netzkomponenten in vielen Fällen vernachlässigt. Gerade zentrale aktive Netzkomponenten müssen jedoch sorgfältig konfiguriert werden. Denn während durch eine fehlerhafte Konfiguration eines Serversystems nur diejenigen Benutzer/innen betroffen sind, die die entsprechenden Dienste dieses Systems nutzen, können bei einer Fehlkonfiguration eines Routers größere Teilnetze bzw. sogar das gesamte Netz ausfallen oder Daten unbemerkt kompromittiert werden.

Im Rahmen des Netzkonzeptes (siehe SYS 6.5 „Entwicklung eines Netzkonzeptes“) sollte auch die sichere Konfiguration der aktiven Netzkomponenten festgelegt werden. Dabei gilt es insbesondere Folgendes zu beachten:

- Für Router und Layer-3-Switching muss ausgewählt werden, welche Protokolle weitergeleitet und welche nicht durchgelassen werden. Dies kann durch die Implementation geeigneter Filterregeln geschehen.
- Es muss festgelegt werden, welche IT-Systeme in welcher Richtung über die Router kommunizieren. Auch dies kann durch Filterregeln realisiert werden.
- Sofern dies von den aktiven Netzkomponenten unterstützt wird, sollte festgelegt werden, welche IT-Systeme Zugriff auf die Ports der Switches und Hubs des lokalen Netzes haben. Hierzu wird die MAC-Adresse des zugreifenden IT-Systems ausgewertet und auf ihre Berechtigung hin überprüft.

Für aktive Netzkomponenten mit Routing-Funktionalität ist außerdem ein geeigneter Schutz der Routing-Updates erforderlich. Diese sind zur Aktualisierung der Routing-Tabellen erforderlich, um eine dynamische Anpassung an die aktuellen Gegebenheiten des lokalen Netzes zu erreichen. Dabei kann man zwei verschiedene Sicherheitsmechanismen unterscheiden:

- *Passwörter*
  Die Verwendung von Passwörtern schützt die so konfigurierten Router vor der Annahme von Routing-Updates durch Router, die nicht über das entsprechende Passwort verfügen. Hierdurch können also Router davor geschützt werden, falsche oder ungültige Routing-Updates anzunehmen. Der Vorteil von Passwörtern gegenüber den anderen Schutzmechanismen ist ihr geringer Overhead, der nur wenig Bandbreite und Rechenzeit benötigt.

- *Kryptographische Prüfsummen*
  Prüfsummen dienen zur Wahrung der Integrität von gültigen Routing-Updates, bzw. Message Authentication Codes schützen vor deren unbemerkten Veränderungen. Dies wird in der Regel bereits durch das Routing Protokoll gewährleistet.

Vgl. auch den NSA „Router Security Configuration Guide“ [NSA-CIS2].

SYS 6.9 Update/Upgrade von Soft- und Hardware im Netzbereich

Relevanz: Umsetzung/Wartung;

Durch ein Update von Software können Schwachstellen beseitigt oder Funktionen erweitert werden. Dies betrifft beispielsweise die Betriebssoftware von aktiven Netzkomponenten wie z.B. Switches oder Router, aber auch eine Netzmanagementsoftware. Ein Update ist insbesondere dann notwendig, wenn Schwachstellen bekannt werden, die Auswirkungen auf den sicheren Betrieb des Netzes haben, wenn Fehlfunktionen wiederholt auftauchen oder eine funktionale Erweiterung aus sicherheitstechnischen oder fachlichen Erfordernissen notwendig wird.

Auch ein Upgrade von Hardware kann in bestimmten Fällen sinnvoll sein, wenn z.B. eine neue Version eines Switches eine höhere Transfer- und Filterrate bietet. Durch diese Maßnahmen kann der Grad der Verfügbarkeit, der Integrität und der Vertraulichkeit unter Umständen erhöht werden.

Bevor ein Upgrade oder ein Update vorgenommen wird, müssen die Funktionalität, die Interoperabilität und die Zuverlässigkeit der neuen Komponenten genau geprüft werden. Dies geschieht am sinnvollsten in einem physikalisch separaten Testnetz, bevor das Update oder Upgrade in den produktiven Einsatz übernommen wird.

SYS 6.10 Festlegung einer Sicherheitsstrategie für ein Client-Server-Netz

Relevanz: Umsetzung/Wartung;

Nachfolgend wird eine methodische Vorgehensweise aufgezeigt, mittels derer eine umfassende Sicherheitsstrategie für ein Client-Server-Netz entwickelt werden kann. Abhängig vom verwendeten Betriebssystem und den eingesetzten Konfigurationen ist für die jeweilige Ausprägung individuell zu entscheiden, welche der beschriebenen Schritte anzuwenden sind.

In der Sicherheitsstrategie muss aufgezeigt werden, wie ein Client-Server-Netz für die jeweilige Organisation sicher aufgebaut, administriert und betrieben wird. Nachfolgend werden die einzelnen Entwicklungsschritte einer solchen Strategie vorgestellt:

1. Definition der Client-Server-Netzstruktur

Im ersten Schritt sind die logische Struktur des Client-Server-Netzes, insbesondere die Zuordnung der Server und der Netz-Domänen festzulegen. Nach Möglichkeit sollte auf die Verwendung von Peer-to-Peer-Funktionalitäten verzichtet werden, da diese die Sicherheit des Client-Server-Netzes beeinträchtigen können. Sofern sich dies jedoch nicht vermeiden lässt, sind verbindliche Regelungen für die Nutzung von Peer-to-Peer-Funktionalitäten zu treffen.

2. Regelung der Verantwortlichkeiten

Ein Client-Server-Netz sollte von geschulten Netzadministratoren nebst Stellvertreterinnen/ Stellvertretern sicher betrieben werden. Diese allein dürfen Sicherheitsparameter im Netz verändern. Sie sind z.B. dafür zuständig, auf den Servern den entsprechenden Verantwortlichen Administrationsrechte und -werkzeuge zur Verfügung zu stellen, damit diese die Vergabe von Datei- und Verzeichnisberechtigungen, die Freigabe der von anderen benötigten Verzeichnisse bzw. Anwendungen, den Aufbau von Benutzergruppen und -accounts sowie die Einstellung der Systemrichtlinien für Benutzer/innen, Zugriffskontrolle und Überwachung vornehmen können. Die Verantwortlichkeiten der einzelnen Benutzer/innen im Client-Server-Netz sind unter Schritt 11 dargestellt.

3. Festlegung von Namenskonventionen

Um die Verwaltung des Client-Server-Netzes zu erleichtern, sollten eindeutige Namen für die Rechner, Benutzergruppen und die Benutzer/innen verwendet werden. Zusätzlich sollten Namenskonventionen für die Freigabenamen von Verzeichnissen oder Druckern eingeführt werden. Sollen keine Rückschlüsse auf den Inhalt eines freigegebenen Verzeichnisses möglich sein, sind entsprechende Pseudonyme zu verwenden.

4. Festlegung der Regeln für Benutzeraccounts

Vor der Einrichtung von Benutzeraccounts sollten die Restriktionen, die für alle bzw. für bestimmte dieser Accounts gelten sollen, festgelegt werden. Dies betrifft insbesondere die Regelungen für Passwörter und für die Reaktion des Systems auf fehlerhafte Login-Vorgänge.

5. Einrichtung von Gruppen

Zur Vereinfachung der Administration sollten Benutzeraccounts, für die die gleichen Anforderungen gelten, zu Gruppen zusammengefasst werden. Benutzerrechte sowie Datei-, Verzeichnis- und Freigabeberechtigungen und ggf. weitere vordefinierte Funktionen werden dann den Gruppen und nicht einzelnen Benutzeraccounts zugeordnet. Die Benutzeraccounts erben die Rechte und Berechtigungen der Gruppen, denen sie angehören. So ist es z.B. denkbar, alle Mitarbeiter/innen einer Abteilung in einer Gruppe zusammenzufassen. Eine Zuweisung von Benutzerrechten und -berechtigungen an einzelne Benutzer/innen sollte nur erfolgen, wenn dies ausnahmsweise unumgänglich ist.

6. Festlegung von Benutzerrechten

Rechte gestatten einem/einer Benutzer/in die Ausführung bestimmter Aktionen auf dem System. Sie beziehen sich auf das gesamte System, sind keinem speziellen Objekt zugeordnet und können die Berechtigungen für ein Objekt außer Kraft setzen, da ein Recht Vorrang vor allen Datei- und Verzeichnisberechtigungen haben kann.

7. Festlegung der Vorgaben für Protokollierung

Bei der Konfiguration der Protokollierung ist zu beachten, dass ein Mehr an Protokollierung nicht unbedingt auch die Sicherheit des überwachten Systems erhöht. Protokolldateien, die nicht ausgewertet werden oder die auf Grund ihres Umfangs nur mit großem Aufwand auswertbar sind, führen nicht zu einer besseren Kontrolle der Systemabläufe, sondern sind letztlich nutzlos. Aus diesen Gründen sollte die Protokollierung so eingestellt werden, dass sie im Normalfall nur die wirklich bedeutsamen Ereignisse aufzeichnet. Dabei sind selbstverständlich die gesetzlichen Vorgaben, insbesondere die Anforderungen aus dem Datenschutzgesetz, vorrangig zu beachten (vgl. dazu auch Kapitel Protokollierung).

8. Regelungen zur Datenspeicherung

Es ist festzulegen, wo Benutzerdaten gespeichert werden. So ist denkbar, dass Benutzerdaten nur auf einem Server abgelegt werden. Eine Datenspeicherung auf der lokalen Festplatte ist bei diesem Modell nicht erlaubt. Möglich ist aber auch, bestimmte Benutzerdaten nur auf der lokalen Festplatte abzulegen. Nach welcher Strategie verfahren werden soll, muss jeweils im konkreten Einzelfall festgelegt werden. Eine generelle Empfehlung ist hier nicht möglich.

9. Einrichtung von Projektverzeichnissen

Um eine saubere Trennung von benutzer- und projektspezifischen Daten untereinander sowie von den Programmen und Daten des Betriebssystems durchzusetzen, sollte eine geeignete Verzeichnisstruktur festgelegt werden, mit der eine projekt- und benutzerbezogene Dateiablage unterstützt wird. So können beispielsweise zwei Hauptverzeichnisse „\ Projekte“ und „\ Benutzer“ angelegt werden, unter denen dann die Dateien und Verzeichnisse der Projekte bzw. Benutzer/innen in jeweils eigenen Unterverzeichnissen abgelegt werden.

10. Vergabe der Zugriffsrechte

Es ist festzulegen, welche Verzeichnisse und ev. welche Dateien für den Betrieb freizugeben und welche Zugriffsrechte ihnen zuzuweisen sind. Dies gilt analog für die Freigabe von Druckern.

11. Verantwortlichkeiten für Administratoren und Benutzer/innen im Client-Server-Netz

Neben der Wahrnehmung der Netzmanagementaufgaben (siehe Pkt. 2) müssen weitere Verantwortlichkeiten festgelegt werden. Es ist festzulegen, welche Verantwortung die einzelnen Administratoren im Client-Server-Netz übernehmen müssen. Dies können zum Beispiel Verantwortlichkeiten sein für

- die Auswertung der Protokolldateien auf den einzelnen Servern oder Clients,
- die Vergabe von Zugriffsrechten,
- das Hinterlegen und den Wechsel von Passwörtern und
- die Durchführung von Datensicherungen.

Auch die Endbenutzer/innen müssen in einem Client-Server-Netz bestimmte Verantwortlichkeiten übernehmen, sofern ihnen Rechte zur Ausführung administrativer Funktionen gegeben werden. In der Regel beschränken sich diese Verantwortlichkeiten jedoch auf die Vergabe von Zugriffsrechten auf die eigenen Dateien, sofern diese explizit festgelegt und nicht von Voreinstellungen des übergeordneten Verzeichnisses übernommen werden.

12. Schulung

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

Die so entwickelte Sicherheitsstrategie ist zu dokumentieren und im erforderlichen Umfang den Benutzer/innen des Client-Server-Netzes mitzuteilen. Weiters ist sie laufend etwaigen Veränderungen im Einsatzumfeld anzupassen.

SYS 6.11 Einsatz von Modems und ISDN-Adaptern

Relevanz: Umsetzung/Wartung; Anwender/innen;

Für den sicheren Einsatz von Modems sind eine Reihe von Regelungen zu treffen.

So ist etwa festzulegen:

- wer die/der Verantwortliche für den sicheren Betrieb des Modems ist (beispielsweise im Stand-alone Einsatz der IT-Benutzer/innen, in vernetzten Systemen der Administrator),
- wer das Modem benutzen darf,
- in welchen Fällen vertrauliche Informationen bei der Übertragung verschlüsselt werden müssen,
- in welchen Fällen durchgeführte Datenübertragungen zu protokollieren sind (z.B. bei Übermittlung personenbezogener Daten). Bietet die Kommunikationssoftware Protokollierungsfunktion an, sollten diese im sinnvollen Rahmen genutzt werden.

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

Der sichere Einsatz eines Modems bedingt weiters einige administrative Maßnahmen:

- Die Telefonnummer eines Modem-Zugangs darf nur den Kommunikationspartnern bzw. -partnerinnen bekannt gegeben werden, um den Zugang vor Einwählversuchen zu schützen. Sie darf nicht im Telefonverzeichnis der Organisation erscheinen.
- Ist ein Modem in einen Netzserver integriert, können Benutzer/innen von ihren Arbeitsplatzrechnern auf das Modem zugreifen. Dann darf ein Zugriff auf die Kommunikationssoftware nur den Benutzer/innen möglich sein, die für die Datenübertragung berechtigt sind.
- Außerdem müssen regelmäßig die Einstellungen des Modems und der Kommunikationssoftware überprüft werden sowie die durchgeführten Datenübertragungen protokolliert werden.

- Es muss sichergestellt sein, dass das Modem die Telefonverbindung unterbricht, sobald der/die Benutzer/in sich vom System abmeldet. Bei einem Stand-alone-System kann dies dadurch realisiert sein, dass das Modem nur solange mit dem Telefonnetz verbunden ist, wie es für die Datenübertragung eingesetzt wird, und es anschließend ausgeschaltet bzw. von der Leitung getrennt wird. Bei einem im Netzserver integrierten Modem muss dies über die Konfiguration sichergestellt werden. Ein externes Modem kann einfach ausgeschaltet werden. Außerdem müssen alle Benutzer/innen darauf hingewiesen werden, dass nach der Datenübertragung auch das Kommunikationsprogramm zu beenden ist.
- Es muss außerdem darauf geachtet werden, dass nach einem Zusammenbruch der Modem-Verbindung externe Benutzer/innen automatisch vom IT-System ausgeloggt werden. Andernfalls kann der/die nächste Anrufer/in unter dieser Benutzerkennung weiterarbeiten, ohne sich einzuloggen.

Sicherheitsmechanismen bei Modems:

Es gibt vielfältige Sicherheitsmechanismen, die in Modems integriert sein können, wie etwa Passwortmechanismen oder Callback-Funktionen (vgl. dazu SYS 6.12 „Geeignete Modem-Konfiguration“). Einige Modems bieten auch die Möglichkeit, die übertragenen Daten zu verschlüsseln.

Die Anschaffung eines Modems mit Verschlüsselungsoption ist vorteilhaft, wenn regelmäßig Übertragungen großer Datenmengen innerhalb einer Organisation mit verstreuten Liegenschaften durchgeführt werden sollen. Diese Online-Verschlüsselung bedingt einen geringeren organisatorischen Aufwand als das Verschlüsseln der Daten mittels Zusatzprodukten. Es ist darauf zu achten, dass die eingesetzten Algorithmen stets dem Stand der Technik entsprechen.

Die vielfach angebotene Callback-Funktion bietet unter Sicherheitsgesichtspunkten den Vorteil, dass auf einfache Weise unautorisierte Anrufer/innen abgewiesen werden können (siehe auch SYS 6.13 „Aktivierung einer vorhandenen Callback-Option“).

SYS 6.12 Geeignete Modem-Konfiguration

Relevanz: Umsetzung/Wartung;

Für Modems gibt es im Allgemeinen sicherheitsrelevante Parameter, die entsprechend einzustellen sind. Es ist wichtig, den Befehlssatz des eingesetzten Modems daraufhin zu überprüfen, wie die im Folgenden beschriebenen Funktionen umgesetzt sind und ob durch fehlerhafte Konfiguration Sicherheitslücken entstehen können.

Die gewählten Einstellungen sollten im nichtflüchtigen Speicher des Modems gespeichert werden. Außerdem sollten sie auf Papier ausgedruckt werden, so dass sie jederzeit mit der aktuellen Einstellung verglichen werden können.

Nachfolgend werden einige sicherheitsrelevante Konfigurationen vorgestellt:

Auto-Answer:

Es kann eingestellt werden, dass das Modem einen ankommenden Ruf automatisch nach einer einzustellenden Anzahl von Klingelzeichen entgegennimmt. Eine Einstellung, die dies verhindert und erzwingt, dass Anrufe manuell entgegengenommen werden müssen, sollte gewählt werden, wenn verhindert werden soll, dass von außen unbemerkt eine Verbindung aufgebaut werden kann. Ansonsten ist ein Callback-Mechanismus einzusetzen (siehe SYS 6.13 „Aktivierung einer vorhandenen Callback-Option“).

Fernkonfiguration des Modems:

Manche Modems können so eingestellt werden, dass sie von entfernten Modems fernkonfiguriert werden können. Es ist darauf zu achten, dass diese Möglichkeit ausgeschaltet ist.

Zum Problem der Fernwartung über Modems siehe BET 1.3 Fernwartung.

Passwortgeschützte Speicherung von (Rückruf-)Nummern:

Bei der Speicherung von Telefonnummern oder Rückrufnummern im nichtflüchtigen Speicher des Modems können diese bei vielen Modellen durch ein Passwort geschützt werden. Wenn diese Möglichkeit vorhanden ist, sollte sie genutzt und die Passwörter entsprechend den Sicherheitsanforderungen (vgl. dazu auch SYS 1.5 Regelungen des Passwortgebrauches) gewählt werden. Bei einigen Modems wird nach Eingabe eines bestimmten Befehls eine Liste der Rufnummern mit den zugehörigen Passwörtern angezeigt. Daher sollte der Zugang zum Modem nur befugten Personen möglich sein

SYS 6.13 Aktivierung einer vorhandenen Callback-Option

Relevanz: Umsetzung/Wartung;

Viele Modems bieten die Option eines automatischen Rückrufs (Callback). Ist diese Option aktiviert, trennt das Modem, wenn es einen Anruf erhält, sofort nach dem erfolgreichen Verbindungsaufbau die Leitung und ruft eine voreingestellte Nummer zurück. Dadurch wird verhindert, dass ein nicht autorisierter Anrufer diesen Modemzugang missbrauchen kann, solange er nicht unter der voreingestellten Nummer erreichbar ist. Callback ist immer dann einzusetzen, wenn feste Kommunikationspartner/innen sich automatisch einwählen können sollen. Zu beachten ist, dass mit dem automatischen Rückruf auch die Kosten der Datenübertragung übernommen werden.

Anmerkung: Privilegierte Benutzer/innen können ev. die Möglichkeit haben, die Nummer einzugeben, unter der sie sich zurückrufen lassen möchten. Hier sollte darauf geachtet werden, dass nur in der Zentrale festgelegte Nummern zurückgerufen werden, und kein “Overrulen” durch den Anrufer möglich ist.

Es ist darauf zu achten, dass der automatische Rückruf nur auf einer Seite aktiviert ist, da der Mechanismus sonst in eine Endlosschleife führt. Callback sollte auf der passiven Seite aktiviert sein, also auf der Seite, von der Dateien abgerufen oder auf der Dateien eingespielt werden.

Es ist sicherzustellen, dass die voreingestellten Rufnummern des Callback sporadisch kontrolliert und aktualisiert werden.

SYS 6.14 Wireless LAN (WLAN)

Relevanz: Umsetzung/Wartung;

Drahtlose Netzwerke bzw. so genannte Wireless LAN (WLAN) – Lösungen ergänzen zunehmend LAN Netzwerke. Zum einen bieten sie Flexibilität bei der Arbeitsplatzgestaltung und zum anderen sind für deren Aufbau keine aufwendigen Verkabelungsarbeiten notwendig. Die steigende Zahl von portablen Computern (Notebooks, PDAs, etc.) unterstreicht die Forderung nach einem WLAN. Sicherheitstechnisch entstehen neue Gefährdungen und es sind einige Maßnahmen zu beachten, um nicht durch die Einführung von WLANs die Sicherheit des gesamten lokalen Netzwerkes zu kompromittieren.

Folgende Maßnahmen sind zu beachten, wenn es um die Installation und Konfiguration eines WLANs geht:

- *Geeignete Positionierung und Ausrichtung der Zugriffspunkte und Antennen:*
  Die Ausstrahlung soll über die Organisationsgrenzen hinweg weitgehend verhindert werden. Der Einsatz von Richtantennen hilft dabei die unbeabsichtigte räumliche Ausstrahlung zu unterbinden.
- *Testen des Umkreises:*
  Der mögliche Empfang im Umkreis der Organisation muss überprüft werden. Bei unerwünschten Reichweiten müssen entsprechende Gegenmaßnahmen ergriffen werden.
- *Deaktivieren des Sendens der Service Set ID:*
  Die Service Set ID (SSID) ist ein Name des WLANs, über den Knoten an das Netz verbinden. Dessen Bekanntgabe an Knoten, die diese eindeutige SSID nicht kennen, ist zu verhindern. Somit soll die Option des Sendens der SSID deaktiviert werden.
- *Verschlüsselungsoptionen aktivieren:*
  Verschlüsselungsoptionen, etwa Wired Equivalent Privacy (WEP), WEP+ oder WiFi Protected Access (WPA), bieten Schutz vor Zugriffen durch Dritte. Es gibt im Allgemeinen die Wahl zwischen unterschiedlichen Schlüssellängen (bei WEP beispielsweise 40 Bit oder 128 Bit). Es ist dabei sinnvoll den Schlüssel mit der größten Länge zu wählen, sofern die verwendeten Endgeräte dies zulassen. Die verwendbaren Schlüssellängen sollten demnach bei der Anschaffung der WLAN-Komponenten bereits berücksichtigt werden. Bietet das System darüber hinaus die Möglichkeit mehrere verschiedene Schlüssel zu verwenden, oder die Möglichkeit eines periodischen Schlüsselwechsels, so sollte dies genutzt werden. Zu beachten ist, dass WEP alleine keinen ausreichenden Schutz vor ambitionierten Angreiferinnen bzw. Angreifern bietet. Zudem sind von WEP zahlreiche Schwächen bekannt. Es empfiehlt sich daher, auf verbesserte Sicherheitsmechanismen wie WPA bzw. künftig 802.11i wenn möglich zurück zu greifen. Darüber hinaus sind zusätzliche Maßnahmen sinnvoll (z.B. VPN - siehe weiter unten).
- *Authentifikation der Knoten:*
  Möglichkeiten der Authentifikation der Knoten sind zu aktivieren, etwa nach IEEE 802.1X.
- *Einsatz einer zusätzlichen Firewall:*
  Eine Firewall zwischen dem Zugriffspunkt und dem eigentlichen Netzwerk kann die Sicherheit erhöhen.
- *Direkten Zugriff auf das Intranet über das WLAN sperren:*
  Ist der Zugang über WLAN nicht durch starke Methoden der Authentifikation der Knoten und Verschlüsselung gesichert, ist er als RAS anzusehen (vgl. Kapitel 5.7).

- *Ändern von Standardeinstellungen (Passwörtern):*
  Standardeinstellungen der Zugriffspunkte – etwa Service Set ID (SSID), SNMP Community String, Administrator-Passwort – sind werksseitig voreingestellt und müssen sofort geändert werden, da die Standardpasswörter Angreiferinnen bzw. Angreifern durchaus bekannt sind (vgl. SYS 1.5 „Regelungen des Passwortgebrauches“).
- *MAC-Adressfilterung am Zugriffspunkt:*
  Der Zugang zu Zugriffspunkten kann bei vielen Geräten auch über die MAC-Adresse kontrolliert werden. Dies sollte nach Möglichkeit genutzt werden.
- *Nutzung eines Virtual Private Networks (VPN):*
  Im WLAN sollte möglichst ein VPN etabliert werden, wodurch die vertraulichen Inhalte mittels IPSEC oder SSL/TLS geschützt werden. Dies bietet über WEP/WEP+/WPA/o.ä. hinausgehend eine Ende-zu-Ende Verschlüsselung.
- Für den Bereich der Öffentlichen Verwaltung sind entsprechende Vorgaben und WLAN-Policies der Stabsstelle IKT-Strategie des Bundes (CIO) zu beachten (z.B.: [IKT-WLAN] [IKT-CLWLAN]).

Weiterführende Informationen, speziell aber nicht nur für die Organisationen der öffentlichen Verwaltung, sind den von der Stabsstelle IKT-Strategie des Bundes (CIO) herausgegebenen Empfehlungen zur Verwendung von WLANs zu entnehmen [IKT-WLAN]. In Ergänzung zu diesen allgemeine Informationen zu WLANs in der Verwaltung wurde von der Stabsstelle IKT-Strategie des Bundes (CIO) die so genannte „Checkliste WLAN“ [IKT-CLWLAN] veröffentlicht. Diese Erweiterung berücksichtigt aktuelle Weiterentwicklungen und Marktveränderungen im Bereich WLAN. Die darin enthaltene Checkliste ermöglicht ein einfaches und pragmatisches Anwenden der Empfehlungen.

5.7 Remote Access

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

Durch Remote Access wird es einem/einer Benutzer/in ermöglicht, sich mit einem lokalen Rechner an ein entferntes Rechnernetz zu verbinden und dessen Ressourcen zu nutzen, als ob eine direkte LAN-Koppelung bestehen würde. Die dafür benutzten Dienste werden Remote Access Service (RAS) genannt.

Generell lassen sich für den Einsatz von RAS im Wesentlichen folgende Szenarien unterscheiden:

- das Anbinden einzelner stationärer Arbeitsplatzrechner (z.B. für Telearbeit einzelner Mitarbeiter/innen),
- das Anbinden mobiler Rechner (z.B. zur Unterstützung von Mitarbeiterinnen/Mitarbeitern im Außendienst oder auf Dienstreise),
- das Anbinden von ganzen LANs (z.B. zur Anbindung von lokalen Netzen von Außenstellen oder Filialen),
- der Managementzugriff auf entfernte Rechner (z.B. zur Fernwartung).

Für diese Szenarien bietet RAS eine einfache Lösung: entfernte Benutzer/innen verbinden sich z.B. über das Telefonnetz mit Hilfe eines Modems mit dem Firmennetz. Diese Direktverbindung kann solange wie nötig bestehen bleiben und als Standleitung angesehen werden, die nur bei Bedarf geschaltet wird.

Unter dem Gesichtspunkt der Sicherheit sind für RAS-Zugänge folgende Sicherheitsziele zu unterscheiden:

1. Zugangssicherheit:

Entfernte Benutzer/innen müssen durch das RAS-System eindeutig zu identifizieren sein. Ihre Identität muss jeweils durch einen Authentisierungsmechanismus bei jedem Verbindungsaufbau zum lokalen Netz sichergestellt werden. Im Rahmen des Systemzugangs müssen weitere Kontrollmechanismen angewandt werden, um den Systemzugang für entfernte Benutzer/innen reglementieren zu können (z.B. zeitliche Beschränkungen oder Einschränkung auf erlaubte entfernte Verbindungspunkte).

2. Zugriffskontrolle:

Sind die entfernten Benutzer/innen authentisiert, so muss das System in der Lage sein, ihre Remote-Zugriffe auch zu kontrollieren. Dazu müssen die Berechtigungen und Einschränkungen, die für lokale Netzressourcen durch befugte Administratoren festgelegt wurden, auch für entfernte Benutzer/innen durchgesetzt werden.

3. Kommunikationssicherheit:

Bei einem Remote-Zugriff auf lokale Ressourcen sollen im Allgemeinen auch über die aufgebaute RAS-Verbindung Nutzdaten übertragen werden. Generell sollen auch für Daten, die über RAS-Verbindungen übertragen werden, die im lokalen Netz geltenden Sicherheitsanforderungen bezüglich Kommunikationsabsicherung (Vertraulichkeit, Integrität, Authentizität) durchsetzbar sein. Der Absicherung der RAS-Kommunikation kommt jedoch eine besondere Bedeutung zu, da zur Abwicklung der Kommunikation verschiedene Kommunikationsmedien in Frage kommen, die in der Regel nicht dem Hoheitsbereich des Betreibers des lokalen Netzes zuzurechnen sind.

4. Verfügbarkeit:

Wird der RAS-Zugang im produktiven Betrieb genutzt, so ist die Verfügbarkeit des RAS-Zugangs von besonderer Bedeutung. Der reibungslose Ablauf von Geschäftsprozessen kann bei Totalausfall des RAS-Zugangs oder bei Verbindungen mit nicht ausreichender Bandbreite unter Umständen beeinträchtigt werden. Durch die Nutzung von alternativen oder redundanten RAS-Zugängen kann diese Gefahr bis zu einem gewissen Grad verringert werden. Dies gilt insbesondere für RAS-Zugänge, die das Internet als Kommunikationsmedium nutzen, da hier in der Regel keine Verbindungs- oder Bandbreitengarantien gegeben werden.

Ein RAS-System besteht aus mehreren Komponenten, die zunächst als Einzelkomponenten abgesichert werden sollten. Zusätzlich zu der Absicherung der RAS-Systemkomponenten muss jedoch auch ein RAS-Sicherheitskonzept erstellt werden, das sich in das bestehende Sicherheitskonzept eingliedert: das RAS-System muss einerseits bestehende Sicherheitsforderungen umsetzen und erfordert andererseits das Aufstellen neuer, RAS-spezifischer Sicherheitsregeln.

SYS 7.1 Durchführung einer RAS-Anforderungsanalyse

Relevanz: Umsetzung/Wartung;

Ziel der Anforderungsanalyse ist es einerseits, alle im konkreten Fall in Frage kommenden Einsatzszenarien zu bestimmen und andererseits daraus Anforderungen an die benötigten Hard- und Softwarekomponenten abzuleiten.

Im Rahmen der Anforderungsanalyse sind u.a. folgende Fragen zu klären:

- Welche Benutzer/innen werden den RAS-Zugang nutzen (Telearbeiter/innen, Außendienstmitarbeiter/innen, Mitarbeiter/innen auf Dienstreise)?
- Soll der RAS-Zugang von mobilen Benutzern/Benutzerinnen genutzt werden?
- Zu welchem Zweck wird der RAS-Zugang jeweils genutzt (Abfragen von Informationen, Einstellen von Informationen, Programmnutzung)?
- Müssen die entfernten Benutzer/innen auf das komplette LAN, d. h. alle dort verfügbaren Daten und Dienste) Zugriff haben?
- Müssen spezielle Softwareprodukte über den RAS-Zugang genutzt werden?
- Müssen spezielle Protokolle über den RAS-Zugang genutzt werden?
- Von welchen (entfernten) Orten wird der RAS-Zugang genutzt (national, international)?
- Welche Telekommunikations-Zugangstechnologien kommen zum Einsatz (Festnetz, Mobiltelefon, Internet)?

Die Anforderungen für die geplanten Szenarien sind zu dokumentieren und mit den Netzadministratoren und dem technischen Personal abzustimmen.

SYS 7.2 Entwicklung eines RAS-Konzeptes

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

Ein RAS-Konzept kann grob in drei Teilbereiche unterteilt werden:

- Organisatorisches Konzept
- Technisches Konzept
- Sicherheitskonzept

Im Folgenden werden jeweils die wesentlichen Fragestellungen aufgezeigt, die im Rahmen der Teilkonzepte beantwortet werden müssen. Je nach konkreter Situation ergibt sich naturgemäß ein speziell auf die jeweiligen organisatorischen und technischen Gegebenheiten zugeschnittener zusätzlicher Abstimmungsbedarf.

Das *organisatorische Konzept* sollte folgende Punkte beinhalten bzw. regeln:

- Festlegung der Verantwortlichkeiten für das RAS-System (Installation, Verwaltung, Überprüfung, Überwachung).
- Festlegung verbindlicher Zugangs- und Zugriffsregelungen und deren Dokumentation
- Anforderungen an Betriebsorte

- Festlegung von Anforderungen an feste Remote-Arbeitsplätze (z.B. Telearbeitsplätze) in Bezug auf Sicherheit, technische Ausstattung und Ergonomie. Das Konzept kann gegebenenfalls eine anfängliche sowie eine periodisch wiederkehrende Überprüfung der Räumlichkeiten vorsehen und regeln, wie und durch wen diese erfolgt.
- Regelungen, von welchen Remote-Standorten aus RAS-Verbindungen zum Ziel-LAN aufgebaut werden dürfen. Abhängig vom geplanten Einsatzszenario kann es auch zweckmäßiger sein, eine Negativliste von besonders ungeeigneten Standorten zu führen. Dazu können z.B. Hotel-Foyers, Hotel-Business-Center oder Zug-Abteile gehören.
- Änderungsmanagement: Für die RAS-Administration sollten Prozeduren festgelegt werden, wie Änderungen an der RAS-Konfiguration durchzuführen sind.

Das *technische Konzept* sollte folgende Punkte beinhalten bzw. regeln:

- Beschreibung der Funktionalität der Hard- und Software-Komponenten des RAS-Systems technisch realisiert ist,
- Beschreibung aller möglichen Zugangspunkte und der darüber verwendeten Zugangsprotokolle,
- Beschreibung aller Dienste und Protokolle, die über den RAS-Zugang zugelassen werden, sowie die darüber zugreifbaren Ressourcen
- Festlegung, welche Teilnetze über den RAS-Zugang erreichbar sein sollen bzw. müssen (vgl. auch RAS-Sicherheitskonzept).

Das *RAS-Sicherheitskonzept* sollte folgende Punkte beinhalten bzw. regeln:

- Erstellung einer Sicherheitspolitik für die RAS-Nutzung: Diese RAS-Sicherheitspolitik muss sich an den existierenden übergreifenden IT-Sicherheitspolitik orientieren. In der Regel gilt der Grundsatz, dass beim Zugriff über das RAS-System geringere Berechtigungen gelten und stärkere Überprüfungen stattfinden sollten, als beim lokalen Zugriff.
- Festlegung der Benutzer-Authentisierung sowie der dafür zu verwendenden Mechanismen
- Erfassung aller an der Authentisierung beteiligten Komponenten und Beschreibung ihrer Aufgaben und Interaktionen
- Erfassung aller an der Zugriffskontrolle beteiligten Komponenten und ihrer Aufgaben und Interaktionen. Auf diese Weise kann festgestellt werden, ob z.B. existierende Zugriffskontrollmechanismen so konfiguriert werden können, dass beim entfernten Zugriff automatisch restriktivere Einstellungen gelten.
- Erfassung aller RAS-Zugangspunkte zum lokalen Netz und Beschreibung, wie diese Zugangspunkte an das LAN angeschlossen werden
- Das Sicherheitskonzept muss analysieren, aufbauend auf der aktuellen Netzstruktur, welche Teilnetze bei Nutzung eines RAS-Zugangs erreichbar sind. Für Bus-basierte Netze (beispielsweise Ethernet) sind typischerweise alle Rechner des Teilnetzes zugreifbar, in dem der RAS-Zugang angesiedelt ist. Hier sollte überlegt werden, dedizierte Zugangsnetze (Access Network) zu bilden, aus denen nur kontrolliert (über Router, Paketfilter bzw. interne Firewall) in das produktive Netz zugegriffen werden kann. Die Bildung von Zugangsnetzen erfordert dabei die Anschaffung und Wartung zusätzlicher Hard- und Software
- Festlegung der Verfügbarkeitsanforderungen an das RAS-System und Planung etwaiger Ausweichlösungen

- Aufnahme der Handlungsanweisungen und Meldewege im Problemfall in die Incident Handling Pläne der Organisation (vgl. PER 3.5 Aktionen bei Auftreten von Sicherheitsproblemen (Incident Handling Pläne) und BET 4.1 Erstellung eines Incident Handling Plans). Im technischen Konzept sollten entsprechend Mechanismen geplant werden, die das Erkennen von Sicherheitsvorfällen erlauben und diese Vorfälle zu dem zuständigen Administrator leiten, der den Anfang des organisatorischen Meldewegs bildet.
- Schulungs- und Awarenessprogramme für Anwender/innen und Administratoren
- Den Administratoren muss nicht nur für den Betrieb der RAS-Systeme ausreichend Zeit zur Verfügung stehen, sondern auch für die Informationssuche über aktuelle Sicherheitslücken und die Einarbeitung in neue Komponenten.

SYS 7.3 Auswahl einer geeigneten RAS-Systemarchitektur

Relevanz: Umsetzung/Wartung;

Je nach den geplanten Einsatzszenarien können unterschiedliche RAS-Systemarchitekturen genutzt werden, um den Remote-Zugang zu einem LAN zu realisieren. Die folgenden RAS-Szenarien, denen jeweils eine typische Systemarchitektur zugeordnet werden kann, kommen in der Praxis häufig zum Einsatz.

1. Anbindung einzelner Rechner an ein LAN (z.B. “Direct Dial-In”)

Vorteil: Durch dieses Verfahren kann ein einzelner Rechner von einem beliebigen Ort aus an das LAN angeschlossen werden. Dies ist insbesondere für mobile Benutzer/innen günstig. Der Einsatz von Mechanismen zur Kommunikationsabsicherung ist auch hier zu empfehlen, also z.B. Verschlüsselung, digitale Signaturen, Authentisierung.

Nachteil: Je nach Entfernung zum Ziel-LAN können unterschiedlich hohe Telefonkosten entstehen, die (ohne besondere Vorkehrungen) in der Regel bei Remote-Benutzer/innen anfallen. Für die Anbindung mehrerer Benutzer/innen, die sich gemeinsam an einem entfernten Ort befinden, ist diese Variante nicht geeignet, da jeweils eine dedizierte Verbindung zwischen Client und Server aufgebaut wird.

2. Anbindung mehrerer Rechner an ein LAN (z.B. “Direct LAN-to-LAN-Dial-In”)

Vorteil: Durch die Funktionstrennung von RAS-Client und Rechner der entfernten Benutzer/innen können über *eine* Verbindung zum Ziel-LAN *mehrere* entfernte IT-Systeme angebunden werden. Der Router, der den RAS-Client enthält, stellt dabei die aufgebaute Verbindung für alle am entfernten LAN angeschlossenen Rechner zur gleichzeitigen Nutzung bereit. Dies ist jedoch zugleich auch nachteilig, da die Verbindungskapazität unter den zugreifenden entfernten IT-Systemen aufgeteilt wird und nicht exklusiv genutzt werden kann.

Nachteil: die Clients sind nicht mehr mobil.

3. Anbindung eines Rechners oder eines LANs über einen Service Provider

Als Erweiterung der beiden vorangegangenen Szenarien kann die Anbindung eines Rechners oder eines LANs auch über eine spezielle Zugangsrufnummer eines Service Providers erfolgen. In diesem Fall kontaktiert der RAS-Client eine besondere Telefonnummer, die häufig eine Ortsgespräch-Rufnummer oder eine kostenfreie Rufnummer ist. Anrufe für diese spezielle Nummer werden vom anbietenden Service Provider innerhalb des Kommunikationsnetzes an den RAS-Server des Ziel-LANs weitergeleitet. Diese Variante erlaubt insbesondere Mitarbeiterinnen/ Mitarbeitern auf Dienstreise eine für sie kostengünstige Verbindungsaufnahme.

4. Anbindung eines Rechners oder eines LANs über Internet

Dieser Fall unterscheidet sich von den obigen Szenarien dadurch, dass vom Client zunächst eine Verbindung zu einem Internet-Dienstanbieter (Internet Service Provider - ISP) aufgebaut wird. Erst im zweiten Schritt verbindet sich der Client über die bestehende Internet-Anbindung mit dem Ziel-LAN.

5. Aufbau eines Virtuellen Privaten Netzes (VPN)

Neben der Möglichkeit, mit Hilfe von Internet-basierten Protokollen und Programmen (z.B. telnet, ftp, POP3) auf Daten des internen Netzes zuzugreifen, können auch so genannte Tunnel-Protokolle benutzt werden. Diese erlauben es, über das Internet als Transportmedium eine Direktverbindung zwischen dem RAS-Client und dem RAS-Server des Ziel-LANs zu *simulieren*. Über diese scheinbare Direktverbindung erfolgt die eigentliche RAS-Kommunikation. Der RAS-Server des Ziel-LANs muss hierzu über das Internet erreichbar sein.

Vorteil: da Internetzugänge mittlerweile weit verbreitet sind, kann hier in einfacher Weise auf einem existierenden Verbindungsnetz aufgebaut werden.

Nachteil: das Internet wurde aufgrund seiner offenen Struktur nicht als sicheres Netz konzipiert. Aus diesem Grund ist hier die Absicherung der Kommunikation besonders wichtig. Beim Tunneling geschieht dies durch den Einsatz kryptographischer Verfahren. Hierdurch wird ein so genanntes Virtuelles Privates Netz (VPN) realisiert.

SYS 7.4 Sichere Installation des RAS-Systems

Relevanz: Umsetzung/Wartung;

Voraussetzung für eine sichere Installation ist die Auswahl geeigneter Hard- und Software für den RAS-Zugang (Qualität, Interoperabilität, Konformität zu bestehenden Standards) durch den vorangegangenen Entscheidungsprozess (vgl. voranstehende Maßnahmen).

Zusätzlich zu den generellen Sicherheitsmaßnahmen, die für die IT-Komponenten zu beachten sind, sollten im Rahmen der Installation eines RAS-Systems folgende zusätzliche Punkte Beachtung finden:

- Es sollte vorgesorgt werden, dass RAS-Zugänge nur über vom Dienstgeber zur Verfügung gestellte - sichere - Geräte möglich sind (mittels Workstation-Zertifikat o.ä.), um zu verhindern, dass Bedienstete mit ihrem RAS-Account von privaten (unkontrollierten und somit extrem unsicheren) PCs auf das interne Netz zugreifen.
- Weder das RAS-System noch Teile davon sollten während der Installationsphase für Benutzer/innen oder fremde Dritte zugreifbar sein. Es sollten also keine Verbindungen zum produktiven LAN und kein Anschluss an TK-Systeme aktiv sein.
- Die Installation ist durch qualifiziertes Personal durchzuführen.
- Die Installation sollte gemäß der RAS-Systemplanung erfolgen.
- Die Installation und Konfiguration ist zu dokumentieren. Dies kann entweder durch eine separate Installationsdokumentation erfolgen, oder aber durch eine Bestätigung, dass die Installation mit den Planungsvorgaben übereinstimmt.
- Ergibt sich im Rahmen der Installation eine Abweichung von den Planungsvorgaben (z.B. geänderte Leitungsführung, zusätzliche Geräte), so sind diese zu dokumentieren und ein begründeter Änderungsvermerk in die Planungsunterlagen zu übernehmen. Diese Dokumentation ist auch im Hinblick auf die Verbesserung zukünftiger Planungen besonders wichtig.
- Das korrekte Funktionieren jeder einzelnen Komponente muss festgestellt werden (z.B. durch Funktionsprüfung bzw. Selbsttest).
- Für jede sicherheitsrelevante Einstellung muss ein Funktionstest der Sicherheitsmechanismen durchgeführt werden. Beispielsweise sollte die Kommunikationsverschlüsselung mittels eines Netzanalysators überprüft werden.
- Das korrekte Funktionieren des Gesamtsystems ist nach Abschluss der Installationsarbeiten zu überprüfen (Abnahme und Freigabe der Installation). In der Regel muss dies durch vorgegebene Abnahmekonfigurationen und nachgestellte Nutzungsszenarien erfolgen. Bei den Tests ist darauf zu achten, dass nur die zum Test befugten Personen Zugriff zum RAS-System erhalten.
- Wenn eine RAS-Verbindung besteht, darf von der RAS-Workstation keine zweite Netzwerkverbindung in ein anderes Netz bestehen (Gefahr des Durchschleifens von Sicherheitsproblemen).

Die Installation eines RAS-Systems sollte mit einer sicheren Anfangskonfiguration abgeschlossen werden, die zunächst nur den berechtigten Administratoren Zugriffe erlaubt (siehe auch SYS 7.5 Sichere Konfiguration des RAS-Systems). Diese überführen das RAS-System dann in einen sicheren Betriebszustand. Ist dieser erreicht, kann der laufende Betrieb aufgenommen werden.

SYS 7.5 Sichere Konfiguration des RAS-Systems

Relevanz: Umsetzung/Wartung;

Die Funktion und die Sicherheit eines RAS-Systems wird wesentlich durch die eingestellten Konfigurationsparameter bestimmt. Da jedoch ein RAS-System nicht aus nur einer Komponente und deren Konfiguration besteht, ergibt sich naturgemäß eine erhöhte Komplexität für die Gesamtkonfiguration. Aufgrund dieser Komplexität können leicht Konfigurationsfehler entstehen, die die Sicherheit des Gesamtsystems verringern können. Das nicht abgestimmte Ändern eines Konfigurationsparameters bei einer Komponente kann daher im Zusammenspiel mit den anderen Komponenten zu Fehlfunktionen führen. Im Extremfall kann dadurch auch die Sicherheit des LANs beeinträchtigt werden.

Da die Konfiguration eines RAS-Systems in der Regel Veränderungen unterworfen ist (z.B. durch Personaländerungen, neue Nutzungsszenarien, Systemerweiterungen), kann nicht davon ausgegangen werden, dass es genau eine sichere (und statische) Konfiguration gibt, die einmal eingestellt und nie wieder verändert wird. Vielmehr unterliegt die Konfiguration fortschreitenden Versionsänderungen. Es ist Aufgabe der für das RAS-System zuständigen Administratoren, dass jeweils nur sichere Versionen der Systemkonfiguration definiert werden und das System von einer sicheren Konfiguration in die nachfolgende sichere Konfiguration überführt wird.

Generell kann zwischen den folgenden Konfigurationskategorien unterschieden werden:

- Die *Default-Konfiguration* ergibt sich durch die vom Hersteller voreingestellten Werte für die Konfigurationsparameter. Diese ist in der Regel nicht ausreichend sicher und sollte daher nicht verwendet werden.
- Nach der Installation und vor der Inbetriebnahme muss - ausgehend von der Default-Konfiguration - eine sichere *Anfangskonfiguration* durch die Administratoren eingestellt werden. Hier sollten möglichst restriktive Einstellungen gelten, so dass nur die berechtigten Administratoren Veränderungen vornehmen können, um z.B. eine erste Betriebskonfiguration einzustellen, die das geplante Sicherheitskonzept umsetzt.
- Die sicheren *Betriebskonfigurationen* ergeben sich aus den jeweiligen Konfigurationen im laufenden Betrieb. Hier muss auch regelmäßig überprüft werden, ob neu bekannt gewordene Sicherheitslücken Anpassungen erfordern (siehe auch M 2.35 „Informationsbeschaffung über Sicherheitslücken des Systems“).
- Schließlich sollten sichere *Notfallkonfigurationen* im Rahmen der Notfallplanung definiert und dokumentiert werden. Sie dienen dazu, auch bei eingeschränkter Betriebsfähigkeit die Sicherheit aufrechtzuerhalten. In der Regel werden durch die Notfallplanung mehrere Notfallsituationen definiert. Es empfiehlt sich, für jede der definierten Situationen eine adäquate Notfallkonfiguration festzulegen. Im einfachsten Fall besteht die Notfallkonfiguration darin, den Zugang zum RAS-System zu sperren.

SYS 7.6 Sicherer Betrieb des RAS-Systems

Relevanz: Umsetzung/Wartung; Anwender/innen;

Voraussetzung für den sicheren Betrieb eines RAS-Systems ist die sichere Installation und Konfiguration der beteiligten Hard- und Software-Komponenten (vgl. SYS 7.4 Sichere Installation des RAS-Systems und SYS 7.5 Sichere Konfiguration des RAS-Systems. Zusätzlich müssen alle organisatorischen Abläufe definiert und umgesetzt worden sein (z.B. Meldewege und Zuständigkeiten). Weiterhin ist zu beachten, dass die angestrebte Systemsicherheit nur gewährleistet werden kann, wenn auch die physikalische Sicherheit der beteiligten Hardware-Komponenten sichergestellt ist.

Die Sicherheit eines RAS-Systems lässt sich grob in drei Bereiche aufteilen:

- die Sicherheit des RAS-Servers,
- die Sicherheit der RAS-Clients und
- die Sicherheit der Datenübertragung.

Im Umfeld des *RAS-Servers* sind folgende Empfehlungen für den sicheren Betrieb zu berücksichtigen:

- Der RAS-Zugang sollte durch den Einsatz von Protokollierungs- und Management-Werkzeugen einer ständigen Überwachung unterliegen.
- Die im Rahmen der Überwachung gesammelten Informationen sollten regelmäßig durch geschulte Administratoren kontrolliert werden. Sie sollten dabei nach Möglichkeit durch eine Software zur Auswertung von Protokollierungsdaten unterstützt werden. Die Bestimmungen des Datenschutzes sind zu beachten.
- Werden Sicherheitsvorfälle festgestellt, so sind sofort die vorher festgelegten Maßnahmen zu ergreifen.
- Damit eine geregelte Benutzer-Authentisierung beim RAS-Zugriff möglich ist, muss die Konsistenz der Authentisierungsdaten sichergestellt sein. Dies kann durch zentrale Verwaltung der Daten (Authentisierungsserver) oder durch periodischen Abgleich geschehen.
- Für jede Verbindungsaufnahme ist immer die Benutzer-Authentisierung über den gewählten Mechanismus durchzuführen.
- Für jede Verbindung sollte die Absicherung der Kommunikation durch eines der im RAS-Sicherheitskonzept erlaubten Verfahren erzwungen werden, damit die übertragenen Daten geschützt sind.
- Die durch die Zugangstechnik zur Verfügung gestellten *zusätzlichen* Sicherheitsmechanismen (Nutzung der Rufnummernübertragung, Rückruf einer voreingestellten Telefonnummer für nicht mobile oder über Mobiltelefon angebundene RAS-Clients) sollten genutzt werden.
- Revision: Das RAS-System sollte in regelmäßigen Abständen einer Revision unterzogen werden. Die Rollen Administrator und Revisor dürfen nicht der gleichen Person zugeordnet werden.

Da RAS-Clients in der Regel in nicht vollständig kontrollierten Umgebungen betrieben werden, müssen für diesen Fall spezielle Mechanismen, Verfahren und Maßnahmen zum Einsatz kommen, die den Schutz des Clients gewährleisten können. Insbesondere mobile RAS-Clients sind hier einer besonderen Gefahr ausgesetzt, da diese physikalisch besonders leicht anzugreifen sind (Diebstahl, Vandalismus). Ist ein RAS-Client kompromittiert, so besteht die Gefahr, dass dadurch auch die Sicherheit des LANs beeinträchtigt wird.

Für den sicheren Betrieb von *RAS-Clients* sind daher folgende Aspekte zu berücksichtigen:

- Die Grundsicherheit des IT-Systems muss gewährleistet sein.
- Da mobile RAS-Clients größeren Risiken ausgesetzt sind als stationäre, sollten sie durch zusätzliche Maßnahmen gesichert werden. Hierzu bietet sich eine Festplattenverschlüsselung an, um sicherzustellen, dass von abhanden gekommenen Geräten weder Daten ausgelesen noch unbefugt eine RAS-Verbindung aufgebaut werden kann.
- Insbesondere beim RAS-Zugriff über Internetverbindungen ist die Installation von Viren-Schutzprogrammen auf allen RAS-Clients notwendig.

- Es sollte überlegt werden, auf den RAS-Clients so genannte PC-Firewalls einzusetzen und so vor unberechtigten Zugriffen aus dem Internet durch Dritte zu schützen. Ähnlich wie herkömmliche Firewalls (siehe Kapitel Gesicherte Anbindung an Fremdnetze (Internet-Sicherheit)) filtern PC-Firewalls die Pakete der Netzkommunikationsprotokolle. Die Filterregeln können jedoch meist dynamisch durch den/die Benutzer/in erzeugt werden. Hierzu wird bei jedem Zugriff, für den noch keine Regel vorliegt, eine Auswahl an möglichen Reaktionen (z.B. erlauben, ablehnen, bedingte Verarbeitung) angeboten, um eine neue Regel zu definieren. Da es für den/die Benutzer/in jedoch in vielen Fällen schwierig ist, zwischen erlaubten und unberechtigten Zugriffen zu unterscheiden, sollte der Regelsatz durch einen Administrator vorinstalliert werden.
- Auch RAS-Clients sollten in das Systemmanagement einbezogen werden, soweit dies möglich ist. Dies erlaubt einerseits die Überwachung der Clients im Rahmen der Aufrechterhaltung des laufenden Betriebes. Andererseits können so einfach Software-Updates (Viren-Datenbanken, Anwendungsprogramme) auf geregeltem Weg eingespielt werden. Entfernte Rechner stellen jedoch erhöhte Anforderungen an das Systemmanagement, da diese nicht permanent mit dem Netz verbunden sind, so dass die Rechner regelmäßig auf (unzulässige) Konfigurationsveränderungen untersucht werden müssen.
- Falls TCP/IP als Protokoll verwendet wird, sollte überlegt werden, für RAS-Clients feste IP-Adressen zu benutzen und diese nicht dynamisch zu vergeben. Dieses Vorgehen bedeutet zwar einen höheren administrativen Aufwand (Wartung der Zuordnungstabellen), erlaubt jedoch eine eindeutige Zuordnung von Netzadresse und Rechner. Der Nachteil bei einer dynamischen Vergabe der Netzadressen besteht darin, dass protokolliert werden muss, welchem RAS-Client zu welchem Zeitpunkt eine bestimmte Netzadresse zugewiesen wurde. Anderenfalls ist es meist nicht möglich festzustellen, welcher RAS-Client eine bestimmte Aktion ausgeführt hat.

Die *Kommunikationsverbindung* zwischen RAS-Client und RAS-Server wird in der Regel über Netze von Dritten aufgebaut. Die dabei benutzten Netzkomponenten unterliegen meist nicht der Kontrolle durch den Betreiber des LANs, mit dem die Verbindung aufgebaut werden soll. Es muss weiter davon ausgegangen werden, dass die Daten nicht nur über das Telekommunikationsnetz eines Anbieters übertragen werden, sondern dass auch die Netze von Kooperationspartnern des Telekommunikationsanbieters benutzt werden. Dies gilt insbesondere beim Zugriff auf ein LAN aus dem Ausland. Um dem Schutzbedarf der so übertragenen Daten gerecht zu werden, müssen Sicherheitsmaßnahmen getroffen werden, die z.B. die Vertraulichkeit der Daten sicherstellen. Daher gilt für die Datenübertragung:

- Die Nutzung der Datenverschlüsselung für alle übertragenen Daten ist für den sicheren Betrieb zwingend erforderlich.
- Es sollten Signaturmechanismen eingesetzt werden, um die Authentizität und Integrität der Daten sicherzustellen.

Um diesen Anforderungen an den Schutz der Daten gerecht zu werden, können verschiedene Sicherungsmechanismen für RAS-Verbindungen benutzt werden. Relevant sind hier unter anderem:

- *Tunneling:*
  Die Kommunikation kann auf niedriger Protokollebene verschlüsselt werden (so genanntes Tunneling, siehe auch SYS 7.8 Einsatz geeigneter Tunnel-Protokolle für die RAS-Kommunikation). Dazu muss ein geeignetes Verfahren ausgewählt werden. Die herkömmlichen RAS-Systeme stellen solche Verfahren standardmäßig, jedoch in unterschiedlicher Zahl und Ausprägung zur Verfügung.

- *SSL-Verschlüsselung:*
  Zur Verschlüsselung kann auch SSL eingesetzt werden, wenn von der Verschlüsselung auf niedriger Protokollebene aus bestimmten Gründen kein Gebrauch gemacht werden kann. Dies gilt besonders für Zugriffe auf WWW-Server oder E-Mail-Server über WWW-Browser, die standardmäßig SSL-gesicherte Kommunikation unterstützen.
- *Verschlüsselung durch Netzkoppelelemente*
  Neben der Absicherung der Kommunikation durch Software kann auch der Einsatz von verschlüsselnden Netzkoppelelementen (Router, Modems) erwogen werden. Diese sind besonders für den stationären Einsatz und zur Anbindung mehrerer Rechner sinnvoll, da die Verschlüsselung transparent erfolgt und die Clients und Server nicht belastet werden. Zu beachten ist jedoch, dass die Geräte sorgfältig konfiguriert und gewartet werden müssen.
- *E-Mail-Verschlüsselung:*
  Für den Austausch von E-Mails über unsichere Kanäle kann die Nutzung von E-Mail-Verschlüsselung sinnvoll sein

SYS 7.7 Nutzung eines Authentisierungsservers beim RAS-Einsatz

Relevanz: Umsetzung/Wartung;

Für RAS-Systeme mit vielen Benutzern bzw. Benutzerinnen muss darüber nachgedacht werden, wie die Benutzerverwaltung für den RAS-Zugang effizient durchgeführt werden kann. Für mittlere und große Netze, die organisatorisch meist in mehrere Teilnetze (Domänen, Verwaltungsbereiche) aufgeteilt sind, besteht in vielen Fällen das Problem, dass in jedem Verwaltungsbereich eine getrennte Verwaltung der Benutzerdaten durchgeführt wird. Sollen sich Benutzer/innen auch an fremden Teilnetzen anmelden können, müssen hier Querberechtigungen (Cross-Zertifikate, Vertrauensstellungen) oder ein zentraler Verzeichnisdienst eingerichtet und gepflegt werden.

Insbesondere im RAS-Kontext haben sich hier spezielle Authentisierungssysteme herausgebildet, die auch für den “normalen” Authentisierungsprozess bei der Systemanmeldung genutzt werden können.

Prinzipiell besitzen diese Systeme folgenden Aufbau:

- Die Authentisierungsdaten der Benutzer/innen werden durch einen zentralen Server verwaltet.
- Das Programm zur Systemanmeldung wendet sich zur Überprüfung der von dem/der Benutzer/in eingegebenen Authentisierungsdaten an den Authentisierungsserver.
- Zur Kommunikation zwischen Anmeldeprozess und Authentisierungsserver wird in der Regel ein abgesichertes Protokoll eingesetzt.

Der Anmeldeprozess muss dazu die Nutzung externer Authentisierungsserver unterstützen und die Netzadresse des zu benutzenden Authentisierungsservers muss in den Konfigurationsdaten des Anmeldeprozesses korrekt eingetragen sein. Will sich ein/e Benutzer/in nun am System anmelden - gleichgültig ob sie/er dazu eine RAS-Verbindung benutzt oder sich direkt im LAN befindet - laufen grob vereinfacht folgende Schritte ab:

- Findet ein Verbindungsaufbau mit dem System- oder RAS-Anmeldeprozess statt, kontaktiert dieser den Authentisierungsserver und informiert ihn über den eingegangenen Verbindungswunsch einer Benutzerin bzw. eines Benutzers. Der Authentisierungsserver sendet - sofern ein "Challenge-Response" Verfahren zum Einsatz kommt - eine so genannte "Challenge" an den Prozess zurück, der diese an den/die Benutzer/in weiterleitet.
- Der/die Benutzer/in gibt ihr/sein Authentisierungsgeheimnis ein. Dies kann je nach verwendetem System ein Passwort oder ein Einmalpasswort in den unterschiedlichsten Ausprägungen (Nummern, Text) sein.
- Der Anmeldeprozess leitet die Daten (meist transparent für Benutzer/innen) an den Authentisierungsserver weiter.
- Der Authentisierungsserver verifiziert die Benutzerdaten und signalisiert dem Anmeldeprozess das Ergebnis der Überprüfung.
- Der Zugang zum (Access-)Netz wird nach erfolgreicher Überprüfung gewährt.

Durch die Verwendung von zentralen Authentisierungsservern kann erreicht werden, dass einerseits die Authentisierungsdaten konsistent verwaltet werden und andererseits bessere Authentisierungsmechanismen genutzt werden können, als sie von den Betriebssystemen standardmäßig unterstützt werden. Hier sind insbesondere Chipkarten- und Token-basierte Mechanismen zu nennen. Je nach System erzeugen diese z.B. Einmalpasswörter, die auf einem Display angezeigt werden und welche der/die Benutzer/in als Passwort angeben muss.

Für mittlere und große Netze wird die Verwendung von Authentisierungsservern insbesondere im RAS-Bereich empfohlen, da diese eine wesentlich höhere Sicherheit bei der Benutzer-Authentisierung bieten. Berücksichtigt werden muss jedoch, dass auch diese Server administriert und gewartet werden müssen. Ein Authentisierungsserver muss so im Netz platziert werden, dass er einerseits performant erreicht werden kann, aber andererseits auch vor unberechtigten Zugriffen geschützt ist.

SYS 7.8 Einsatz geeigneter Tunnel-Protokolle für die RAS-Kommunikation

Relevanz: Umsetzung/Wartung;

Wird über Remote Access auf ein LAN zugegriffen, so geschieht dies über eine Datenverbindung, an deren Bereitstellung meist externe Dritte beteiligt sind. So wird beispielsweise bei der Nutzung der direkten Einwahl (Direct Dial-In) das Netz des Telekommunikationsanbieters benutzt. Geschieht der Verbindungsaufbau über das Internet, so werden die Daten über die Netze der beteiligten Internetdienstanbieter (und ggf. deren Kooperationspartner) geleitet. Da über eine RAS-Verbindung die direkte Anbindung des RAS-Clients in ein LAN erfolgt, muss der zur Datenübertragung benutzte Netzpfad so abgesichert werden, dass die Sicherheit der Daten (Vertraulichkeit, Integrität, Authentizität) gewährleistet ist. Die Absicherung wird durch das Verschlüsseln und das Signieren der ausgetauschten Datenpakete erreicht, nachdem die Kommunikationspartner authentisiert wurden. Im RAS-Umfeld haben sich verschiedene Verfahren und Mechanismen zur Absicherung der Kommunikationsverbindung (z.B. Tunneling, vgl. SYS 7.6 Sicherer Betrieb des RAS-Systems) herausgebildet.

Die Wahl des Verfahrens, das zur Absicherung einer RAS-Verbindung zu benutzen ist, hängt von verschiedenen Faktoren ab, u.A.

- von den Sicherheitsanforderungen an die Stärke der Verfahren (hierdurch werden beispielsweise die Schlüssellängen bestimmt),
- von den auf Protokollebene einsetzbaren Verfahren (siehe unten),
- von den durch die RAS-Hard- und Software unterstützten Verfahren.

Generell gilt:

- Das RAS-Produkt bietet in der Regel eine Auswahl von unterstützten Standardverfahren zur Kommunikationsabsicherung an. Hier sollte eine möglichst breite Unterstützung von Verfahren angestrebt werden und entsprechende Standards angewendet werden (beispielsweise IPSEC, SSL/TLS).
- Die zum Datentransport benutzten Protokolle bieten selbst schon Sicherheitsmechanismen an. Diese können vom RAS-Produkt genutzt werden. Alternativ kann das RAS-Produkt auch eigene Verfahren anbieten.

Die Sicherheitsmechanismen basieren auf unterschiedlichen kryptographischen Verfahren.

5.8 Gesicherte Anbindung an Fremdnetze (Internet-Sicherheit)

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

Die Vernetzung vorhandener Teilnetze mit globalen Netzen wie dem Internet führt zu einem neuen Informationsangebot, lässt aber auch neue Gefährdungen entstehen, da prinzipiell nicht nur ein Informationsfluss von außen in das zu schützende Netz stattfinden kann, sondern auch in die andere Richtung. Darüber hinaus gefährdet die Möglichkeit remote, d.h. von einem entfernten Rechner aus (z.B. aus dem Internet), Befehle auf Rechnern im lokalen Netz ausführen zu lassen, die Integrität und die Verfügbarkeit der lokalen Rechner und dadurch indirekt auch die Vertraulichkeit der lokalen Daten.

Ein zu schützendes Teilnetz sollte daher nur dann an ein anderes Netz angeschlossen werden, wenn dies unbedingt erforderlich ist. Dies gilt insbesondere für Anschlüsse an das Internet. Dabei ist auch zu prüfen, inwieweit das zu schützende Netz in anschließbare, nicht anschließbare und bedingt anschließbare Teile segmentiert werden muss.

IT-Systeme, die zeitweise oder dauernd an Produktionsnetze angeschlossen sind, dürfen nur unter Verwendung ausreichender Sicherheitseinrichtungen mit Fremdnetzen verbunden werden. Diese Sicherheitseinrichtungen, die im Allgemeinen aus einem zwei- oder mehrstufigen System bestehen, werden im Folgenden als “Firewalls” bezeichnet.

Zur Absicherung von Netzwerken gibt es eine Vielzahl von Tutorials und weiterführenden Informationsquellen (z.B. [NSA-SD7]). Im Folgenden werden grundsätzliche Maßnahmen zur Gewährleistung einer sicheren Anbindung an Fremdnetze, wie etwa das Internet, angeführt.

Im Bereich der Öffentlichen Verwaltung ist die periodisch aktualisierte Internet Policy [IKT-IPOL] der Stabsstelle IKT-Strategie des Bundes (CIO) zur Anwendung empfohlen.

SYS 8.1 Erstellung einer Internet-Sicherheitspolitik

Relevanz: Management; Umsetzung/Wartung;

Eine Internet-Sicherheitspolitik stellt eine IT-Systemsicherheitspolitik im Sinne von Kap. 5.3 des Teiles 1 [KIT S01] des vorliegenden Handbuches dar. Sie muss mit der organisationsweiten IT-Sicherheitspolitik der Behörde bzw. des Unternehmens kompatibel sein.

Die Erstellung der Internet-Sicherheitspolitik umfasst im Wesentlichen folgende Schritte (vgl. SMG 1.2 Erarbeitung einer organisationsweiten IT-Sicherheitspolitik):

- Festlegung der Sicherheitsziele
- Auswahl der Kommunikationsanforderungen
- Diensteauswahl
- organisatorische Regelungen

Beispiele für *Sicherheitsziele* sind:

- Schutz des internen Netzes gegen unbefugten Zugriff von außen,
- Schutz einer Firewall gegen Angriffe aus dem externen Netz, aber auch gegen Manipulationen aus dem internen Netz,
- Schutz der lokal übertragenen und gespeicherten Daten gegen Angriffe auf deren Vertraulichkeit oder Integrität,
- Schutz der lokalen Netzkomponenten gegen Angriffe auf deren Verfügbarkeit (insbesondere gilt dies auch für Informationsserver, die Informationen aus dem internen Bereich für die Allgemeinheit zur Verfügung stellen),
- Verfügbarkeit der Informationen des externen Netzes im zu schützenden internen Netz, (Die Verfügbarkeit dieser Informationen muss aber gegenüber dem Schutz der lokalen Rechner und Informationen zurückstehen!),
- Schutz vor Angriffen, die auf IP-Spoofing beruhen oder die Source-Routing Option, das ICMP-Protokoll bzw. Routingprotokolle missbrauchen,
- Schutz vor Angriffen durch das Bekannt werden von neuen sicherheitsrelevanten Softwareschwachstellen. (Da die Anzahl der potentiellen Angreifer/innen und deren Kenntnisstand bei einer Anbindung an das Internet als sehr hoch angesehen werden muss, ist dieses Sicherheitsziel von besonderer Bedeutung.)

Im nächsten Schritt ist festzulegen, welche Arten der Kommunikation mit dem äußeren Netz zugelassen werden. Bei der *Auswahl der Kommunikationsanforderungen* müssen speziell die folgenden Fragen beantwortet werden:

- Welche Informationen dürfen nach außen hindurch- bzw. nach innen hereingelassen werden?
- Welche Informationen sollen verdeckt werden (z.B. die interne Netzstruktur oder die Benutzernamen)?
- Welche Authentisierungsverfahren sollen benutzt werden (z.B. Einmalpasswörter oder Chipkarten)?
- Welche Zugänge werden benötigt (z.B. nur über einen Internet-Service-Provider oder auch über einen Modempool)?
- Welcher Datendurchsatz ist zu erwarten?

Diensteauswahl

Im dritten Schritt wird aus den Kommunikationsanforderungen abgeleitet, welche Dienste im zu sichernden Netz erlaubt und welche verboten werden müssen.

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

In der Sicherheitspolitik muss für jeden Dienst explizit festgelegt werden,

- welche Dienste für welche Benutzer/innen und/oder Rechner zugelassen werden sollen und
- für welche Dienste Vertraulichkeit und/oder Integrität gewährleistet werden müssen.

Es sollten nur die Dienste zugelassen werden, die unbedingt notwendig sind. Alle anderen Dienste müssen verboten werden. Dies muss auch die Voreinstellung sein: Alle Dienste, für die noch keine expliziten Regeln festgelegt wurden, dürfen nicht zugelassen werden.

Die Entscheidung darüber, zu welchen Diensten ein/e Benutzer/in im Internet Zugang erhalten kann, hängt von der Qualität der Firewall, vom dienstlichen Aufgabenbereich der Benutzerin bzw. des Benutzers sowie von ihrem/seinem Problembewusstsein ab.

Es muss festgelegt werden, ob und welche der übertragenen Nutzinformationen gefiltert bzw. überprüft werden sollen (z.B. zur Kontrolle auf Viren).

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

Ausnahmeregelungen, insbesondere für neue Dienste und kurzzeitige Änderungen (z.B. für Tests), müssen vorgesehen werden.

Darüber hinaus sind eine Reihe von *organisatorischen Regelungen* erforderlich, wie beispielsweise:

- Es müssen Verantwortliche sowohl für die Erstellung als auch für die Umsetzung und die Kontrolle der Einhaltung der Internet-Sicherheitspolitik benannt werden (z.B. Bereichs-IT-Sicherheitsbeauftragte, s. Teil 1 des vorliegenden Handbuches [KIT S01]).
- Es muss festgelegt werden, welche Informationen protokolliert werden und wer die Protokolle auswertet. Es müssen sowohl alle korrekt aufgebauten als auch die abgewiesenen Verbindungen protokolliert werden. Die Protokollierung muss den datenschutzrechtlichen Bestimmungen entsprechen.
- Die Benutzer/innen müssen über ihre Rechte, insbesondere auch über den Umfang der Nutzdaten-Filterung, umfassend informiert werden.
- Jeder Internetdienst birgt Gefahren, die nicht auf technischer Ebene durch eine Firewall abgefangen werden können. Es ist daher eine Schulung erforderlich, die dem/der Benutzer/in mögliche Risiken aufzeigt und ihr/sein Problembewusstsein fördert.

- Angriffe auf eine Firewall sollten nicht nur erfolgreich verhindert, sondern auch frühzeitig erkannt werden können. Angriffe können über die Auswertung der Protokolldateien erkannt werden. Die Firewall sollte aber auch in der Lage sein, auf Grund von vordefinierten Ereignissen, wie z.B. häufigen fehlerhaften Passworteingaben auf einem Application-Gateway oder Versuchen, verbotene Verbindungen aufzubauen, Warnungen auszugeben oder evtl. sogar Aktionen auszulösen.
- Es ist zu klären, welche Aktionen bei einem Angriff gestartet werden, ob z.B. der/die Angreifer/in verfolgt werden soll oder ob die Netzverbindungen nach außen getrennt werden sollen. Da hiermit starke Eingriffe in den Netzbetrieb verbunden sein können, müssen Verantwortliche bestimmt sein, die entscheiden können, ob ein Angriff vorliegt, und die entsprechenden Maßnahmen einleiten. Die Aufgaben und Kompetenzen für die betroffenen Personen und Funktionen müssen eindeutig festgelegt sein.
- Daneben müssen je nach Organisationsstruktur und -größe ein oder mehrere Verantwortliche für die Pflege der angebotenen Kommunikationsdienste benannt werden. Neben dem Serverbetrieb wie Mail-, News- oder FTP-Server müssen auch die von den Benutzerinnen bzw. Benutzern eingesetzten Kommunikationsclients betreut werden.

SYS 8.2 Entwicklung eines Firewallkonzeptes

Relevanz: Umsetzung/Wartung;

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

Die Firewall muss

- auf einer umfassenden Sicherheitspolitik aufsetzen (vgl. SYS 8.1 Erstellung einer Internet-Sicherheitspolitik),
- in der IT-Sicherheitspolitik und dem IT-Sicherheitskonzept der Organisation eingebettet sein,
- korrekt installiert und
- korrekt administriert werden.

Der Anschluss an ein Fremdnetz darf erst dann erfolgen, wenn überprüft worden ist, dass mit dem gewählten Firewallkonzept sowie den personellen und organisatorischen Randbedingungen alle Risiken beherrscht werden können.

Die Aufgaben und Anforderungen an die Firewall müssen in der Internet-Sicherheitspolitik festgelegt werden.

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

- Jede Kommunikation zwischen den beiden Netzen muss ausnahmslos über die Firewall geführt werden. Dafür muss sichergestellt sein, dass die Firewall die einzige Schnittstelle zwischen den beiden Netzen darstellt. Es müssen Regelungen getroffen werden, dass keine weiteren externen Verbindungen unter Umgehung der Firewall geschaffen werden dürfen. Wählleitungsmodems stellen prinzipiell ein erhöhtes Sicherheitsrisiko dar; sie sind daher nur über Firewalls oder äquivalente Sicherheitsmaßnahmen in das Netz einzubinden.

- Eine Firewall darf nur zwei Anschlüsse (sicheres / unsicheres Netz) haben.
- Eine Firewall darf ausschließlich als schützender Übergang zum internen Netz eingesetzt werden, daher dürfen auf einer Firewall nur die dafür erforderlichen Dienste verfügbar sein und keine weiteren Dienste wie z.B. Remote-Login angeboten werden.
- Ein administrativer Zugang zur Firewall darf nur über einen gesicherten Weg möglich sein, also z.B. über eine gesicherte Konsole, eine verschlüsselte Verbindung oder ein separates Netz.
- Eine Firewall baut auf einer für das zu schützende Netz definierten Sicherheitspolitik auf und gestattet nur die dort festgelegten Verbindungen. Diese Verbindungen müssen nach IP-Adresse, Dienst, Zeit, Richtung getrennt festgelegt werden können. Eine Festlegung der Verbindungen auf Benutzerebene ist anzustreben.
- Jede Sicherheitspolitik muss konzeptionell auf bestmögliche Reduktion des eventuellen Schadensfalles ausgelegt sein (Betrieb von Teilnetzen, frühzeitiger Einsatz von Routern, ...). In diesem Zusammenhang ist auch der Raum, in dem die Firewall betrieben wird, zusammen mit den Netzwerkeinrichtungen wie Routern einer besonderen Zugangskontrolle zu unterwerfen (vgl. INF 1.4 Zutrittskontrolle und INF 5.6 Serverräume).
- Es ist zu entscheiden, ob besonders sensible Daten im Netz besser und kostengünstiger durch organisatorische als durch technische Maßnahmen geschützt werden sollen.
- Für die Konzeption und den Betrieb einer Firewall muss geeignetes Personal zur Verfügung stehen. Der zeitliche Aufwand für den Betrieb einer Firewall darf nicht unterschätzt werden. Alleine die Auswertung der angefallenen Protokolldaten nimmt erfahrungsgemäß viel Zeit in Anspruch. Die Logfiles sollten täglich (mindestens jedoch zweimal pro Woche) kontrolliert werden. Ein Firewall-Administrator muss fundierte Kenntnisse über die eingesetzten IT-Komponenten besitzen und auch entsprechend geschult werden.
- Das Firewallkonzept muss sich permanent an Betriebserfahrungen der Firewall sowie aktuellen Entwicklungen orientieren und bei Bedarf unverzüglich angepasst werden.
- Die Benutzer/innen des lokalen Netzes sollten durch den Einsatz einer Firewall möglichst wenig Einschränkungen hinnehmen müssen.

Eine Firewall kann das interne Netz vor vielen Gefahren beim Anschluss an das Internet schützen, aber nicht vor allen. Beim Aufbau einer Firewall und der Erarbeitung einer Firewall-Sicherheitspolitik sollte man sich daher die Grenzen einer Firewall verdeutlichen:

- Es werden Protokolle überprüft, nicht die Inhalte. Eine Protokollprüfung bestätigt beispielsweise, dass eine E-Mail mit ordnungsgemäßen Befehlen zugestellt wurde, kann aber keine Aussagen zum eigentlichen Inhalt der E-Mail machen.
- Die Filterung von aktiven Inhalten ist unter Umständen nur teilweise erfolgreich.
- Sobald Benutzer/innen eine Kommunikation über eine Firewall herstellen dürfen, können sie über das verwendete Kommunikationsprotokoll beliebige andere Protokolle tunneln. Damit könnte ein/e Innentäter/in jemandem Externen den Zugriff auf interne Rechner ermöglichen.
- Eine Einschränkung der Internetzugriffe auf festgelegte Webserver ist in der Realität unmöglich, da zu viele WWW-Server auch als Proxies nutzbar sind, so dass eine Sperrung bestimmter IP-Adressen leicht umgangen werden kann.
- Die Filtersoftware ist häufig noch unausgereift. Beispielsweise ist es möglich, dass nicht alle Arten der Adressierung erfasst werden.
- Die Filterung von Spam-Mails ist noch nicht ausgereift. Keine Firewall kann zweifelsfrei feststellen, ob eine E-Mail vom Empfänger erwünscht ist oder nicht. Spam-Mails dürften erst dann verschwinden, wenn die Absender zweifelsfrei nachweisbar sind, was noch einige Zeit dauern wird.

- Firewalls schützen nicht vor allen Denial-of-Service-Attacken. Wenn ein/e Angreifer/in z.B. die Anbindung zum Provider lahm legt, kann auch die beste Firewall nicht helfen. Außerdem gibt es immer wieder Implementationsfehler von Protokollen auf Endgeräten, die eine Firewall nicht abfangen kann.
- Leider ermöglichen viele Firewalls es nicht, durch Hintereinanderschaltung von verschiedenen Firewalls eine erhöhte Sicherheit zu erlangen. Gerade in größeren Firmen ist dies problematisch, wenn innerhalb der Firma auch Firewalls eingesetzt werden, z.B. zur Bildung von abgesicherten Teilnetzen.
- Eine Firewall kann zwar einen Netzübergang sichern, sie hat aber keinen Einfluss auf die Sicherheit der Kommunikation innerhalb dieser Netze!

SYS 8.3 Installation einer Firewall

Relevanz: Umsetzung/Wartung;

Bei der Installation einer Firewall sind folgende Schritte in der angegebenen Reihenfolge zu setzen (vgl. [KIT S04]):

- Festlegen der Sicherheitspolitik sowie der Benutzerordnung durch organisatorisch und technisch Verantwortliche in Zusammenarbeit mit Benutzervertretern/Benutzervertreterinnen (vgl. auch PER 1.1 Verpflichtung der Mitarbeiter/innen auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen)
- Bestimmung der Sicherheitsverantwortlichen (Datenschutz-/IT-Sicherheitsbeauftragte/r (soweit nicht bereits nominiert) und Bereichs-IT-Sicherheitsbeauftragte/r (”Internet-Sicherheitsbeauftragte/r”) lt. Teil 1 des vorliegenden Handbuches [KIT S01])
- Definition der angebotenen und anzufordernden Dienste
- Analyse der Hard- und Softwarevoraussetzungen im internen Netz
- Auswahl geeigneter Produkte
- *Installation und Konfiguration der Firewall*
  Der administrative Zugang zur Sicherheitseinrichtung darf nur über einen gesicherten Weg möglich sein.
- Überprüfung der Installation durch Querlesen der Definitionen und Funktionskontrolle
- Dokumentation der Installation zum Zweck der Nachvollziehbarkeit, der Wartung und der Validierung
- Laufende Beobachtung und Wartung
- Periodische Sicherheitsüberprüfung durch befugte Externe zu nicht angekündigten Zeitpunkten mindestens einmal im Quartal (”Screening”, vgl. SYS 8.4 „Sicherer Betrieb einer Firewall“) sowie Weitermeldung der erhobenen Fakten an die/den Vorgesetzte/n
- Revision der Behebung der bei den Sicherheitstests erhobenen Mängel
- Sammlung der relevanten Projekterfahrungen als Grundlage für eine Weiterentwicklung der Internet-Sicherheitspolitik und des Firewallkonzeptes. Im Bereich der öffentlichen Verwaltung sollten diese Projekterfahrungen an die IKT Koordinierungsstelle weitergegeben werden.
- Aus- und Weiterbildung des administrierenden Personals

SYS 8.4 Sicherer Betrieb einer Firewall

Relevanz: Umsetzung/Wartung;

Für einen sicheren Betrieb einer Firewall sind eine fachgemäße Administration sowie eine regelmäßige Überprüfung auf die korrekte Einhaltung der umgesetzten Sicherheitsmaßnahmen (Screening) erforderlich.

Insbesondere müssen die für den Betrieb der Firewall getroffenen organisatorischen Regelungen regelmäßig oder zumindest sporadisch auf ihre Einhaltung überprüft werden. Es sollte in zyklischen Abständen kontrolliert werden, ob neue Zugänge unter Umgehung der Firewall geschaffen wurden. Alle Sicherheitskontrollen sollten zumindest teilweise auch durch Externe vorgenommen werden.

Administration

Die Administration einer Firewall umfasst die nachfolgend angeführten Aufgaben:

- Anlegen und Entfernen von Benutzerinnen/Benutzern, Profilen, Filtern etc.
- Ändern von Berechtigungen, Funktionen etc.
- Kontrolle und Auswertung der Logfiles
- Einschränken und Beenden des Internetzugangs
- Weiterleitung sicherheitsrelevanter Beobachtungen an die in der Sicherheitspolitik definierten Instanzen
- Benachrichtigung der zuständigen Instanzen bei Entdecken von Angriffen aus dem Internet
- Verfolgen der aktuellen Entwicklungen im Bereich Sicherheit (z.B. durch Lesen der entsprechenden Newsgroups) sowie entsprechende Weiterbildung

Durch eine angemessene Stellvertreterregelung (und eine entsprechende Schulung der Stellvertreter/innen) ist eine kontinuierliche Administration zu gewährleisten.

Regelmäßige Überprüfung

Zusätzlich zu den regelmäßigen Wartungsaktivitäten ist es erforderlich, eine Firewall regelmäßig (etwa einmal pro Quartal) durch eine geeignete Instanz kontrollieren zu lassen. Sicherheitsrelevante Änderungen erfordern zusätzlich “ad hoc”-Kontrollen. Diese Kontrollen sollten vorzugsweise durch eine vertrauenswürdige externe Instanz erfolgen, da die Gefahr besteht, dass Firewall-Administratoren durch Gewöhnungseffekte und Routinearbeit bestimmte Sicherheitslücken übersehen könnten, die neutralen Beobachtern mit hoher Wahrscheinlichkeit auffallen. (Vgl. auch: “Screening, Security Compliance Checking”.)

Eine derartige Prüfung ist wie folgt durchzuführen:

- Überprüfung der Installation von außen
- interne Überprüfung der Internet-Sicherheitspolitik
- interne Überprüfung der Konfiguration
- interne Durchführung eventuell notwendiger Korrekturen
- erneute Prüfung von außen

Dabei sind die folgenden Punkte zu beachten:

- Alle Filterregeln müssen korrekt umgesetzt sein. Dabei ist zu testen, dass nur die Dienste zugelassen werden, die in der Sicherheitspolitik vorgesehen sind.
- Die Defaulteinstellung der Filterregeln und die Anordnung der Komponenten müssen sicherstellen, dass alle Verbindungen, die nicht explizit erlaubt sind, blockiert werden. Dies muss auch bei einem völligen Ausfall der Firewall-Komponenten gelten.
- Es muss die Regel "Alles, was nicht ausdrücklich erlaubt ist, ist verboten" realisiert sein. So darf z.B. ein/e Benutzer/in, die/der keinen Eintrag in einer Access-Liste hat, keine Möglichkeit haben, Dienste des Internets zu benutzen.
- Um ein Mitlesen oder Verändern der Authentisierungsinformationen zu verhindern, dürfen sich Administrator und Revisor nur über einen vertrauenswürdigen Pfad authentisieren. Dies könnte z.B. direkt über die Konsole, eine verschlüsselte Verbindung oder ein separates Netz erfolgen.
- Es müssen in regelmäßigen Abständen Integritätstests der eingesetzten Software durchgeführt werden. Im Fehlerfall ist die Firewall abzuschalten.
- Die Firewall muss auf ihr Verhalten bei einem Systemabsturz getestet werden. Insbesondere darf kein automatischer Neustart möglich sein, und die Access-Listen müssen auf einem schreibgeschützten Medium speicherbar sein. Die Access-Listen sind die wesentlichen Daten für den Betrieb der Firewall und müssen besonders gesichert werden, damit keine alten oder fehlerhaften Access-Listen bei einem Neustart benutzt werden, der durch eine/n Angreifer/in provoziert wird.
- Bei einem Ausfall der Firewall muss sichergestellt sein, dass in dieser Zeit keine Netzverbindungen aus dem zu schützenden Netz heraus oder zu diesem aufgebaut werden können.
- Auf den eingesetzten Komponenten dürfen nur Programme, die für die Funktionsfähigkeit der Firewall nötig sind, vorhanden sein. Der Einsatz dieser Programme muss ausführlich dokumentiert und begründet werden. Beispielsweise sollten die Software für die graphische Benutzeroberfläche sowie alle Treiber, die nicht benötigt werden, entfernt werden. Diese sollten auch aus dem Betriebssystem-Kern entfernt werden. Das Verbleiben von Software muss dokumentiert und begründet werden.
- Beim Wiedereinspielen von gesicherten Datenbeständen muss darauf geachtet werden, dass für den sicheren Betrieb der Firewall relevante Dateien wie Access-Listen, Passwortdateien oder Filterregeln auf dem aktuellsten Stand sind.

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

SYS 8.5 Firewalls und aktive Inhalte

Relevanz: Umsetzung/Wartung;

Eines der größten Probleme bei der Konzeption einer Firewall ist die Behandlung der Probleme, die durch die Übertragung aktiver Inhalte zu den Rechnern im zu schützenden Netz entstehen. Hierunter fällt nicht nur die Erkennung und Beseitigung von Viren, die verhältnismäßig einfach auch auf den Rechnern der Anwender/innen durchgeführt werden kann, sondern auch das weit schwieriger zu lösende Problem der Erkennung von ActiveX-Controls, Java-Applets oder Scripting-Programmen mit einer Schadfunktion. Hierfür existieren zurzeit noch keine brauchbaren Programme, die eine ähnlich wirksame Erkennung von Schadfunktionen ermöglichen, wie sie im Bereich der Viren möglich sind.

Die Größe der Gefährdung, die von aktiven Inhalten für die Rechner im zu schützenden Netz ausgeht, lässt sich anhand des folgenden Beispiels darstellen. Ein Java-Applet bzw. der Browser darf gemäß der Java-Spezifikationen eine Netzverbindung zu dem Server aufbauen, von dem es geladen worden ist. Diese zurzeit noch recht wenig benutzte Möglichkeit ist eine zentrale Voraussetzung, wenn Netz-Computer (NC) oder Ähnliches eingesetzt werden sollen, die auch ohne spezielle Initiierung durch den/die Anwender/in Programme vom Server laden müssen. Um diese Eigenschaft trotz der Verwendung eines Paket-Filters vollständig unterstützen zu können, müssen sehr viel mehr Portnummern freigeschaltet werden oder es muss ein dynamischer Paket-Filter eingesetzt werden. Ist das der Fall, können Java-Applets verwendet werden, um kaum zu kontrollierende IP-Verbindungen aufbauen zu können.

Es gibt generell zwei Ansätze, wie der Problematik - aktive Inhalte mit Schadfunktion - begegnet werden kann. Zum einen kann die Kontrolle und damit auch die Verantwortung für die Ausführung auf die Benutzer/innen verlagert werden, die in ihren Browsern die Möglichkeit haben, die aktiven Inhalte abzuschalten und nur bei einzelnen - vertrauenswürdigen - Angeboten wieder einzuschalten. Das Hauptproblem bei dieser Lösung ist, wie festgestellt werden kann, welche Anbieter vertrauenswürdig sind und welche nicht.

Die zweite Möglichkeit, aktive Inhalte zu kontrollieren, besteht im Einsatz eines entsprechenden Filters in Verbindung mit einer Firewall. Proxy-Prozesse sind aufgrund ihres Aufbaus prinzipiell sehr gut dazu geeignet, die übertragenen Nutzdaten zu analysieren. Die entsprechenden Programme werden über spezielle Tags (Tag = Kennzeichen für Strukturen innerhalb einer HTML-Seite) innerhalb einer HTML-Seite aufgerufen. Denkbar ist also die Lösung, alle Zeilen mit entsprechenden Tags aus einer HTML-Seite zu löschen oder sie durch Ausgabezeilen zu ersetzen, die dem/der Anwender/in einen Hinweis geben, dass das gewünschte Java-Applet von der Firewall abgeblockt worden ist.

Das Problem bei dieser Vorgehensweise besteht darin, dass es nicht auf einfache Weise möglich ist, alle HTML-Seiten und in diesen wiederum alle zu löschenden Tags zu erkennen. So können, und dies wird heute schon vielfach gemacht, HTML-Seiten als Inhalt einer E-Mail übertragen werden. Intelligente E-Mail-Programme erkennen dies und starten automatisch einen Browser, der diese HTML-Seite anzeigen kann und der dann natürlich auch das Java-Applet bzw. ActiveX-Control ausführt. Auch die Erkennung eines speziellen Tags innerhalb einer HTML-Seite ist aufgrund der komplexen Möglichkeiten der aktuellen HTML-Version nicht einfach.

Leider werden Java-Applets nicht durchgängig als Datei mit der Endung. *class* verschickt. Stattdessen können auch komprimierte Dateien eingesetzt werden, die z.B. die Endung *.jar* (Java-Archive) haben. Das bedeutet, dass ein Java-Filter auch alle von den verwendeten Browsern unterstützten Komprimierungsverfahren kennen und berücksichtigen muss.

Eine weitere Alternative besteht darin, eine Datenbank mit Verifikationsschlüsseln vertrauenswürdiger Hersteller anzulegen und die Signatur jedes aus dem Internet geladenen Programms zu verifizieren. Dieses Verfahren steht noch ganz am Anfang seiner Entwicklung und es bleibt abzuwarten, ob die entsprechenden Programme ähnlich wirksam werden, wie es die Programme zur Abwehr von Viren sind.

Zusätzliches Schadenspotential resultiert aus der Möglichkeit, JavaScript aus Java heraus auszuführen. Eine abgestufte Filterung von Java und JavaScript sollte deshalb auf ihre Wirksamkeit überprüft werden.

SYS 8.6 Firewalls und Verschlüsselung

Relevanz: Umsetzung/Wartung;

Da im Internet die Daten über nicht vorhersagbare Wege und Knotenpunkte verschickt werden, sollten die versandten Daten möglichst nur verschlüsselt übertragen werden. Hierbei wäre es sinnvoll, wenn entsprechende Mechanismen schon in den unteren Schichten des Protokolls vorgesehen würden.

Zunächst sollte aber unterschieden werden zwischen

- Verschlüsselung auf der Firewall bzw. auf Netzkoppelelementen, die zum Aufbau sicherer Teilnetze eingesetzt werden kann, und
- Verschlüsselung auf den Endgeräten, die z.B. von Benutzerinnen/Benutzern bedarfsabhängig eingesetzt wird.

Verschlüsselung auf der Firewall:

Um mit externen Kommunikationspartnern Daten über ein offenes Netz auszutauschen und/oder diesen Zugriff auf das eigene Netz zu geben, kann der Aufbau von virtuellen privaten Netzen (VPNs) sinnvoll sein. Dafür sollten alle Verbindungen von und zu diesen Partnern verschlüsselt werden, damit Unbefugte keinen Zugriff darauf nehmen können. Zum Aufbau von verschlüsselten Verbindungen können eine Vielzahl von Hard- und Softwarelösungen eingesetzt werden. Sollen hierbei nur wenige Liegenschaften miteinander verbunden werden, sind insbesondere Hardwarelösungen basierend auf symmetrischen kryptographischen Verfahren eine einfache und sichere Lösung.

Die Ver- bzw. Entschlüsselung kann auf verschiedenen Geräten erfolgen. So könnte eine Hardwarelösung im Paketfilter als Schlüsselgerät arbeiten. Dies ist insbesondere dann sinnvoll, wenn keine unverschlüsselte Kommunikation über dieses Gerät gehen soll. Die Integration der Verschlüsselung auf dem Application Gateway hat dagegen den Vorteil einer leichteren Benutzerverwaltung. Zudem kann ein/e Angreifer/in, der/die einen externen Informationsserver unter seine/ihre Kontrolle gebracht hat, die verschlüsselte Kommunikation nicht belauschen.

Verschlüsselung auf den Endgeräten:

Zum Schutz der Vertraulichkeit bestimmter Daten, insbesondere bei der Versendung von E-Mails, bietet sich auch der Gebrauch von Mechanismen an, die eine Ende-zu-Ende-Verschlüsselung ermöglichen. Hierfür wird zum Beispiel häufig das frei verfügbare Programmpaket PGP (Pretty Good Privacy) eingesetzt. Für eine vertrauenswürdige Datenübertragung mit ausgewählten Partnern im Internet sollten geänderte telnet und ftp Programme eingesetzt werden, die eine Verschlüsselung der übertragenen Daten unterstützen.

Die Verschlüsselung auf den Endsystemen wird auf absehbare Zeit noch applikationsgebunden sein, z.B. durch den Einsatz von S/MIME, SSL oder PGP. Die Verschlüsselung von Daten stellt andererseits aber auch ein großes Problem für den wirksamen Einsatz von Firewalls dar, d.h. den Filtern. Wenn die Übertragung verschlüsselter Daten über die Firewall zugelassen wird (z.B. SSL), sind Filter auf der Anwendungsschicht nicht mehr in der Lage, die Nutzdaten z.B. in Hinblick auf Viren oder andere Schadprogramme zu kontrollieren. Auch die Protokollierungsmöglichkeiten werden durch eine Verschlüsselung stark eingeschränkt. Eine erste ad-hoc-Lösung könnte darin

bestehen, von bestimmten internen Rechnern den Aufbau von SSL-Verbindungen zu erlauben, u.U. nur zu ausgewählten Zielsystemen. Andererseits sind die Daten selbst dann geschützt, wenn ein/e Angreifer/in das Application Gateway unter seine/ihre Kontrolle gebracht hat.

Eine temporäre Entschlüsselung auf einer Filterkomponente zu Analysezwecken ist weder praktikabel noch wünschenswert.

Eine generelle Empfehlung für oder gegen den Einsatz von Verschlüsselung über oder an der Firewall kann nicht gegeben werden, dies hängt von den Anforderungen im Einzelfall ab.

SYS 8.7 Festlegung einer Sicherheitspolitik für E-Mail-Nutzung

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

Vor der Freigabe von E-Mail-Systemen sollte festgelegt werden, für welchen Einsatz E-Mail vorgesehen ist. Abhängig davon differieren auch die Ansprüche an Vertraulichkeit, Verfügbarkeit, Integrität und Verbindlichkeit der zu übertragenden Daten sowie des eingesetzten E-Mail-Programms. Es muss geklärt werden, ob über E-Mail ausschließlich unverbindliche oder informelle Informationen weitergegeben werden sollen oder ob einige oder sogar alle der bisher schriftlich bearbeiteten Geschäftsvorfälle nun per E-Mail durchgeführt werden sollen. Bei letzterem ist zu klären, wie Anmerkungen an Vorgängen wie Verfügungen, Abzeichnungen oder Schlusszeichnungen, die bisher handschriftlich angebracht wurden, elektronisch abgebildet werden sollen. Weiters ist festzulegen, ob und in welchem Rahmen eine private Nutzung von E-Mail erlaubt ist.

Die Organisation muss eine E-Mail-Sicherheitspolitik festlegen, in der folgende Punkte beschrieben sind:

- Wer einen E-Mail-Anschluss erhält,
- welche Regelungen von den Mail-Administratoren und den E-Mail-Benutzerinnen/Benutzern zu beachten sind (vgl. SYS 8.8 Regelung für den Einsatz von E-Mail und anderen Kommunikationsdiensten),
- bis zu welchem Vertraulichkeits- bzw. Integritätsanspruch Informationen per E-Mail versandt werden dürfen (vgl. dazu auch Kap. 3.2.5 in Teil 1 dieses Handbuches [KIT S01]),
- ob und unter welchen Rahmenbedingungen eine private Nutzung von E-Mail erlaubt ist,
- wie die Benutzer/innen geschult werden und
- wie jederzeit technische Hilfestellung für die Benutzer/innen gewährleistet wird.

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

- Für Organisationen im öffentlichen Bereich sind die im Rahmen der Internet-Policy [IKT-IPOL] enthaltenen E-Mail Richtlinien [IKT-MPOL] gemäß IKT-Board-Beschluss vom 17.09.2002 [IKTB-170902-1] umzusetzen.
- Die E-Mail-Progamme der Benutzer/innen müssen durch die Systemadministration so vorkonfiguriert sein, dass ohne weiteres Zutun der Benutzer/innen maximale Sicherheit erreicht werden kann (siehe auch SYS 8.11 „Sichere Konfiguration der Mailclients“).

- Für E-Mail-Adressen sind Namenskonventionen festzulegen. Insbesondere ist darauf zu achten, dass Sonderzeichen (Umlaute, ...) vermieden werden, da diese inhaltlich nicht einheitlich codiert sind. (vgl. E-Mail Richtlinien [IKT-MPOL] im Rahmen der Internet-Policy [IKT-IPOL] gemäß [IKTB-170902-1] für Organisationen der öffentlichen Verwaltung zur Anwendung empfohlen)
- Für E-Mail-Adressen in Behörden bzw. in Organisationen der öffentlichen Verwaltung ist die in der anzuwendenden E-Mail-Policy enthaltene Naming-Policy empfohlen. (gemäß [IKTB-170902-1]).
- Neben personenbezogenen E-Mail-Adressen können auch organisations- bzw. funktionsbezogene E-Mail-Adressen eingerichtet werden. Dies ist insbesondere bei zentralen Anlaufstellen wichtig.
- Die Übermittlung von Daten darf erst nach erfolgreicher Identifizierung und Authentisierung des Senders beim Übertragungssystem möglich sein.
- Die Benutzer/innen müssen vor erstmaliger Nutzung von E-Mail in die Handhabung der relevanten Applikationen eingewiesen werden. Die organisationsinternen Benutzerregelungen zur Dateiübermittlung müssen ihnen bekannt sein.
- Zur Beschreibung des Absenders werden bei E-Mails so genannte Signatures (Absenderangaben) an das Ende der E-Mail angefügt. Der Inhalt einer Signature sollte dem eines Briefkopfs ähneln, also Name, Organisationsbezeichnung und Telefonnummer u.ä. enthalten. Eine Signature sollte nicht zu umfangreich sein, da dies nur unnötig Übertragungszeit und Speicherplatz kostet. Die Behörde bzw. das Unternehmen sollte einen Standard für die einheitliche Gestaltung von Signatures festlegen.
- Von den eingesetzten Sicherheitsmechanismen hängt es ab, bis zu welchem Vertraulichkeitsanspruch Dateien per E-Mail versandt werden dürfen. Es ist grundsätzlich festzulegen, ob Mails bzw. Attachments in verschlüsselter Form übertragen werden dürfen. Dies erhöht zwar die Sicherheit gegen unautorisiertes Lesen oder Verändern, erschwert aber die Suche nach Viren oder macht sie gänzlich unmöglich. Ist der Einsatz von Verschlüsselungsverfahren prinzipiell erlaubt, so sollte geregelt werden, ob und wann übertragene Dateien verschlüsselt werden müssen (siehe auch Kap. 3.2.5 in Teil 1 dieses Handbuches [KIT S01] und Kap. „Kryptographische Maßnahmen“). Gleichermaßen ist festzulegen, ob und in welcher Form kryptographische Mechanismen zur Überprüfung der Integrität von Daten (MACs, Digitale Signaturen, ...) eingesetzt werden dürfen bzw. müssen. Es ist zentral festzulegen, welche Applikationen für die Verschlüsselung bzw. den Einsatz von elektronischen Signaturen von den Benutzerinnen/Benutzern zu verwenden sind. Diese müssen den Benutzerinnen/Benutzern zur Verfügung gestellt werden, die wiederum in deren Anwendung unterwiesen werden müssen.
- Für Organisationen der Öffentlichen Verwaltung sind die „Richtlinien für E-Mail Zertifikate in der Verwaltung“ [IKT-MZERT] gemäß IKT-Board Beschluss [IKTB-230903-17] zu beachten.
- Es sollte festgelegt werden, unter welchen Bedingungen ein- oder ausgehende E-Mails zusätzlich ausgedruckt werden müssen.
- Die Dateiübertragung kann (optional) dokumentiert werden. Für jede stattgefundene Übermittlung ist dann in einem Protokoll festzuhalten, wer wann welche Informationen erhalten hat. Bei der Übertragung personenbezogener Daten sind die gesetzlichen Vorgaben zur Protokollierung zu beachten.
- Ob und wie ein externer Zugang zu E-Mail Diensten technisch und organisatorisch realisiert werden soll, ist zu prüfen und muss festgelegt werden. Technisch ist ein E-Mail-Zugang von Außen geeignet abzusichern, z.B. VPN, etc. In Organisationen der öffentlichen Verwaltung ist gemäß IKT-Board Beschluss [IKTB-110903-8] die Möglichkeit der Identifikation und Authentifikation mittels Bürgerkarte zu beachten.

E-Mails, die intern versandt werden, dürfen das interne Netz nicht verlassen. Dies ist durch die entsprechenden administrativen Maßnahmen sicherzustellen. Beispielsweise sollte die Übertragung von E-Mails zwischen verschiedenen Liegenschaften einer Organisation über eigene Standleitungen und nicht über das Internet erfolgen. Durch heutige Techniken (z.B. VPN) entfällt diese Forderung, wenn Nachrichten entsprechend verschlüsselt werden.

SYS 8.8 Regelung für den Einsatz von E-Mail und anderen Kommunikationsdiensten

Relevanz: Umsetzung/Wartung; Anwender/innen;

Für den Einsatz von E-Mails sind u.a. folgende Punkte zu beachten:

- Die Adressierung von E-Mail muss eindeutig erfolgen, um eine fehlerhafte Zustellung zu vermeiden. Innerhalb einer Organisation sollten Adressbücher und Verteilerlisten gepflegt werden, um die Korrektheit der gebräuchlichsten Adressen sicherzustellen. Durch den Versand von Testnachrichten an neue E-Mail-Adressen ist die korrekte Zustellung von Nachrichten zu prüfen.
- Für alle nach außen gehenden E-Mails ist eine Signatur (Absenderangabe am Ende der Mail) zu verwenden.
- Ausgehende E-Mails sollten protokolliert werden, da E-Mails auch “verschwinden” können.
- Die Betreffangabe (Subject) des Kommunikationssystems sollte immer ausgefüllt werden, z.B. entsprechend der Betreffangabe in einem Anschreiben.
- Die Korrektheit der durchgeführten Datenübertragung sollte überprüft werden. Die Empfängerseite sollte den korrekten Empfang überprüfen und der Senderseite bestätigen.
- Verwendung residenter Virenscanner für ein- bzw. ausgehende Dateien: Vor dem Absenden bzw. vor der Dateiübermittlung sind die ausgehenden Dateien explizit auf Viren zu überprüfen.
- Erfolgt über die E-Mail auch eine Dateiübertragung, so sollten die folgenden Informationen an den/die Empfänger/in zusätzlich übermittelt werden:
  - Art der Datei (z.B. MS Word),
  - Kurzbeschreibung über den Inhalt der Datei,
  - Hinweis, dass Dateien auf Viren überprüft sind,
  - ggf. Art des verwendeten Packprogramms (z.B. PKZIP)
  - ggf. Art der eingesetzten Software für Verschlüsselung bzw. Elektronischen Signatur.

  Jedoch sollte nicht vermerkt werden:
  - welches Passwort für die eventuell geschützten Informationen vergeben wurde,
  - welche Schlüssel ggf. für eine Verschlüsselung der Informationen verwendet wurden.
- Regelmäßiges Löschen von E-Mails: E-Mails sollten nicht unnötig lange im Posteingang gespeichert werden. Sie sollten entweder nach dem Lesen gelöscht werden oder in Benutzerverzeichnissen gespeichert werden, wenn sie erhalten bleiben sollen. Viele Mailprogramme löschen E-Mails nicht sofort, sondern transferieren sie in spezielle Ordner. Benutzer/innen müssen darauf hingewiesen werden, wie sie E-Mails auf ihren Clients vollständig löschen können.

Bei den meisten E-Mail-Systemen werden die Informationen unverschlüsselt über offene Leitungen transportiert und können auf diversen Zwischenrechnern gespeichert werden, bis sie schließlich ihre/n Empfänger/in erreichen. Auf diesem Weg können Informationen leicht manipuliert werden. Aber auch der/die Versender/in einer E-Mail hat meistens die Möglichkeit, seine/ihre Absenderadresse (From) beliebig einzutragen, so dass grundsätzlich gilt, dass man sich nicht auf die Echtheit der Absenderangabe verlassen und sich nur nach Rückfrage oder bei Benutzung von Digitalen Signaturen der Authentizität des Absenders sicher sein kann. In Zweifelsfällen sollte daher die Echtheit des Absenders durch Rückfrage oder durch den Einsatz von Verschlüsselung und/oder Digitalen Signaturen (vgl. Kap. „Kryptographische Maßnahmen“) überprüft werden.

Es ist allerdings zu beachten, dass verschlüsselte Nachrichten im Allgemeinen nicht zentral auf Viren überprüft werden können (dazu wäre die zentrale Hinterlegung der notwendigen Schlüssel erforderlich). Es ist daher in der E-Mail-Sicherheitspolitik festzulegen, ob verschlüsselte Nachrichten zugelassen sind und wie damit zu verfahren ist. Wenn verschlüsselte Nachrichten nicht zugelassen sind, können diese etwa durch eine Poststelle (s. SYS 8.10 „Einrichtung eines Postmasters“) geblockt werden.

Es ist festzulegen, ob und gegebenenfalls in welchem Rahmen eine private Nutzung von E-Mail-Diensten zulässig ist. Diese Festlegung sollte im Rahmen einer Betriebsvereinbarung oder bei Abschluss des Arbeitsvertrages getroffen werden. Weiters sind auch die zulässigen Kontrollmaßnahmen des/der Arbeitgebers/Arbeitgeberin (Protokollierung, Auswertung, ...) und die möglichen Sanktionen bei Verstößen gegen die getroffenen Vereinbarungen zu regeln.

Alle Regelungen und Bedienungshinweise zum Einsatz von E-Mail sind schriftlich zu fixieren und sollten den Mitarbeiterinnen/Mitarbeitern jederzeit zur Verfügung stehen.

Die Benutzer/innen müssen vor dem Einsatz von Kommunikationsdiensten wie E-Mail geschult werden, um Fehlbedienungen zu vermeiden und die Einhaltung der organisationsinternen Richtlinien zu gewährleisten. Insbesondere müssen sie hinsichtlich möglicher Gefährdungen und einzuhaltender Sicherheitsmaßnahmen beim Versenden bzw. Empfangen von E-Mail sensibilisiert werden.

Zur Vermeidung von Überlastung durch E-Mail sind die Mitarbeiter/innen über potentielles Fehlverhalten zu belehren. Sie sollten dabei ebenso vor der Teilnahme an E-Mail-Kettenbriefen, vor Spams, der unnötigen Weiterverbreitung von Virenwarnungen sowie vor der Abonnierung umfangreicher Mailinglisten gewarnt werden.

Benutzer/innen müssen darüber informiert werden, dass Dateien, deren Inhalt Anstoß erregen könnte, weder verschickt noch auf Informationsservern eingestellt noch nachgefragt werden dürfen.

Außerdem sollten Benutzer/innen darauf verpflichtet werden, dass bei der Nutzung von Kommunikationsdiensten

- die fahrlässige oder gar vorsätzliche Unterbrechung des laufenden Betriebes unter allen Umständen vermieden werden muss (vgl. dazu §126a zu Datenbeschädigung (StGB), BGBl. Nr. 60/1974 i.d.g.F.). Zu unterlassen sind insbesondere Versuche, ohne Autorisierung Zugang zu Netzdiensten - welcher Art auch immer - zu erhalten, Informationen, die über die Netze verfügbar sind, zu verändern, in die individuelle Arbeitsumgebung einer Netznutzerin bzw. eines Netznutzers einzugreifen oder unabsichtlich erhaltene Angaben über Rechner und Personen weiterzugeben.

- die Verbreitung von für die Allgemeinheit irrelevanten Informationen unterlassen werden muss. Die Belastung der Netze durch ungezielte und übermäßige Verbreitung von Informationen sollte vermieden werden.
- Eindringversuche an internen/externen Netzen/Geräten zu unterlassen sind,
- die Verbreitung von redundanten Informationen vermieden werden sollte.

Für den Bereich der öffentlichen Verwaltung wurde im Rahmen des IKT-Boards als Bestandteil der "Internet-Policy" [IKT-IPOL] eine "E-Mail-Policy" [IKT-MPOL] beschlossen und zur Anwendung empfohlen [IKTB-170902-1]. Nähere Details dazu sind auch unter dem Punkt SYS 8.19 „Geeignete Auswahl eines E-Mail-Clients/Server" zu finden. Darüber hinaus sind im Bereich öffentliche Verwaltung der Externe Zugang zu E-Mail-Diensten unter Beachtung des IKT-Board Beschlusses [IKTB-110903-8] zu gestalten, sowie die Handhabe von E-Mail-Zertifikaten nach den "Richtlinien für E-Mail-Zertifikate in der Verwaltung" [IKT-MZERT] der Stabsstelle IKT-Strategie des Bundes (CIO) zu richten.

SYS 8.9 Sicherer Betrieb eines Mail-Servers

Relevanz: Umsetzung/Wartung;

Der sichere Betrieb eines Mailservers setzt voraus, dass sowohl die lokale Kommunikation als auch die Kommunikation auf Seiten des öffentlichen Netzes abgesichert wird. Der Mailserver nimmt von anderen Mailservern E-Mails entgegen und leitet sie an die angeschlossenen Benutzer/innen oder Mailserver weiter. Weiters reicht der Mailserver die gesendeten E-Mails lokaler Benutzer/innen an externe Mailserver weiter. Der Mailserver muss hierbei sicherstellen, dass lokale E-Mails der angeschlossenen Benutzer/innen nur intern weitergeleitet werden und nicht in das öffentliche Netz gelangen können.

Die E-Mails werden vom Mailserver bis zur Weitergabe zwischengespeichert. Viele Internetprovider und Administratoren archivieren zusätzlich die ein- und ausgehenden E-Mails. Damit Unbefugte nicht über den Mailserver auf Nachrichteninhalte zugreifen können, muss der Mailserver gegen unbefugten Zugriff gesichert sein (vgl. dazu §126a zu Datenbeschädigung (StGB), BGBl. Nr. 60/1974 i.d.g.F.). Dafür sollte er gesichert (in einem Serverraum oder Serverschrank) aufgestellt sein. Für den ordnungsgemäßen Betrieb sind Administratoren und Stellvertreter zu benennen und zum Betrieb des Mailservers und des zugrunde liegenden Betriebssystems zu schulen. Es muss ein Postmaster-Account eingerichtet werden, an den alle unzustellbaren E-Mails und alle Fehlermeldungen weitergeleitet werden (siehe auch SYS 8.10 „Einrichtung eines Postmasters").

Auf die Mailboxen der lokal angeschlossenen Benutzer/innen dürfen nur diese Zugriff haben. Auf die Bereiche, in denen E-Mails nur temporär für die Weiterleitung zwischengespeichert werden (z.B. Spooldateien), ist der Zugriff auch für die lokalen Benutzer/innen zu unterbinden.

- Es muss regelmäßig kontrolliert werden, ob die Verbindung mit den benachbarten Mailservern, insbesondere dem Mailserver des Mail-Providers, noch stabil ist, und
- ob der für die Zwischenspeicherung der Mail zur Verfügung stehende Plattenplatz noch ausreicht, da ansonsten kein weiterer Nachrichtenaustausch möglich ist.

Umfang und Inhalt der Protokollierung der Aktivitäten des Mail-Servers sind festzulegen.

Der Mailserver sollte ein abgeschlossenes, eigenes Produktionssystem sein, insbesondere sollten von der Verfügbarkeit des Mailservers keine weiteren Dienste abhängig sein. Es sollte jederzeit kurzfristig möglich sein, ihn abzuschalten, z.B. bei Verdacht auf Manipulationen.

Die Benutzernamen auf dem Mailserver sollten nicht aus den E-Mail-Adressen unmittelbar ableitbar sein, um mögliche Angriffe auf Benutzeraccounts zu erschweren.

Eingehende E-Mails sollten am Firewall oder am Mailserver auf Viren und andere schädliche Inhalte wie aktive Inhalte (z.B. Java-Applets) überprüft werden (vgl. auch SYS 8.5 „Firewalls und aktive Inhalte“).

Über Filterregeln können für bestimmte E-Mail-Adressen der Empfang oder die Weiterleitung von E-Mails gesperrt werden. Dies kann z.B. sinnvoll sein, um sich vor Spam-Mail zu schützen. Auch über die Filterung anderer Header-Einträge kann versucht werden, Spam auszugrenzen. Hierbei muss mit Bedacht vorgegangen werden, damit der Filterung keine erwünschten E-Mails zum Opfer fallen. Daher sollten entsprechende Filterregeln sehr genau definiert werden, indem beispielsweise aus jeder Spam-Mail eine neue dedizierte Filterregel abgeleitet wird. Entsprechende Filterlisten sind im Internet verfügbar bzw. können von verschiedenen Herstellern der Kommunikationssoftware bezogen werden.

Es ist festzulegen, welche Protokolle und Dienste am Mailserver erlaubt sind.

Ein Mailserver sollte davor geschützt werden, als Spam-Relay verwendet zu werden. Dafür sollte ein Mailserver so konfiguriert werden, dass er E-Mails nur für die Organisation selber entgegennimmt und nur E-Mails verschickt, die von Mitarbeiterinnen/Mitarbeitern der Organisation stammen.

Wenn eine Organisation keinen eigenen Mailserver betreibt, sondern über einen oder mehrere Mailclients direkt auf den Mailserver eines Providers zugreift, muss mit dem Provider ein Dienstleistervertrag im Sinne des §11 Datenschutzgesetz (DSG 2000), BGBl. I Nr. 165/1999 i.d.g.F. abgeschlossen werden.

Für Organisationen der öffentlichen Verwaltung, welche einen eigenen Mailserver unterhalten, ist zusätzlich die auf Basis des IKT-Board-Beschlusses [IKTB-170902-1] empfohlene E-Mail-Policy anzuwenden. Demnach sind auch Maßnahmen und Empfehlungen aus SYS 8.19 zu beachten.

SYS 8.10 Einrichtung eines Postmasters

Relevanz: Umsetzung/Wartung; Anwender/innen;

In größeren Organisationen sollte zum reibungslosen Ablauf des E-Mail-Dienstes ein “Postmaster” benannt werden.

Dieser nimmt folgende Aufgaben wahr:

- Bereitstellen der Maildienste auf lokaler Ebene,
- Pflege der Adresstabellen,
- Überprüfung, ob die externen Kommunikationsverbindungen funktionieren,
- Überprüfung der Attachments auf Viren,

- Setzen von Maßnahmen, falls ein Virus gefunden wurde (Verhinderung einer Weiterleitung, Ablage in speziellen Quarantänebereichen, Verständigung der betroffenen Benutzer/innen, ...)
- Überprüfung, ob der gesamte Inhalt einer E-Mail einem gültigen Dokumentformat genügt (als Grundlage können hier die Richtlinien über Dokumentenaustauschformate (s. [KIT T05] bzw. für die betreffende Organisation oder für ein IT-System speziell erstellte Richtlinien gelten),
- Setzen von Maßnahmen, wenn der Inhalt einer E-Mail (zur Gänze oder teilweise) nicht einem gültigen Dokumentenaustauschformat entspricht (etwa Blocken der Nachricht, Verständigung des/der Absenders/Absenderin bzw. Empfängers/Empfängerin, Speicherung in einem Zwischenbereich, automatische Löschung nach einer vorgegebenen Zeitspanne, ev. Freigabe durch Sicherheitsbeauftragte nach Rücksprache und Begründung),
- Anlaufstelle bei Mailproblemen für Endbenutzer/innen sowie für die Betreiber von Gateway- und Relaydiensten.

Alle unzustellbaren E-Mails und alle Fehlermeldungen müssen an Postmaster weitergeleitet werden, die versuchen sollten, die Fehlerquellen zu beheben. E-Mail, die unzustellbar bleibt, muss nach Ablauf einer vordefinierten Frist vernichtet werden, der/die Absender/in ist mittels einer entsprechenden Fehlermeldung zu informieren.

Zuständige Betreuer/innen (ev. Hotline oder Helpdesk) sollten jederzeit von den Benutzerinnen/Benutzern telefonisch erreicht werden könnten.

SYS 8.11 Sichere Konfiguration der Mailclients

Relevanz: Umsetzung/Wartung; Anwender/innen;

Die E-Mail-Progamme der Benutzer/innen müssen durch den Administrator so vorkonfiguriert sein, dass ohne weiteres Zutun der Benutzer/innen maximale Sicherheit erreicht werden kann. Die Benutzer/innen sind darauf hinzuweisen, dass sie die Konfiguration nicht selbsttätig ändern dürfen.

Insbesondere sollten bei der Konfiguration der E-Mail-Clients folgende Punkte berücksichtigt werden:

- Das E-Mail-Passwort darf keinesfalls dauerhaft vom E-Mail-Programm gespeichert werden. Dabei wird das Passwort auf der Client-Festplatte abgelegt, u.U. sogar im Klartext oder nur schwach verschlüsselt. Jede/r, der Zugriff auf den Mailclient hat, hat so die Möglichkeit, unter fremdem Namen E-Mails zu verschicken bzw. das E-Mail-Passwort auszulesen.
- Als Reply-Adresse ist die E-Mail-Adresse der Benutzerin bzw. des Benutzers einzustellen, um sicherzustellen, dass keine internen E-Mail-Adressen weitergegeben werden.

Bei der Konfiguration von E-Mail-Clients kann auf produktbezogene und aktuelle von vertrauenswürdigen Stellen veröffentlichte Leitlinien zurückgegriffen werden (z.B. [NSA-ECC1]).

SYS 8.12 Festlegung einer WWW-Sicherheitsstrategie

Relevanz: Umsetzung/Wartung;

Vor der Nutzung von WWW-Diensten ist zunächst in einem Konzept darzustellen, welche Dienste genutzt und welche angeboten werden sollen. Hierbei ist die Absicherung eines WWW-Servers ebenso zu betrachten wie die der WWW-Clients und der Kommunikationsverbindungen zwischen diesen.

WWW-Server sind für Hacker/innen sehr attraktive Ziele, da einem erfolgreichen Angriff oft sehr große Publizität zuteil wird. Daher muss der Absicherung eines WWW-Servers ein hoher Stellenwert eingeräumt werden. Vor dem Einrichten eines WWW-Servers sollte in einer WWW-Sicherheitsstrategie beschrieben werden, welche Sicherheitsmaßnahmen in welchem Umfang umzusetzen sind. Anhand der in der WWW-Sicherheitsstrategie festgelegten Anforderungen kann dann regelmäßig überprüft werden, ob die getroffenen Maßnahmen ausreichend sind.

In der WWW-Sicherheitsstrategie muss neben einer Sicherheitsstrategie für den Betrieb eines WWW-Servers auch eine Sicherheitsstrategie für die WWW-Nutzung enthalten sein.

WWW-Sicherheitsstrategie für den Betrieb eines WWW-Servers

In der Sicherheitsstrategie für den Betrieb eines WWW-Servers sollten die folgenden Fragen beantwortet werden:

- Wer darf welche Informationen einstellen?
- Welche Randbedingungen sind beim Betrieb eines WWW-Servers zu beachten?
- Wie werden die Verantwortlichen geschult, insbesondere hinsichtlich möglicher Gefährdungen und einzuhaltender Sicherheitsmaßnahmen?
- Welche Dateien dürfen aufgrund ihres Inhaltes nicht auf dem WWW-Server eingestellt werden (z.B. weil die Inhalte vertraulich sind, nicht zur Veröffentlichung zulässig sind oder nicht der Firmen- bzw. Behördenpolitik entsprechen)?
- Welche Zugriffsbeschränkungen auf den WWW-Server sollen realisiert werden?

Teil einer Sicherheitsstrategie muss auch die regelmäßige Informationsbeschaffung über potentielle Sicherheitslücken sein, um rechtzeitig Vorsorge dagegen treffen zu können. Eine wichtige Informationsquelle für Sicherheitshinweise zur WWW-Nutzung stellt die “World Wide Web Security FAQ” (unter http://www.w3.org/Security/Faq/) dar.

WWW-Sicherheitsstrategie für die WWW-Nutzung

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

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

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

- Die Browser der Benutzer/innen müssen durch den Administrator so vorkonfiguriert sein, dass ohne weiteres Zutun der Benutzer/innen maximale Sicherheit erreicht werden kann (siehe auch SYS 8.14 Sicherheit von WWW-Browsern).
- Dateien, deren Inhalt Anstoß erregen könnte, dürfen weder auf WWW-Servern eingestellt noch nachgefragt werden. Es muss festgelegt werden, welche Inhalte als anstößig gelten.
- Nach dem Download von Dateien sind diese explizit auf Viren zu überprüfen, soweit dies nicht durch eine zentrale Überprüfung gewährleistet wird.

Alle Regelungen und Bedienungshinweise zur WWW-Nutzung sind schriftlich zu fixieren und sollten den Mitarbeiterinnen/Mitarbeitern jederzeit zur Verfügung stehen.

Die Benutzer/innen müssen vor der WWW-Nutzung geschult werden, sowohl in der Nutzung ihrer WWW-Browser als auch des Internets, um Fehlbedienungen zu vermeiden und die Einhaltung der organisationsinternen Richtlinien zu gewährleisten. Insbesondere müssen sie hinsichtlich möglicher Gefährdungen und einzuhaltender Sicherheitsmaßnahmen sensibilisiert werden.

SYS 8.13 Sicherer Betrieb eines WWW-Servers

Relevanz: Umsetzung/Wartung;

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

Daher sollte ein WWW-Server, der Informationen im Internet anbietet, entsprechend den folgenden Vorgaben installiert werden:

- Auf einem WWW-Server sollte nur ein Minimum an Programmen vorhanden sein, d.h. das Betriebssystem sollte auf die unbedingt erforderlichen Funktionalitäten reduziert werden und auch sonst sollten sich nur unbedingt benötigte Programme auf dem WWW-Server befinden.
- Ein WWW-Server sollte insbesondere keine unnötigen Netzdienste enthalten, verschiedene Dienste gehören auf verschiedene Rechner (beispielsweise ein WWW-Server und ein E-Mail-Server).
- Der Zugriff auf Dateien oder Verzeichnisse muss geschützt werden (siehe SYS 8.15 „Schutz der WWW-Dateien“).
- Die Kommunikation mit dem WWW-Server sollte durch einen Paketfilter auf ein Minimum beschränkt werden.
- Die Administration des WWW-Servers sollte nur über eine sichere Verbindung erfolgen, d.h. die Administration sollte direkt an der Konsole, nach starker Authentisierung (bei Zugriff aus dem LAN) oder über eine verschlüsselte Verbindung (bei Zugriff aus dem Internet) erfolgen.
- Weiterhin sollte der WWW-Server vor dem Internet durch einen Firewall-Proxy oder aber zumindest durch einen Paketfilter abgesichert werden. Er darf sich nicht zwischen Firewall und internem Netz befinden, da ein Fehler auf dem WWW-Server sonst Zugriffe auf interne Daten ermöglichen könnte.

Je nach Art des WWW-Servers bieten sich unterschiedliche Möglichkeiten zum Schutz an. Allen diesen Möglichkeiten gemeinsam ist allerdings, dass der eigentliche Serverprozess des WWW-Servers, nämlich der http-Daemon, nur mit eingeschränkten Rechten ausgestattet sein sollte. Er muss üblicherweise mit root-Privilegien gestartet werden, sollte aber nach dem Start so schnell wie möglich mit den Rechten einer/eines weniger privilegierten neuen Benutzerin/Benutzers weiterarbeiten. Hierfür sollte ein eigener Benutzeraccount wie *wwwserver* eingerichtet werden. Wichtig ist, dass diese/r Benutzer/in keine Schreibrechte auf die Protokolldateien besitzt. Ein/e Angreifer/in könnte sonst durch Ausnutzung eines Fehlers diese mit den Rechten des HTTP-Servers manipulieren.

Für die verschiedensten Server-Produkte sind teilweise detaillierte Leitlinien zu deren sicheren Konfiguration verfügbar (vgl. z.B. [NSA-SD2], [NSA-SD3], [NSA-SD4], [NSA-SD5] u.ä.).

SYS 8.14 Sicherheit von WWW-Browsern

Relevanz: Umsetzung/Wartung; Anwender/innen;

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

Ursachen dafür können sein:

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

Eine Gefährdung der lokalen Daten geht beispielsweise von Programmen aus, die aus dem Internet geladen werden und ohne Nachfrage auf dem lokalen Rechner ausgeführt werden (z.B. ActiveX-Programme, Java-Applets o.ä., vgl. SYS 8.5 Firewalls und aktive Inhalte). Auch innerhalb von Dokumenten oder Bildern können Befehle enthalten sein, die automatisch beim Betrachten ausgeführt werden und zu Schäden führen können (z.B. Makro-Viren in Winword- oder Excel-Dokumenten). Um solche Probleme zu vermeiden, sollten die im Folgenden beschriebenen Maßnahmen umgesetzt werden. Darüber hinaus kann es auch sinnvoll sein, produktspezifische Konfigurationsleitlinien zu verwenden (z.B. [NSA-SD8], [NSA-SD10], etc.).

Laden von Dateien und/oder Programmen:

Beim Laden von Dateien und/oder Programmen können eine Vielzahl von Sicherheitsproblemen auftreten, die bekanntesten sind sicherlich Viren, Makro-Viren und trojanische Pferde. Die Benutzer/innen dürfen sich nie darauf verlassen, dass die geladenen Dateien oder Programme aus vertrauenswürdigen Quellen stammen.

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

Aktuelle Virenschutzprogramme sollten auf *allen* Rechnern mit Internetzugang installiert sein und automatisch ausgeführt werden.

Alle Benutzer/innen müssen darauf hingewiesen werden, dass sie selber dafür verantwortlich sind, beim Dateiladen alle entsprechenden Vorsichtsmaßnahmen zu ergreifen. Selbst wenn über die Firewall automatisch die geladenen Informationen auf Viren überprüft werden, bleiben die Benutzer/innen verantwortlich für die Schadensfreiheit von geladenen Dateien oder Programmen. Grundsätzlich müssen bei der Installation von Programmen natürlich die organisationsinternen Sicherheitsregeln beachtet werden. Insbesondere dürfen nur getestete und zugelassene Programme installiert werden (vgl. dazu auch ENT 1.7 „Abnahme und Freigabe von Software“, ENT 1.8 „Installation und Konfiguration von Software“ und SYS 3.1 „Nutzungsverbot nicht-freigegebener Software“). Vor der Installation sollten auf Stand-alone-Rechnern Tests auf die Schadensfreiheit der Programme durchgeführt werden. In Zweifelsfällen ist die IT-Administration hinzuzuziehen.

Plug-Ins und Zusatzprogramme

Nicht alle Browser können alle Dateiformate direkt verarbeiten, d.h. im Allgemeinen anzeigen, in manchen Fällen auch abspielen. Bei einigen Dateiformaten werden zusätzlich noch Plug-Ins bzw. Zusatzprogramme benötigt.

Bei Plug-Ins handelt es sich um Bibliotheksdateien (z.B. DLL-Dateien), die von Installationsprogrammen ins Plug-In-Verzeichnis geladen werden und bei Aufruf des entsprechenden Dateiformates vom Browser ausgeführt werden.

Zusatzprogramme, z.B. Viewer, sind eigenständige Programme, die in der Lage sind, bestimmte Dateiformate zu verarbeiten. Der Aufruf eines solchen Zusatzprogramms wird über eine Konfigurationsdatei des Browsers gesteuert, in der Dateiendung und Programm verknüpft sind. Bei Viewern von Office-Dokumenten sollte darauf geachtet werden, dass diese keine Makro-Befehle ausführen können („Schutz vor Makro-Viren“, vgl. SYS 4.6).

Beim Hinzufügen von Plug-Ins bzw. Zusatzprogrammen für einen WWW-Browser sind dieselben Vorsichtsmaßnahmen wie beim Laden von Dateien und/oder Programmen zu beachten. Es dürfen keine Programme installiert werden, denen man nicht unbedingt vertrauen kann.

Plug-Ins verbrauchen natürlich auch Speicherplatz und verlängern die Startzeit des Browsers. Daher sollten alle nicht benötigten Plug-Ins entfernt werden. Das ist nicht immer einfach: Viele Deinstallationsroutinen erkennen Plug-Ins nicht und nicht alle Browser bieten eine Übersicht über die installierten Plug-Ins. Dann müssen alle zu einem Plug-In gehörenden Dateien im Plug-In-Verzeichnis des Browsers manuell gelöscht werden.

Cookies:

In so genannten Cookie-Dateien werden auf dem Rechner der Benutzerin bzw. des Benutzers Informationen über abgerufene WWW-Seiten, Passwörter und Benutzerverhalten gespeichert. Damit können WWW-Anbieter beim nächsten Besuch der/des jeweiligen Benutzerin/Benutzers spezielle Informationen für diese/n anbieten oder dieser/diesem passwortgesichert nur bestimmte Dienste zugänglich machen. Allerdings kann ein WWW-Anbieter hiermit auch Benutzerprofile erstellen, z.B. für zielgruppenorientierte Werbung.

Um dies zu verhindern, sollte das Anlegen von Cookie-Dateien verhindert werden oder, wo das nicht möglich ist, diese regelmäßig gelöscht werden. Cookies finden sich meist im Konfigurationsverzeichnis des benutzten WWW-Browsers in Dateien wie *cookie.txt* oder Verzeichnissen wie *cookies*. Es sollten vorzugsweise Browser eingesetzt werden, mit denen sich das Anlegen von Cookies verhindern lässt. Wo dies nicht möglich ist, sollten zumindest solche Browser eingesetzt werden, die die Benutzer/innen vor der Annahme von Cookies warnen. Diese Option muss immer aktiviert werden. Lassen sich die Benutzer/innen vor der Annahme von Cookies warnen, bekommen sie mit der Warnung auch den zu erwartenden Inhalt des Cookies angezeigt, so dass damit auch transparent wird, welche Anbieter welche Informationen über die Benutzer/innen sammeln.

Um das Anlegen von Cookie-Dateien zu verhindern, kann auch eine leere Cookie-Datei angelegt werden und mit einem Schreibschutz versehen werden. Inwieweit dies effektiv ist, hängt vom eingesetzten Betriebssystem und der Browser-Variante ab. Hier ist insbesondere zu überprüfen, ob der Browser weder den Schreibschutz zurücksetzen kann noch dadurch einen Absturz verursacht.

Ansonsten kann es hilfreich sein, das regelmäßige Löschen der Cookies über eine Batch-Datei zu steuern, die beispielsweise bei jedem Systemstart oder jeder Benutzeranmeldung die alten Cookie-Dateien löscht.

Datensammlungen:

Nicht nur extern werden Daten über die Internetnutzung der verschiedenen Benutzer/innen gesammelt, sondern auch lokal. Auch hier muss sichergestellt werden, dass nur Befugte darauf Zugriff haben können. Dies gilt insbesondere auch für die von Browsern angelegten Dateien über History, Hotlists und Cache. Die Benutzer/innen müssen informiert werden, wo auf ihren lokalen Rechnern solche Daten gespeichert werden und wie sie diese löschen können.

Diese Dateien sind auf Proxy-Servern besonders sensibel, da auf einem Proxy-Server alle externen WWW-Zugriffe aller Mitarbeiter/innen protokolliert werden, inklusive der IP-Nummer des Clients, der die Anfrage gestartet hat, und der nachgefragten URL. Ein schlecht administrierter Proxy-Server kann daher massive Datenschutz-Verletzungen nach sich ziehen.

Von den meisten Browsern werden viele Informationen über den/die Benutzer/innen und sein/ihr Nutzerverhalten gesammelt, von denen diese/r einerseits vielleicht nicht will, dass sie weitergegeben werden, und die anderseits in ihrer Masse den verfügbaren Speicherplatz mit überflüssigen Informationen blockieren. Zu diesen Informationen gehören:

- Favoriten,
- abgerufene WWW-Seiten,
- Newsserver Visiten (s.u.),
- History Datenbank (s.u.),
- URL Liste (Liste der letzten aufgerufenen URLs),
- Cookie Liste,
- Informationen über Benutzer/innen, die im Browser gespeichert und evtl. auch weitergegeben werden (s.u.),
- Informationen im Cache (s.u.).

Informationen über Newsserver Visiten:

Aus den meisten Browsern heraus kann direkt auf Newsserver zugegriffen werden. Damit kann für ein Benutzerprofil festgestellt werden, welche Newsgruppen und welche News ein/e Benutzer/in gelesen hat. Manche Browser speichern auch den vollständigen Inhalt aller gelesenen News.

History Datenbank:

History Datenbanken enthalten eine vollständige Sammlung über alle Aktivitäten, die mit einem Browser durchgeführt worden sind, d.h. Angaben über betrachtete Bilder, Adressen, evtl. betrachtete vertrauliche interne Dokumente etc..

Dadurch verbraucht die History Datenbank auch schnell sehr viel Speicherplatz und sollte regelmäßig aufgeräumt werden. Die Dateien der History Datenbank sollten nicht einfach gelöscht werden, sondern durch vorbereitete Kopien einer leeren History Datenbank ersetzt werden, da bestimmte Einträge erhalten bleiben müssen.

Informationen über Benutzer/innen:

In einem Browser werden auch diverse Informationen über Benutzer/innen gespeichert und evtl. auch weitergegeben, z.B. Realname, E-Mail-Adresse, Organisation. Um nicht mit Werbe-E-Mail überflutet zu werden, empfiehlt es sich, für die Browser-Benutzung einen Alias zu verwenden.

Informationen im Cache:

Viele Browser erzeugen in einem Cache-Verzeichnis große Mengen an Dateien, die den Text und die Bilder aller besichtigten Web-Seiten enthalten, seit der Cache das letzte Mal gelöscht wurde. Der Cache dient dazu, um das mehrfache Laden von Informationen einer Seite während einer Sitzung zu verhindern. Manche Browser löschen diese Daten, die in jeder weiteren Sitzung absolut nutzlos sind, allerdings nicht eigenständig, so dass sich in einem nicht regelmäßig gelöschten Cache schnell Dutzende Megabyte Datenmüll ansammeln. Aus diesen Daten lassen sich darüber hinaus auch Benutzerprofile erstellen. Daher sollte der Cache ebenso wie der Verlaufsordner regelmäßig gelöscht werden.

Wenn auf mit SSL gesicherte WWW-Seiten zugegriffen wird, kann dies unter anderem dazu dienen, sensible Informationen wie Kreditkartennummern verschlüsselt über das Internet zu übertragen. Daher sollten solche Seiten von vornherein nicht im Cache abgelegt werden. Im Internet Explorer kann dies beispielsweise unter *Ansicht/Optionen/Erweitert/Kryptografieeinstellungen* unter “Sichere Seiten nicht lokal speichern” deaktiviert werden.

Zugriff auf Client-Festplatte:

Bei einigen Browsern wird WWW-Servern die Möglichkeit gegeben, aktiv auf die Festplatte des Client zuzugreifen (ActiveX, Java).

Java- bzw. ActiveX-Programme werden über den Browser statt auf dem Server auf der Client-Seite ausgeführt. Dies führt aber zu einer Verlagerung des Sicherheitsrisikos vom Server auf den Client. Daher sind in Java und ActiveX verschiedene Sicherheitsmechanismen eingebaut, um einen möglichen Missbrauch zu verhindern, allerdings sind bereits mehrfach Sicherheitslücken gefunden worden.

Die Benutzung von Browsern, die Zugriffe auf Dateien des Client gestatten, birgt im Zusammenhang mit ActiveX und Java gewisse Sicherheitsrisiken. ActiveX erlaubt unter bestimmten Bedingungen die Nutzung lokaler Ressourcen. Bei Java ist ein solcher Zugriff ebenfalls möglich, jedoch nur wenn dem/der Anwender/in dies explizit gestattet. Das Sicherheitskonzept von ActiveX basiert darauf, dass der/die Anwender/in dem Anbieter und einer authentifizierten dritten Stelle im World Wide Web vertraut. Dieses Vertrauen ist problematisch, wenn Web-Seiten eines unbekannten oder eines neuen Anbieters aufgerufen werden.

Auf Grund der bestehenden Probleme mit ActiveX, Java und JavaScript sollten diese generell abgeschaltet werden. Falls die Benutzung von ActiveX, Java und JavaScript unbedingt notwendig ist, sollten diese nur auf Rechnern zugelassen sein, die gegenüber anderen internen Rechnern so abgeschottet sind, dass die Vertraulichkeit und Integrität sicherheitsrelevanter Daten nicht beeinträchtigt werden können.

Sicherheitslücken in den WWW-Browsern:

In den meisten Browsern sind bereits gravierende Sicherheitslücken gefunden worden. Es ist daher sehr wichtig, sich über neu bekannt gewordene Schwachstellen zu informieren und entsprechende Gegenmaßnahmen zu ergreifen.

Mögliche Gegenmaßnahmen sind das Einspielen von Patches zur Beseitigung bekannter Sicherheitslücken, der Einsatz neuer Versionen (Achtung: gerade in neuen Versionen können ev. neue, zunächst noch unbekannte Sicherheitsprobleme auftreten!), sowie zusätzliche organisatorische und administrative Maßnahmen.

Verschlüsselung:

Da im Internet alle Daten im Klartext übertragen werden, sollten sensible Daten nur verschlüsselt übertragen werden. Hierbei wäre es sinnvoll, wenn entsprechende Mechanismen schon in den unteren Schichten des Protokolls vorgesehen würden. Es ist zu überlegen, inwieweit zur sicheren Übertragung von Daten über das Internet neuere Protokolle wie IPSEC, HTTPS oder SSL eingesetzt werden können.

Neuere Browser unterstützen die Benutzung diverser Sicherheitsprotokolle, zumindest SSL sollte unterstützt werden.

Nutzung vorhandener Sicherheitsfunktionalitäten:

Die vorhandenen Sicherheitsfunktionalitäten der Browser (Rückfrage vor dem Ausführen von Programmen, Zugriff nur auf eingeschränkte Dateisysteme, keine Möglichkeit zum Verändern lokaler Daten) sollten auf jeden Fall genutzt werden.

Beim Surfen im Internet sollte die automatische Ausführung von Programmen verhindert werden (z.B. über die Option Disable Java) und nur bei vertrauenswürdigen Servern wieder eingeschaltet werden.

News-Reader und Mail-Clients bieten häufig die Möglichkeit, beliebige Daten im MIME-Format zu lesen. Auch in diesen Daten können Befehle enthalten sein, die zu einem automatischen Starten von Programmen auf dem lokalen Rechner führen. Die entsprechenden Möglichkeiten sollten daher in den Konfigurationsdateien entfernt werden bzw. nur nach Rückfrage gestartet werden können.

Regelungen:

Ein Großteil der oben beschriebenen Maßnahmen liegt im Verantwortungsbereich der Benutzer/innen, da deren Umsetzung wie beispielsweise die Aktivierung bestimmter Optionen nicht ständig durch die Systemadministration überprüft werden kann. Daher sollte jede/r Benutzer/in vor der Nutzung von Internet-Diensten durch entsprechende Anweisungen verpflichtet werden, die aufgeführten Sicherheitsrichtlinien zu beachten. Es empfiehlt sich vor der Zulassung von Benutzerinnen/Benutzern zu Internet-Diensten, diese auf eine Benutzerordnung zu verpflichten. Die Inhalte der Internet-Sicherheitsrichtlinie und der Benutzerordnung sind den Benutzerinnen und Benutzern in einer Schulung darzulegen.

In dieser Benutzerordnung sollten die zur Verfügung stehenden Kommunikationsdienste kurz erläutert und alle relevanten Regelungen aufgeführt werden. Jede/r Benutzer/in sollte durch Unterschrift bestätigen, dass die dargestellten Regelungen zur Kenntnis genommen wurden und bei Benutzung der Kommunikationsdienste beachtet werden.

Es sollten alle Benutzer/innen darauf hingewiesen werden, dass die Nutzung von Internetdiensten mit nicht unerheblichen Kosten verbunden ist. Dementsprechend sollte darauf geachtet werden, im Internet gesammelte Informationen den anderen Mitarbeiterinnen und Mitarbeitern zur Verfügung zu stellen, um wiederholte Zugriffe auf dieselben externen WWW-Seiten zu vermeiden. Dafür sollte im internen Netz ein spezieller Bereich vorgesehen werden, in dem solche Informationen strukturiert abgelegt werden können.

Weiterhin müssen die Benutzer/innen darauf hingewiesen werden, dass

- die Konfiguration der WWW-Programme nicht eigenmächtig geändert werden darf,
- welche Daten protokolliert werden,
- wer die Ansprechpartner bei Sicherheitsproblemen sind.

SYS 8.15 Schutz der WWW-Dateien

Relevanz: Umsetzung/Wartung;

Die Dateien und Verzeichnisse auf einem WWW-Server müssen gegen unbefugte Veränderungen, aber auch u.U. - abhängig von den Sicherheitsanforderungen - gegen unbefugten Zugriff geschützt werden.

Generelle Aspekte

Falls Scripts über cgi-bin eingebunden werden, muss auf eine sichere Programmierung geachtet werden, um zu verhindern, dass diese Scripts zur Umgehung der Schutzmechanismen des Servers genutzt werden können.

Eine Möglichkeit, unbefugten Zugang zu erschweren, ist es, die Scripts unter einer Benutzer-ID auszuführen, die nur Zugang zu ausgewählten Dateien hat. Insbesondere ist es wichtig, die Konfigurationsdateien zu schützen, da sonst alle Zugangsrestriktionen leicht ausgeschaltet werden können.

Die Schreib- und Leserechte der WWW-Dateien sollten als lokale Dateien nur berechtigten Benutzerinnen/Benutzern Zugang erlauben.

Schutz vor unbefugten Veränderungen

Auf einem typischen WWW-Server ändern sich nur die Protokolldateien ständig, alle anderen Dateien sind statisch. Dies trifft insbesondere auf Systemprogramme und die WWW-Seiten zu. WWW-Seiten werden zwar regelmäßig aktualisiert, sollten aber nicht auf dem WWW-Server selber bearbeitet werden.

Um sicherzustellen, dass keine Dateien auf dem WWW-Server unbemerkt abgeändert werden können, sollten über alle statischen Dateien und Verzeichnisse Prüfsummen gebildet und regelmäßig überprüft werden. Um zu verhindern, dass WWW-Dateien überhaupt von Unbefugten geändert werden können, können statische Daten auf einem schreibgeschützten Speichermedium (z.B. CD-ROM oder Festplatte mit Schreibschutz) gespeichert werden.

Schutz vor unbefugtem Zugriff

Der Zugriff auf Dateien oder Verzeichnisse eines WWW-Servers ist zu schützen.

Diese können auf verschiedene Arten geschützt werden:

- Der Zugriff kann auf frei wählbare IP-Adressen, Teilnetze oder Domänen beschränkt werden.
- Es können benutzerspezifische Kennungen und Passwörter vergeben werden.
- Zugriffskontrolle wäre auch durch eine SSL-Verbindung mit clientseitigen Zertifikaten zur Authentifizierung möglich. Generelles zu Zertifikaten in der Öffentlichen Verwaltung siehe [IKTB-110903-3] und [IKTB-281003-19].
- Die Dateien können verschlüsselt abgelegt werden und die zugehörigen kryptographischen Schlüssel werden nur dem Zielpublikum bekannt gegeben.

SYS 8.16 Geeignete Auswahl eines Internet Service Providers

Relevanz: Management; Umsetzung/Wartung;

Bei einem Provider, über den ein/e Benutzer/in an das Internet angeschlossen ist, fallen nicht nur Informationen über ein- und ausgehende E-Mail an, sondern auch über alle WWW-Seiten, die die Benutzer/innen aufrufen. Außerdem laufen alle Daten, die zwischen dem Rechner der Benutzer/innen und einem Server im Internet ausgetauscht werden, über die IT-Systeme des Providers.

Bei der Auswahl eines Internet Service Providers sollte hinterfragt werden,

- ob Ansprechpartner/innen zu technischen Problemen rund um die Uhr zur Verfügung stehen und wie kompetent diese sind,
- wie er auf den Ausfall einer oder mehrerer seiner IT-Systeme vorbereitet ist (Notfallplanung, Datensicherungskonzept),
- welche Verfügbarkeit (maximale Ausfallzeit) er garantieren kann,
- ob er regelmäßig überprüft, ob die Verbindungen zum Kunden noch stabil sind und im negativen Fall entsprechende Schritte unternimmt,
- was er zur Absicherung seiner IT-Systeme und der seiner Kunden unternimmt.

Man sollte sich vom Provider dokumentieren lassen, dass dessen IT-Systeme sicher betrieben werden, also z.B. die in SYS 8.13 „Sicherer Betrieb eines WWW-Servers“ beschriebenen Anforderungen erfüllt sind. Bei jedem Provider sollten ein IT-Sicherheitskonzept und Sicherheitsrichtlinien selbstverständlich sein. Die Sicherheitsrichtlinien sollten für Externe einsehbar sein. Die Mitarbeiter/innen des Providers sollten für IT-Sicherheitsaspekte sensibilisiert sein, auf die Einhaltung der Sicherheitsrichtlinie verpflichtet worden sein und regelmäßig geschult werden (nicht nur in Sicherheitsfragen).

Beim Provider sind Daten über die Benutzer/innen für Abrechnungszwecke gespeichert (Name, Adresse, Benutzerkennung, Bankverbindung) ebenso wie Verbindungsdaten und für eine je nach Provider kürzere oder längere Zeitspanne auch die übertragenen Inhalte. Die Anwender/innen sollten sich bei ihrem Provider erkundigen, welche Daten wie lange über sie gespeichert werden. Bei der Auswahl von Providern sollte berücksichtigt werden, dass österreichische Betreiber den einschlägigen datenschutzrechtlichen Regelungen für die Verarbeitung dieser Daten unterliegen.

SYS 8.17 Einsatz von Verschlüsselungsverfahren zur Netzkommunikation

Relevanz: Umsetzung/Wartung;

Kommunikationsnetze transportieren Daten zwischen IT-Systemen. Dabei werden die Daten selten über eine dedizierte Kommunikationsleitung zwischen den an der Kommunikation beteiligten Partnern übertragen. Vielmehr werden die Daten über viele Zwischenstationen geleitet. Je nach Kommunikationsmedium und verwendeter Technik können die Daten von den Zwischenstationen unberechtigt abgehört werden, oder auch von im jeweiligen Vermittlungsnetz angesiedelten Dritten (z.B. bei der Verwendung des Ethernetprotokolls ohne Punkt-zu-Punkt-Vernetzung). Da die zu übertragenden Daten nicht von unberechtigten Dritten abgehört, verändert oder zur späteren Wiedereinspeisung in das Netz (Replay-Attacke) benutzt werden sollen, muss ein geeigneter Mechanismus eingesetzt werden, der dies verhindert. Verschlüsselung der Daten mit - wenn nötig - gegenseitiger Authentifizierung der Kommunikationspartner kann diese Gefahr (je nach Stärke des gewählten Verschlüsselungsverfahrens sowie der Sicherheit der verwendeten Schlüssel) reduzieren.

In der Regel kommunizieren Anwendungen miteinander, um anwendungsbezogene Informationen auszutauschen. Die Verschlüsselung der Daten kann nun auf mehreren Ebenen erfolgen:

- *Auf Applikationsebene:*
  Die kommunizierenden Applikationen müssen dabei jeweils über die entsprechenden Ver- und Entschlüsselungsmechanismen verfügen.
- *Auf Betriebssystemebene:*
  Die Verschlüsselung wird vom lokalen Betriebssystem durchgeführt. Jegliche Kommunikation über das Netz wird automatisch oder auf Anforderung verschlüsselt.
- *Auf Netzkoppelelementebene:*
  Die Verschlüsselung findet zwischen den Netzkoppelelementen (z.B. Router) statt.

Die einzelnen Mechanismen besitzen spezifische Vor- und Nachteile. Die Verschlüsselung auf Applikationsebene hat den Vorteil, dass die Verschlüsselung vollständig der Kontrolle der jeweiligen Applikation unterliegt. Ein Nachteil ist, dass zur verschlüsselten Kommunikation nur eine mit demselben Verschlüsselungsmechanismus ausgestattete Partnerapplikation in Frage kommt. Weiterhin können entsprechende Authentifizierungsmechanismen zwischen den beiden Partnerapplikationen zur Anwendung kommen.

Im Gegensatz dazu findet die Verschlüsselung im Fall der Verschlüsselung auf Betriebssystemebene transparent für jede Applikation statt. Jede Applikation kann mit jeder anderen Applikation verschlüsselt kommunizieren, sofern das Betriebssystem, unter dem die Partnerapplikation abläuft, über den Verschlüsselungsmechanismus verfügt. Nachteilig wirkt sich hier aus, dass bei einer Authentifizierung lediglich die Rechner gegenseitig authentifiziert werden können, und nicht die jeweiligen Partnerapplikationen.

Der Einsatz von verschlüsselnden Netzkoppelelementen besitzt den Vorteil, dass applikations- und rechnerseitig keine Verschlüsselungsmechanismen vorhanden sein müssen. Die Verschlüsselung ist auch hier transparent für die Kommunikationspartner, allerdings findet die Kommunikation auf der Strecke bis zum ersten verschlüsselnden Netzkoppelelement unverschlüsselt statt und birgt damit ein Restrisiko. Authentifizierung ist hier nur zwischen den Koppelelementen möglich. Die eigentlichen Kommunikationspartner werden hier nicht authentifiziert.

Werden sensitive Daten über ein Netz (auch innerhalb des Intranets) übertragen, empfiehlt sich der Einsatz von Verschlüsselungsmechanismen. Bieten die eingesetzten Applikationen keinen eigenen Verschlüsselungsmechanismus an oder wird das angebotene Verfahren als zu schwach eingestuft, so sollte von der Möglichkeit der betriebssystemseitigen Verschlüsselung Gebrauch gemacht werden. Hier bieten sich z.B. Verfahren wie SSL an, die zur transparenten Verschlüsselung auf Betriebssystemebene entworfen wurden. Je nach Sicherheitspolitik können auch verschlüsselnde Netzkoppelelemente eingesetzt werden, etwa um ein virtuelles privates Netz (VPN) mit einem Kommunikationspartner über das Internet zu realisieren. Entsprechende Softwaremechanismen sind in der Regel auch in Firewall-Systemen verfügbar.

Erfolgt der Zugang auf sensible Daten über einen externen Zugang, so sind kryptographische Einmalverfahren mit einer Besitzkomponente einzusetzen. Wegen der einheitlichen Administrierbarkeit wird empfohlen für den Zugang die Bürgerkarte/Dienstkarte und MOA-ID zu verwenden [IKTB-140605-01].

Beim Einsatz von verschlüsselter Kommunikation und gegenseitiger Authentifizierung sind umfangreiche Planungen im Rahmen der Sicherheitspolitik eines Unternehmens bzw. einer Behörde nötig. Im Rahmen der hier angesprochenen Kommunikationsverschlüsselungen sind insbesondere folgende Punkte zu beachten:

- Welche Verfahren sollen zur Verschlüsselung benutzt werden bzw. werden angeboten (z.B. in Routern)?
- Unterstützen/Nutzen die eingesetzten Verschlüsselungsmechanismen existierende oder geplante Standards (IPSec, IPv6, IKE; SSL, TLS); vergleiche dazu auch SYS 8.19 zu Zugang zu E-Mail.
- Sind gemäß der Sicherheitspolitik ausreichend starke Verfahren und entsprechend lange Schlüssel gewählt worden?
- Werden die Schlüssel sicher aufbewahrt?
- Werden die Schlüssel in einer sicheren Umgebung erzeugt, und gelangen sie auf sicherem Weg zum notwendigen Einsatzpunkt (Rechner, Softwarekomponente)?
- Sind Schlüssel-Recovery-Mechanismen nötig?

Ähnliche Fragestellungen sind bei der Nutzung von Zertifikaten zur Authentifizierung von Kommunikationspartnern zu beachten.

Im Bereich der öffentlichen Verwaltung sind außerdem bezüglich der Verschlüsselung des E-Mail-Verkehrs entsprechende Vorgaben, wie etwa die Vorgabe der Eigenschaften von Verschlüsselungszertifikaten gemäß des IKT-Board-Beschlusses [IKTB-181202-1] zu beachten.

SYS 8.18 Einsatz von Stand-alone-Systemen zur Nutzung des Internets

Relevanz: Umsetzung/Wartung;

Um die Gefährdungen, die durch Angriffe aus dem Internet auf lokale Daten oder Rechner im LAN entstehen, zu verringern, ist es sinnvoll Rechner einzusetzen, die nur mit dem Internet vernetzt sind und keine weitere Netzverbindung zu einem LAN haben.

Hierfür bieten die verschiedenen Betriebssysteme unterschiedliche Möglichkeiten mit jeweils spezifischen Gefährdungen für die Vertraulichkeit und Integrität der Daten auf diesem Rechner.

Wichtig ist es zu beachten, dass bei der Installation der Internet-Zugangssoftware keine unnötigen Programme installiert werden. So gibt es bei einigen Produkten und Betriebssystemen die Möglichkeiten, durch die Installation von Server-Programmen den Rechner zu einem vollständigen Internet-Server zu machen. Die Installation der TCP/IP-Software bietet eine vollständige bidirektionale Verbindung zum Internet, über die Daten sowohl ins Internet geschickt als auch von dort abgeholt werden können.

SYS 8.19 Geeignete Auswahl eines E-Mail-Clients/Server

Relevanz: Umsetzung/Wartung;

Gemäß den Vorgaben der E-Mail-Strategie des Bundes müssen E-Mail-Programme (E-Mail-Clients und E-Mail-Server) unter dem Gesichtspunkt offener internationaler Standards gewählt werden.

Die durch den IKT-Board-Beschluss [IKTB-170902-1] für die Organisationen der öffentlichen Verwaltung empfohlene E-Mail-Policy schreibt dabei die Einhaltung der folgenden Mindesteigenschaften vor:

- *Kommunikation:*
  Für die Kommunikation zwischen Clients und Servern im E-Mailverkehr sowie für die Kommunikation zwischen E-Mail-Servern selbst sind folgende Protokolle festgelegt: POP3 [RFC1939], IMAP [RFC 2060], SMTP [RFC 2821]
- *Adress-Verwaltung:*
  Die Verwaltung von E-Mail-Adressen und Attributen erfolgt in Verzeichnisdiensten. Eine komfortable Umsetzung erfordert, dass die eingesetzten Clients und Server entsprechende Interfaces zu diesen Verzeichnisdiensten aufweisen. Dafür wird folgender Standard im Rahmen der E-Mail-Policy für die öffentliche Verwaltung vorgeschrieben: LDAP V3 [RFC 2251]
- *Sicherheit:*
  Für die E-Mail-Sicherheit ist S/MIME V3 einzusetzen. Die Verschlüsselungen und Signaturen müssen jedenfalls CMS kompatibel sein. Die dabei eingesetzten Schlüssellängen der symmetrischen Schlüsselkomponenten müssen mindestens 100 Bit betragen. Für die Signatur von Attachments sind als Signaturformate PKCS#7 oder XML zu verwenden. PGP kann für die Vertraulichkeit in einer Übergangszeit in manchen Bereichen notwendig bleiben. Für die öffentliche Verwaltung ist die “Richtlinie für E-Mail Zertifikate in der Verwaltung” [IKT-MZERT] zu beachten [IKTB-230903-17].

- *Zugang von Außen:*
  Der uneingeschränkte Zugang von außen ist nur über eine geeignete Verschlüsselung einzurichten (z.B. VPN oder IPSEC), die auch die End-To-End Authentifizierung sicherstellt. Mailzugänge über Web-Interfaces müssen zumindest verschlüsselt sein (Standard SSL bzw. TLS oder IPSEC mit einer Schlüssellänge von mindestens 100 Bit). Darüber hinaus gilt es die existierende WEBMAIL-Policy (sowie vorhandene Checklisten) zu beachten. Derartige Anforderungen werden im Detail in der für Organisationen der öffentlichen Verwaltung zu beachtenden E-Mail-Policy des Chief Information Office des Bundes behandelt. Im Bereich der öffentlichen Verwaltung ist für den externen E-Mail-Zugang auch der IKT-Board Beschluss [IKTB-110903-8] zu berücksichtigen, in dem die Verwendung der Bürgerkarte zur Identifikation und Authentifikation empfohlen wird.
- *Nachweis der Standardkonformität:*
  Für die Bereiche der öffentlichen Verwaltung wird ein Testmailservice angeboten. Dieses dient zur Kompatibilitätsfeststellung der eingesetzten Systeme sowohl nach innen als auch nach außen. Damit kann der Nachweis der Konformität der Systeme mit den geforderten Standards und der Einhaltung der Mindestantwortzeiten erbracht werden.

Für weitere detaillierte Vorschriften, die für die Organisationen der öffentlichen Verwaltung gemäß dem IKT-Board-Beschluss [IKTB-170902-1] anwendbar sind, sei auf die entsprechenden Kapitel der “Internet Policy” [IKT-IPOL], sowie auf die “E-Mail-Policy” [IKT-MPOL] der Stabsstelle IKT-Strategie des Bundes (CIO) verwiesen.

SYS 8.20 Portalverbundsystem in der öffentlichen Verwaltung

Relevanz: Umsetzung/Wartung;

Der Portalverbund ist ein Zusammenschluss von Verwaltungsportalen zur gemeinsamen Nutzung der bestehenden Infrastruktur. Der Vorteil eines Portals ist, dass mehrere Anwendungen über einen Punkt zugänglich sind.

Portale zwischen den Verwaltungen bilden die technische Basis für das zentrale Melderegister, für EKIS und für eine Reihe weiterer wichtiger Anwendungen verschiedener Ressorts. Im Portalverbund wird durch - mit einheitlichen Attributen versehene - Zertifikate die Sicherheit einerseits aber auch die Offenheit gegenüber dem Markt andererseits erreicht.

Seitens der Arbeitsgruppe (Bund / Länder) wurde ein Protokoll (Spezifikation Portal Verbund Protokoll PVP 1.5.1 [IKT-PVP]) und eine Struktur (Spezifikation LDAP-gv.at 2.0.1 [IKT-LDAP]) zum Portalverbund vorgeschlagen. Diese wurde im Rahmen des IKT-Board Beschlüsse [IKTB-040402-3] und [IKTB-051102-1] zur Verwendung in der öffentlichen Verwaltung empfohlen. Seitens des IKT-Boards werden zusätzliche Anmerkungen zur Verständlichkeit angefügt:

- Soweit symmetrische Schlüssel angewendet werden, sind die Schlüssellängen mit mindestens 100 BIT zu wählen.
- Für die Zertifikate von Server und Client sind Zertifizierungsdienste zu verwenden, deren Sicherheitsvorgaben nach österreichischer Rechtslage wirksam sind.
- Generell haben sich Portale, die an andere Portale koppeln, dies mit Client-Identifikation via Zertifikat durchzuführen.
- Diese Portalstruktur ist für Organwalter und gesetzliche Vertretungen für den jeweils eigenen Wirkungsbereich - nicht jedoch für Bürger/innen anwendbar.

- Bei der Umsetzung von Anwendungsportalen ist darauf zu achten, dass diese das Portalverbundprotokoll unterstützen. Die Benutzer/innen sind dabei entsprechend der Organisations-Zugehörigkeit zu erfassen [IKTB-240304-01].
- Bei Zugriff auf Verwaltungsanwendungen (z.B. SAP und ESS) ist auf die entsprechende Sicherheitsklasse des Zugangs zu achten [IKTB-270705-01].
- Weitere Portalkopplungsstrukturen werden nur nach vorheriger Abstimmung zwischen Bund, Ländern, Städten und Gemeinden eingesetzt.

Für die Signatur und die Identifikation wird empfohlen die Module für Sicherheitstechniken für Online Verfahren (MOA-ID, MOA-SS/SP) einzubinden. [IKTB-161203-01] Im Rahmen der Anwendungen des Bundes werden diese dann auch zur Sicherung der Konvergenz verwendet. Neben den Protokollen für den Portalverbund ist eine einheitliche Vorgehensweise in den Bereichen

- Verwendbare Verschlüsselungsverfahren
- Zertifikatsspezifikationen
- Keystoreformate und
- Zertifikatsmanagement

anzuwenden.

In Hinblick auf die Verwendung von Zertifikaten in der Öffentlichen Verwaltung werden besonders in den IKT-Board Beschlüssen [IKTB-110903-3] und [IKTB-281003-19] entsprechende Dokumente und Richtlinien beschlossen und zur Anwendung empfohlen (siehe dazu auch Richtlinien der IKT-Stabsstelle für Server-Zertifikate [IKT-SZERT]).

SYS 8.21 Richtlinien bei Verbindung mit Netzen Dritter (Extranet)

Relevanz: Umsetzung/Wartung;

Zunehmend werden die nach außen hin abgeschotteten und abgesicherten Netzwerke von Organisationen zu einem Verbund zusammengeschlossen (Extranet). Für diesen Schritt sind als Grundlage von allen Beteiligten einzuhaltende Richtlinien bzw. Vereinbarungen notwendig.

In einer derartigen Vereinbarung (sog. Data Connection Agreement – DCA) sollen detaillierte Angaben zu folgenden Punkten enthalten sein:

- Bestimmung der Verantwortlichen
- Haftungs- und Schadensersatzregeln (z.B. auch bei Virenbefall, Hackerangriff, etc.)
- eventuell Non-Disclosure-Agreement (NDA)
- Festlegung der Datennutzung
- Benennung von Ansprechpartnerinnen/Ansprechpartnern (in technischen, organisatorischen und sicherheitstechnischen Belangen)
- welche Dienste werden zur Verfügung gestellt (z.B. ftp, http, etc.)
- welche Plattformen werden unterstützt
- Richtlinien zur Protokollierung (wer protokolliert was/wann und wie werden Protokolldaten ggf. ausgetauscht)
- welche Sicherheitsmaßnahmen müssen gewährleistet werden

- wie sind weitere Vertragspartner in die Vereinbarung einzubinden
- Regelung über das Vorgehen beim Auftreten von Sicherheitslücken (betrifft Informationspflicht, Vorgehen bei Netzwerktrennung, etc.)

Sicherheitslücken müssen von allen Beteiligten vor dem Netzzusammenschluss beseitigt werden. Dabei sind gegenseitige (stichprobenartige) Überprüfungen der vereinbarten und einzuhaltenden Sicherheitsmaßnahmen sinnvoll.

SYS 8.22 Sichere Nutzung von E-Commerce bzw. E-Government Applikationen

Relevanz: Umsetzung/Wartung;

E-Commerce und E-Government Anwendungen ergänzen zunehmend das Angebot im Internet. Beispielhafte Applikationen in diesem Sinne wären Online-Banking, Internet-Shopping oder das Angebot von Behörden wie etwa FINANZ-Online. Bei diesen Anwendungen sollte in der Regel ein hohes Maß an Sicherheit gewahrt werden.

Über generelle Empfehlungen hinaus (vgl. SYS 8.14 Sicherheit von WWW-Browsern), sind auch die folgenden Empfehlungen und Kriterien in diesem Zusammenhang zu beachten:

- Die Anwendung muss die Anforderungen an Datenschutz und Datensicherheit erfüllen.
- Clientseitig sind Virenschutzmaßnahmen zu treffen (vgl. Abschnitt 5.4).
- Im Falle notwendiger spezieller Software (z.B.: Online-Banking-Software) ist diese nur von vertrauenswürdigen Quellen zu beziehen und es ist auf dessen Aktualität (bzgl. Updates, sicherheitsrelevanter Patches, etc.) zu achten.
- Der für derartige Internet-Anwendungen genutzte Rechner sollte einem/einer festen Benutzer/in zugeordnet sein – öffentlich zugängliche Internet-PCs sollten dafür nicht herangezogen werden.
- Die Verwendung von verschlüsselten Verbindungen mittels SSL/TLS ist bei E-Commerce und E-Government Anwendungen immer vorauszusetzen (vgl. SYS 8.14). Zu diesem Thema veröffentlicht die Operative Unit des Chief Information Office ein Papier zur Kategorisierung von SSL/TLS-Verbindungen.
- Werden bei SSL/TLS Zertifikate zur Authentisierung des Servers verwendet, so ist auf deren Gültigkeit sowie auf die Übereinstimmungen zwischen Server und den Angaben im Zertifikat zu achten.
- Bei E-Government Anwendungen ist beim Server-Zertifikat auf die Verwaltungseigenschaft (vgl. “Richtlinien für Zertifikate für das E-Government (E-Government OID)” [IKT-ZERT]) und auf eine geeignete Zertifikatshierarchie zu achten [IKTB-110504-02].
- Um dem Missbrauch reservierter Domänen in abgewandelter Form vorzubeugen, wird empfohlen für Domänen mit Umlauten, diese in beiden Schreibweisen z.B. sowohl “ae” als auch “ä” einzurichten [IKTB-110504-01].
- Zur Verringerung der Länge der Signaturstrings ist die Verwendung von elliptischen Kurven anzuraten. Die MOA Dienste sind für diese Kurven vorbereitet [IKTB-110505-03].
- Für elektronische Bescheide wird das Bescheidschema empfohlen [IKTB-230904-01].

SYS 8.23 Verwendung von Web-Mail externer Anbietern

Relevanz: Umsetzung/Wartung; Anwender/innen;

Eine Vielzahl von externen Maildiensteanbietern stellen ihre Services oft kostenlos (evtl. in Verbindung mit Werbung) zur Verfügung. In diesem Zusammenhang wird der Zugang zu den E-Mail-Konten in der Regel via Web-Mail angeboten, bei dem der/die Anwender/in die E-Mail-Dienste ohne jegliche clientseitige Software sondern nur unter Verwendung des Browsers nutzen kann.

Die Anbieter derartiger Webmaildienste unterscheiden sich nicht nur hinsichtlich ggf. anfallender Kosten. Es ergeben sich auch Unterschiede bezüglich Mailbox-Größen, Verfügbarkeit, dem Einsatz von Spam-Filtern, usw. Diesbezüglich ist eine genaue Durchsicht der Allgemeinen Geschäftsbedingungen (AGB) des jeweiligen Anbieters vorzunehmen. Darüber hinaus sind die gebotenen Sicherheitsvorkehrungen zu beachten, wie etwa:

- ist es möglich, über eine verschlüsselte Verbindung (z.B. SSL/TLS) auf die Mailbox zuzugreifen
- können E-Mails elektronisch signiert und/oder verschlüsselt werden
- findet eine Identitätsprüfung von Neukunden statt
- wird der Service durch fachkundiges und sicherheitstechnisch geschultes Personal realisiert (Social Engineering Attacks: beispielsweise soll das Erfragen des Passwortes durch einen fingierten Anruf am Helpdesk nicht möglich sein)
- eine Virenprüfung der E-Mails sollte anbieterseitig gewährleistet sein
- Spam-Filter sollten zur Verfügung stehen

Bei der Verwendung von Web-Mail sollte der/die Anwender/in Folgendes beachten (vgl. auch SYS 8.19):

- Wahl eines geeigneten Passwortes (vgl. SYS 1.5)
- Zugriffe auf das Web-Mail-Konto dürfen nur über verschlüsselte Verbindungen erfolgen (SSL/TLS)
- trotz eines vorhandenen anbieterseitigen Virenschutzes sollten Attachments clientseitig auf Viren geprüft werden
- Beenden des Web-Mail-Dienstes nur über den vorgesehenen Ausstiegsmechanismus (Log-Out-Button, etc.)

5.9 Telearbeit

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

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

Es gibt unterschiedliche Formen von Telearbeit, wie z.B. Telearbeit in Telearbeitszentren, mobile Telearbeit sowie Telearbeit in der Wohnung des Arbeitnehmers bzw. der Arbeitsnehmerin. Bei der letzteren unterscheidet man zwischen ausschließlicher Teleheimarbeit und alternierender Telearbeit, d.h. der/die Arbeitnehmer/in arbeitet teilweise im Büro und teilweise zu Hause.

Dieses Kapitel konzentriert sich auf die Formen der Telearbeit, die teilweise oder ganz im häuslichen Umfeld durchgeführt werden. Es wird davon ausgegangen, dass zwischen dem Arbeitsplatz zu Hause und der Institution eine Telekommunikationsverbindung besteht, die den Austausch von Daten oder ggf. auch den Zugriff auf Daten in der Institution ermöglicht.

Die Maßnahmenempfehlungen dieses Kapitels umfassen vier Bereiche:

- die Organisation der Telearbeit,
- den Telearbeitsrechner der Telearbeiterin bzw. des Telearbeiters,
- die Kommunikationsverbindung zwischen Telearbeitsrechner und Institution und
- den Kommunikationsrechner der Institution zur Anbindung des Telearbeitsrechners.

Die in diesem Kapitel aufgeführten Maßnahmenempfehlungen konzentrieren sich auf zusätzliche Sicherheitsanforderungen, die sich aus einem Einsatz eines IT-Systems im Bereich der Telearbeit ergeben. Alle übrigen für dieses IT-System erforderlichen organisatorischen, personellen und technischen Sicherheitsmaßnahmen sind selbstverständlich ebenfalls vollinhaltlich zur Anwendung zu bringen.

SYS 9.1 Geeignete Einrichtung eines häuslichen Arbeitsplatzes

Relevanz: Umsetzung/Wartung; Anwender/innen;

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

Die Einrichtung sollte unter Berücksichtigung von Ergonomie, Sicherheit und Gesundheitsschutz ausgewählt werden. Aus dem Aspekt der Sicherheit entstehen insbesondere folgende zusätzliche Anforderungen:

- Sichtschutz des Monitors, falls er durch ein Fenster beobachtet werden könnte,
- Überspannungsschutz
- Bereitstellung versperrbarer Behältnisse zur Aufbewahrung von Datenträgern und Dokumenten

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

SYS 9.2 Regelungen für Telearbeit

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

Da es bisher kein "Telearbeitsgesetz" mit eigenständigen gesetzlichen Regelungen gibt, sollten wichtige Fragen entweder durch Kollektivverträge, Betriebsvereinbarungen oder zusätzlich zum Arbeitsvertrag getroffene individuelle Vereinbarungen zwischen Telearbeiter/innen und Arbeitgeber geklärt werden.

Insbesondere sollten folgende Punkte geregelt werden:

- Freiwilligkeit der Teilnahme an der Telearbeit,
- Mehrarbeit und Zuschläge,
- Aufwendungen für Fahrten zwischen Betrieb und häuslicher Wohnung,

- Aufwendungen z.B. für Strom und Heizung,
- Haftung (bei Diebstahl oder Beschädigung der IT, aber auch bei Arbeitsunfall oder Berufskrankheit),
- Beendigung der Telearbeit.

Am häuslichen Arbeitsplatz sollten dieselben Vorschriften und Richtlinien bezüglich der Gestaltung des Arbeitsplatzes (z.B. Einrichtung eines Bildschirmarbeitsplatzes) und der Arbeitsumgebung gelten wie in der Institution. Dies sollte in Absprache mit dem/der Telearbeiter/in durch den/die in der Institution Verantwortlichen für den Arbeitsschutz, dem/der Datenschutz-/IT-Sicherheitsbeauftragten sowie dem Betriebs- bzw. Personalrat und dem direkten Vorgesetzten der Telearbeiterin bzw. des Telearbeiters begutachtet werden können.

Im Sinne der IT-Sicherheit sollten zusätzlich folgende Punkte behandelt werden:

- *Arbeitszeitregelung:*
  Die Verteilung der Arbeitszeiten auf Tätigkeiten in der Institution und am häuslichen Arbeitsplatz muss geregelt sein und feste Zeiten der Erreichbarkeit am häuslichen Arbeitsplatz müssen festgelegt werden.
- *Reaktionszeiten:*
  Es sollte geregelt werden, in welchen Abständen aktuelle Informationen eingeholt werden (z.B. wie häufig E-Mails gelesen werden) und wie schnell darauf reagiert werden sollte.
- *Arbeitsmittel:*
  Es kann festgeschrieben werden, welche Arbeitsmittel Telearbeiter/innen einsetzen können und welche nicht genutzt werden dürfen (z.B. nicht freigegebene Software). So kann ein E-Mail-Anschluss zur Verfügung gestellt werden, aber die Nutzung von anderen Internet-Diensten wird untersagt. Weiters kann die Benutzung von Disketten (Gefahr von Viren) untersagt werden, wenn der Telearbeitsrechner dies nicht erfordert.
- *Datensicherung:*
  Der/die Telearbeiter/in ist zu verpflichten, regelmäßig eine Datensicherung durchzuführen. Darüber hinaus sollte vereinbart werden, dass jeweils eine Generation der Datensicherung bei der Institution zur Unterstützung der Verfügbarkeit hinterlegt wird.
- *IT-Sicherheitsmaßnahmen:*
  Der/die Telearbeiter/in ist zu verpflichten, die für die Telearbeit notwendigen IT-Sicherheitsmaßnahmen zu beachten und zu realisieren. Die umzusetzenden IT-Sicherheitsmaßnahmen sind dem/der Telearbeiter/in in schriftlicher Form zu übergeben.
- *Datenschutz:*
  Der/die Telearbeiter/in ist auf die Einhaltung einschlägiger Datenschutzvorschriften zu verpflichten sowie auf die notwendigen Maßnahmen bei der Bearbeitung von personenbezogenen Daten am häuslichen Arbeitsplatz hinzuweisen.
- *Datenkommunikation:*
  Es muss festgelegt werden, welche Daten auf welchem Weg übertragen bzw. welche Daten nicht oder nur verschlüsselt elektronisch übermittelt werden dürfen.
- *Transport von Dokumenten und Datenträgern:*
  Die Art und Absicherung des Transports zwischen häuslichem Arbeitsplatz und Institution ist zu regeln.
- *Meldewege:*
  Der/die Telearbeiter/in ist zu verpflichten, IT-sicherheitsrelevante Vorkommnisse unverzüglich an eine zu bestimmende Stelle in der Institution zu melden.

- *Zutrittsrecht zum häuslichen Arbeitsplatz:*
  Für die Durchführung von Kontrollen und für die Verfügbarkeit von Dokumenten und Daten im Vertretungsfall kann ein Zutrittsrecht zum häuslichen Arbeitsplatz (ggf. mit vorheriger Anmeldung) vereinbart werden.

Es empfiehlt sich, diese Regelungen schriftlich festzulegen und jedem/jeder Telearbeiter/in auszuhändigen. Entsprechende Merkblätter sind regelmäßig zu aktualisieren.

SYS 9.3 Regelung des Dokumenten- und Datenträgertransports zwischen häuslichem Arbeitsplatz und Institution

Relevanz: Umsetzung/Wartung; Anwender/innen;

Damit der Austausch von Dokumenten und Datenträgern zwischen häuslichem Arbeitsplatz und Institution sicher vollzogen werden kann, ist eine Regelung über Art und Weise des Austausches aufzustellen.

Darin sollten zumindest folgende Punkte betrachtet bzw. geregelt werden:

- welche Dokumente bzw. Datenträger über welchen Transportweg (Postweg, Kurier, Paketdienst, ...) ausgetauscht werden dürfen,
- welche Schutzmaßnahmen beim Transport zu beachten sind (beispielsweise Transport in geschlossenem Behälter, in Versandtasche, per Einschreiben, mit Begleitschreiben oder mit Versiegelung) und
- welche Dokumente bzw. Datenträger nur persönlich transportiert werden dürfen.

Da Schriftstücke oftmals Unikate sind, muss bei der Auswahl eines geeigneten Dokumentenaustauschverfahrens beachtet werden, welchen Schaden der Verlust bedeuten würde. Hingegen kann beim Datenträgeraustausch vorab eine Datensicherung erfolgen.

SYS 9.4 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger

Relevanz: Anwender/innen;

Dienstliche Unterlagen und Datenträger dürfen auch am häuslichen Arbeitsplatz nur dem/der autorisierten Mitarbeiter/in zugänglich sein. Aus diesem Grund muss ein verschließbarer Bereich (Schrank, Schreibtisch o.ä.) verfügbar sein. Die dienstlichen Unterlagen und Datenträger müssen außerhalb der Nutzungszeit darin verschlossen aufbewahrt werden. Die Schutzwirkung des abschließbaren Bereiches hat den Sicherheitsanforderungen der darin zu verwahrenden Unterlagen und Datenträger zu entsprechen.

Backup-Datenträger müssen im häuslichen Bereich verschlossen aufbewahrt werden. Es ist sicherzustellen, dass nur der/die Telearbeiter/in selber bzw. deren Vertretung darauf Zugriff hat. Jeweils eine Generation der Backup-Datenträger sollte jedoch in der Institution aufbewahrt werden, damit im Katastrophenfall der/dieVertreter/in auf die Backup-Datenträger zugreifen kann.

SYS 9.5 Betreuungs- und Wartungskonzept für Telearbeitsplätze

Relevanz: Umsetzung/Wartung; Anwender/innen;

Für die Telearbeitsplätze muss ein spezielles Betreuungs- und Wartungskonzept erstellt werden.

Dieses sollte folgende Punkte vorsehen:

- *Benennen von problembezogenen Ansprechpartnern für den Benutzerservice:*
  An diese Stelle wenden sich Telearbeiter/innen bei Software- und Hardwareproblemen. Der Benutzerservice versucht (auch telefonisch) kurzfristig Hilfestellung zu leisten bzw. leitet Wartungs- und Reparaturarbeiten ein.
- *Wartungstermine:*
  Die Termine für vor Ort durchzuführende Wartungsarbeiten sollten frühzeitig bekannt gegeben werden, damit die Telearbeiter/innen zu diesen Zeiten den Zutritt zum häuslichen Arbeitsplatz gewährleisten können.
- *Einführung von Standard-Telearbeitsrechnern:*
  Wenn möglich sollten alle Telearbeiter/innen einer Institution einen definierten Standard-Telearbeitsrechner haben. Dies verringert den konzeptionellen und administrativen Aufwand für den Aufbau eines sicheren Telearbeitsrechners und erleichtert Problemlösungen für den Benutzerservice.
- *Fernwartung:*
  Falls der Telearbeitsrechner über Fernwartung administriert und gewartet werden kann, sind die notwendigen Sicherheitsmaßnahmen sowie die erforderlichen Online-Zeiten zu vereinbaren. Insbesondere ist ein Sicherungsverfahren festzulegen, um den Missbrauch eines Fernwartungszugangs zu verhindern (vgl. BET 1.3 „Fernwartung“)
- *Transport der IT:*
  Es sollte aus Gründen der Haftung festgelegt werden, wer autorisiert ist, IT-Komponenten zwischen Institution und häuslichem Arbeitsplatz der Telearbeiterin bzw. des Telearbeiters zu transportieren.

SYS 9.6 Geregelte Nutzung der Kommunikationsmöglichkeiten

Relevanz: Umsetzung/Wartung; Anwender/innen;

Grundsätzlich verfügt ein Telearbeitsrechner über elektronische Kommunikationsmöglichkeiten. Im Sinne der IT-Sicherheit muss geregelt werden, auf welche Weise die vorhandenen Kommunikationsmöglichkeiten genutzt werden dürfen. Grundsätzlich sollte die private Nutzung der Kommunikationsmöglichkeiten untersagt werden.

Zu klären sind zumindest folgende Punkte:

- Datenflusskontrolle
  - Welche Dienste dürfen zur Datenübertragung genutzt werden?
  - Welche Dienste dürfen explizit nicht genutzt werden?
  - Welche Informationen dürfen an wen versendet werden?
  - Welcher Schriftverkehr darf über E-Mail abgewickelt werden?
  - Falls der Telearbeitsrechner ein Fax-Modem besitzt oder wenn am Telearbeitsplatz ein Faxgerät vorhanden ist, so ist zu klären, welche Informationen per Fax an wen übermittelt werden dürfen.
  - Der elektronische Versand welcher Informationen bedarf der vorherigen Zustimmung der Institution?
- Informationsgewinnung
  - Welche elektronischen Dienstleistungen (Datenbankabfragen, elektronische Recherchen) dürfen vom Telearbeitsrechner aus in Anspruch genommen werden? Beispielsweise können aus der Art der Abfragen u.U. Rückschlüsse auf Unternehmensstrategien gezogen werden.
  - Welches Budget steht für elektronische Dienstleistungen zur Verfügung?
- IT-Sicherheitsmaßnahmen
  - Für welche Daten sollen welche Verschlüsselungsverfahren eingesetzt werden?
  - Für welche Daten ist eine Löschung nach erfolgreicher Übertragung notwendig? Dies kann beispielsweise für personenbezogene Daten gelten.
  - Von welchen Daten soll trotz der erfolgreichen Übertragung eine Kopie der Daten auf dem Telearbeitsrechner verbleiben?
  - Wird vor Versand oder nach Erhalt von Daten ein Viren-Check der Daten durchgeführt?
  - Für welche Datenübertragung soll eine Protokollierung erfolgen? Falls eine automatische Protokollierung nicht möglich sein sollte, ist festzulegen, ob und in welchem Umfang eine handschriftliche Protokollierung vorzusehen ist.
- Internet-Nutzung
  - Wird die Nutzung von Internet-Diensten generell verboten?
  - Welche Art von Daten darf aus dem Internet geladen werden? Werden Daten von fremden Servern geladen, so besteht die Gefahr, dass Viren importiert werden.
  - Welche Optionen dürfen im Internet-Browser aktiviert werden?
  - Welche Sicherungsverfahren sollen im Internet-Browser aktiviert werden?
  - Ist die Zustimmung der Institution erforderlich, wenn der/die Telearbeiter/in sich am Informationsaustausch mittels Newsgruppen beteiligen will? Ggf. ist eine anonyme Nutzung erforderlich.
- Unterschriftenregelung
  - Ist eine Unterschriftenregelung für die Kommunikation vorgesehen?
  - Werden gesetzeskonforme elektronische Signaturen eingesetzt?
  - Werden andere Authentisierungsverfahren für den Schriftverkehr genutzt?

SYS 9.7 Regelung der Zugriffsmöglichkeiten von Telearbeiter/innen

Relevanz: Umsetzung/Wartung; Anwender/innen;

Erfordert die Telearbeit den Zugriff auf die IT der Institution (zum Beispiel auf einen Server), muss zuvor festgelegt werden, welche Objekte (Daten, Programme, IT-Komponenten) der/die Telearbeiter/in tatsächlich für die Erfüllung seiner/ihrer Aufgaben benötigt. Entsprechend sind die notwendigen Rechte wie Lese- und Schreibrechte auf diese Objekte zuzuweisen.

Auf Objekte, die der/die Telearbeiter/in für seine/ihre Aufgabenwahrnehmung nicht braucht, sollte er/sie auch nicht zugreifen können. Dies gilt sowohl für den Zugriff auf Daten wie auf in der Institution verfügbare IT-Komponenten. Damit soll erreicht werden, dass der Schaden, der auf Grund eines Hacker-Angriffs auf den Kommunikationsrechner entstehen kann, minimiert wird.

SYS 9.8 Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner- Institution

Relevanz: Umsetzung/Wartung; Anwender/innen;

Erfolgt im Rahmen der Telearbeit eine Datenübertragung zwischen einem Telearbeitsrechner und dem Kommunikationsrechner der Institution, werden dabei dienstliche Informationen üblicherweise über öffentliche Kommunikationsnetze übertragen. Da weder die Institution noch die Telearbeiter/innen großen Einfluss darauf nehmen können, ob die Vertraulichkeit, Integrität und Verfügbarkeit im öffentlichen Kommunikationsnetz gewahrt werden, sind ggf. zusätzliche Maßnahmen erforderlich, falls das öffentliche Netz keine ausreichende Sicherheit bieten kann.

Generell muss die Datenübertragung zwischen Telearbeitsrechner und Institution folgende Sicherheitsanforderungen erfüllen:

- *Sicherstellung der Vertraulichkeit der übertragenen Daten:*
  Es muss durch eine ausreichend sichere Verschlüsselung erreicht werden, dass auch durch Abhören der Kommunikation zwischen Telearbeitsrechner und Kommunikationsrechner der Institution kein Rückschluss auf den Inhalt der Daten möglich ist. Dazu gehört neben einem geeigneten Verschlüsselungsverfahren auch ein angepasstes Schlüsselmanagement mit periodischem Schlüsselwechsel.
- *Sicherstellung der Integrität der übertragenen Daten:*
  Die eingesetzten Übertragungsprotokolle müssen eine zufällige Veränderung übertragener Daten erkennen und beheben. Bei Bedarf kann auch ein zusätzlicher Fehlererkennungsmechanismus benutzt werden, um absichtliche Manipulationen während der Datenübertragung erkennen zu können (vgl. dazu §126a zu Datenbeschädigung (StGB), BGBl. Nr. 60/1974 i.d.g.F.).
- *Sicherstellung der Verfügbarkeit der Datenübertragung:*
  Falls zeitliche Verzögerungen bei der Telearbeit nur schwer zu tolerieren sind, sollte ein redundant ausgelegtes öffentliches Kommunikationsnetz als Übertragungsweg ausgewählt werden, in dem der Ausfall einzelner Verbindungsstrecken nicht den Totalausfall der Kommunikationsmöglichkeiten bedeutet. Auf eine redundante Einführung der Netzanbindung an den Telearbeitsrechner und die Schnittstelle der Institution kann ggf. verzichtet werden.

- *Sicherstellung der Authentizität der Daten:*
  Bei der Übertragung der Daten zwischen Telearbeitsrechner und Institution muss vertrauenswürdig feststellbar sein, ob die Kommunikation zwischen den richtigen Teilnehmern stattfindet, so dass eine Maskerade ausgeschlossen werden kann. Dies bedeutet, dass Daten mit Absender "Telearbeitsrechner" auch tatsächlich von dort stammen. Ebenso muss der Ursprung von Institutionsdaten zweifelsfrei auf die Institution zurückgeführt werden können.
- *Sicherstellung der Nachvollziehbarkeit der Datenübertragung:*
  Um eine Kommunikation nachvollziehbar zu machen, können Protokollierungsfunktionen eingesetzt werden, die nachträglich feststellen lassen, welche Daten wann an wen übertragen wurden.
- *Sicherstellung des Datenempfangs:*
  Ist es für die Telearbeit von Bedeutung, ob Daten korrekt empfangen wurden, so können Quittungsmechanismen eingesetzt werden, aus denen hervorgeht, ob der/die Empfänger/in die Daten korrekt empfangen hat.

Die Stärke der dazu erforderlichen Mechanismen richtet sich dabei nach dem Schutzbedarf der übertragenen Daten.

SYS 9.9 Sicherheitstechnische Anforderungen an den Kommunikationsrechner

Relevanz: Umsetzung/Wartung; Anwender/innen;

Je nach Art der Telearbeit und der dabei durchzuführenden Aufgaben gestaltet sich der Zugriff der Telearbeiter/innen auf Institutionsdaten anders. So ist denkbar, dass zwischen Telearbeiterinnen/ Telearbeitern und Institution nur E-Mails ausgetauscht werden. Andererseits kann auch ein Zugriff auf Server in der Institution für die Telearbeiter/innen notwendig sein.

Unabhängig von den Zugriffsweisen muss der Kommunikationsrechner der Institution im Allgemeinen folgende Sicherheitsanforderungen erfüllen:

- *Identifikation und Authentisierung:*
  Sämtliche Benutzer/innen des Kommunikationsrechners, also Administratoren, Mitarbeiter/innen in der Institution und Telearbeiter/innen, müssen sich vor einem Zugriff auf den Rechner identifizieren und authentisieren. Nach mehrfachen Fehlversuchen ist der Zugang zu sperren. Voreingestellte Passwörter sind zu ändern. Ggf. muss es für den Kommunikationsrechner auch möglich sein, während der Datenübertragung eine erneute Authentisierung der Telearbeiterin bzw. des Telearbeiters oder des Telearbeitsrechners anzustoßen, um aufgeschaltete Angreifer abzuwehren. Im Rahmen der Identifikation und Authentisierung der Benutzer/innen sollte auch zusätzlich eine Identifizierung der Telearbeitsrechner stattfinden (zum Beispiel über Rufnummern und Callback-Verfahren).
- *Rollentrennung:*
  Die Rollen der Administratoren und der Benutzer/innen des Kommunikationsrechners sind zu trennen. Eine Rechtevergabe darf ausschließlich Administratoren möglich sein.
- *Rechteverwaltung und -kontrolle:*
  Der Zugriff auf Dateien des Kommunikationsrechners darf nur im Rahmen der gebilligten Rechte erfolgen können. Der Zugriff auf angeschlossene Rechner in der Institution und darauf gespeicherte Dateien ist zu reglementieren. Dabei ist darauf zu achten, dass die Zugriffsmöglichkeiten auf das notwendige Mindestmaß beschränkt werden. Bei Systemabsturz oder bei Unregelmäßigkeiten muss der Kommunikationsrechner in einen sicheren Zustand übergehen, in dem ggf. kein Zugriff mehr möglich ist.

- *Minimalität der Dienste:*
  Dienste, die durch den Kommunikationsrechner zur Verfügung gestellt werden, müssen dem Minimalitätsprinzip unterliegen: alles ist verboten, was nicht ausdrücklich erlaubt wird. Die Dienste selbst sind auf den Umfang zu beschränken, der für die Aufgaben der Telearbeiter/innen notwendig ist.
- *Protokollierung:*
  Datenübertragungen vom, zum und über den Kommunikationsrechner sind mit Uhrzeit, Benutzer/in, Adresse und Dienst zu protokollieren. Dem Administrator bzw. dem Revisor sollten Werkzeuge zur Verfügung stehen, um die Protokolldaten auszuwerten. Dabei sollten Auffälligkeiten automatisch gemeldet werden.
- *Automatische Virenprüfung:*
  Übertragene Daten sind einer automatischen Prüfung auf Viren zu unterziehen.
- *Verschlüsselung:*
  Daten, die auf dem Kommunikationsrechner für die Telearbeiter/innen vorgehalten werden, sind bei entsprechender Vertraulichkeit - in Abstimmung mit der organisationsweiten IT-Sicherheitspolitik - zu verschlüsseln.
- *Vermeidung oder Absicherung von Fernadministration:*
  Benötigt der Kommunikationsrechner keine Fernadministration, so sind sämtliche Funktionalitäten zur Fernadministration zu sperren. Ist eine Fernadministration unvermeidbar, so muss sie ausreichend abgesichert werden. Jegliche Fernadministration darf nur nach vorhergehender erfolgreicher Identifikation und Authentisierung stattfinden. Administrationstätigkeiten sind zu protokollieren. Administrationsdaten sollten verschlüsselt übertragen werden. Voreingestellte Passwörter und kryptographische Schlüssel sind zu ändern.

SYS 9.10 Informationsfluss, Meldewege und Fortbildung

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

Damit der/die Telearbeiter/in nicht vom betrieblichen Geschehen abgeschnitten wird, sollte der/die Vorgesetzte einen regelmäßigen Informationsaustausch zwischen Telearbeiter/innen und den Arbeitskolleginnen und -kollegen ermöglichen. Dies ist wichtig, damit der/die Telearbeiter/in auch zukünftig über Planungen und Zielsetzungen in seinem/ihrem Arbeitsbereich informiert ist, damit Frustrationen vermieden werden und ein positives Telearbeitsklima geschaffen wird und erhalten bleibt.

Die Beteiligung der Telearbeiter/innen an Umlaufverfahren für Hausmitteilungen, einschlägige Informationen und Zeitschriften ist zu regeln. Dies stellt dann ein Problem dar, wenn der/die Telearbeiter/in ausschließlich zu Hause arbeitet. Eine Lösung wäre eventuell das Einscannen wichtiger Schriftstücke, um sie dann dem/der Telearbeiter/in per E-Mail zuzustellen. Zusätzlich sind die Telearbeiter/innen über Änderungen von IT-Sicherheitsmaßnahmen zu unterrichten.

Weiters müssen die Arbeitskolleginnen und -kollegen über Anwesenheits- und Erreichbarkeitszeiten sowie E-Mail-Adressen bzw. Telefonnummer der Telearbeiter/innen in Kenntnis gesetzt werden.

Folgende Punkte müssen darüber hinaus bei der Telearbeit geklärt werden:

- Wer ist Ansprechperson bei technischen und/oder organisatorischen Problemen in der Telearbeit?
- Wem müssen Sicherheitsvorkommnisse mitgeteilt werden?
- Wie erfolgt die Aufgabenzuteilung?
- Wie erfolgt die Übergabe der Arbeitsergebnisse?

Treten technisch-organisatorische Probleme auf, müssen diese von dem/der Telearbeiter/in unverzüglich der Institution gemeldet werden.

Da für die Telearbeit zum Teil andere IT-Sicherheitsmaßnahmen ergriffen werden müssen als für die Arbeit innerhalb der Institution, ist es notwendig, dass ein Sicherheitskonzept für die Telearbeitsplätze erstellt wird. Nach Bekanntgabe des Konzeptes müssen Telearbeiter/innen in die zu realisierenden Sicherheitsmaßnahmen eingewiesen und eventuell in ihrem Umgang geschult werden. Darüber hinaus ist der/die Telearbeiter/in so weit im Umgang mit dem Telearbeitsrechner zu schulen, dass er/sie einfache Tätigkeiten (z.B. Druckerpatrone wechseln) wahrnehmen kann bzw. einfache Probleme selbstständig lösen kann.

SYS 9.11 Vertretungsregelung für Telearbeit

Relevanz: Umsetzung/Wartung; Anwender/innen;

Über die Maßnahme PER 1.3 Vertretungsregelungen hinaus sind im Falle der Vertretung von Telearbeitern und Telearbeiterinnen weitere Schritte notwendig. Da der/die Telearbeiter/in hauptsächlich außerhalb der Institution tätig ist, muss ein Informationsfluss zu seiner/ihrer Vertretung vorgesehen werden. Auch eine Dokumentation der Arbeitsergebnisse seitens der Telearbeiterin bzw. des Telearbeiters ist unabdingbar. Ggf. sind sporadische oder regelmäßige Treffen zwischen Telearbeiter/innen und ihren Vertretungen sinnvoll.

Ergänzend dazu muss geregelt werden, wie Vertreter im unerwarteten Vertretungsfall Zugriff auf die Daten im Telearbeitsrechner oder am Telearbeitsplatz vorhandene Unterlagen nehmen kann.

Es empfiehlt sich, den Vertretungsfall probeweise durchzuspielen.

5.10 Protokollierung

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

SYS 10.1 Erstellung von Protokolldateien

Relevanz: Umsetzung/Wartung;

Art und Umfang von Protokollierungen hängen von den speziellen Anforderungen des IT-Systems und der darauf befindlichen Applikationen und Daten ab und sind im Einzelfall sorgfältig festzulegen. Die im Folgenden angeführten Anforderungen an die Protokollierung stellen Mindestanforderungen dar, wie sie für die meisten Systeme Gültigkeit haben.

Demnach sind bei der Administration von IT-Systemen die folgenden Aktivitäten vollständig zu protokollieren:

- *Systemgenerierung und Modifikation von Systemparametern:*
  Da auf dieser Ebene in der Regel keine systemgesteuerten Protokolle erzeugt werden, bedarf es entsprechender detaillierter manueller Aufzeichnungen, die mit der Systemdokumentation korrespondieren sollten.
- *Einrichten von Benutzerinnen und Benutzern:*
  Es ist vollständig zu protokollieren, wem von wann bis wann durch wen das Recht eingeräumt worden ist, das betreffende IT-System zu benutzen. Diese Protokolle sind Grundlage praktisch jeder Revisionsmaßnahme.
- *Erstellung von Rechteprofilen:*
  Im Rahmen der Protokollierung der Benutzerverwaltung kommt es insbesondere auch darauf an aufzuzeichnen, wer die Anweisung zur Einrichtung bestimmter Benutzerrechte erteilt hat.
- *Einspielen und Änderung von Anwendungssoftware:*
  Die Protokolle repräsentieren das Ergebnis der Programm- und Verfahrensfreigaben.
- *Änderungen an der Dateiorganisation:*
  Im Hinblick auf die vielfältigen Manipulationsmöglichkeiten, die sich bereits bei Benutzung der "Standard-Dateiverwaltungssysteme" ergeben, kommt einer vollständigen Protokollierung eine besondere Bedeutung zu (vgl. z.B. Datenbankmanagement).
- *Durchführung von Datensicherungsmaßnahmen:*
  Da derartige Maßnahmen (Backup, Restore) mit der Anfertigung von Kopien bzw. dem Überschreiben von Datenbeständen verbunden sind und häufig in "Ausnahmesituationen" durchgeführt werden, besteht eine erhöhte Notwendigkeit zur Protokollierung.
- *Sonstiger Aufruf von Administrations-Tools:*
  Die Benutzung aller Administrations-Tools ist zu dokumentieren, um feststellen zu können, ob Unbefugte sich Systemadministrator-Rechte erschlichen haben.
- *Versuche unbefugten Einloggens und Überschreitung von Befugnissen:*
  Geht man von einer wirksamen Authentisierungsprozedur und sachgerechten Befugniszuweisungen aus, kommt der vollständigen Protokollierung aller "auffälligen Abnormitäten" beim Einloggen und der Benutzung von Hard- und Softwarekomponenten eine zentrale Bedeutung zu. Benutzer/innen in diesem Sinne sind auch Systemadministratoren.

Um eine ordnungsgemäße Auswertung der Protokolldaten zu ermöglichen ist zu beachten:

- Die Speicherung der Protokolldaten hat in einer nicht manipulierbaren Form zu erfolgen (die Daten dürfen nicht gezielt verändert, unbefugt gelöscht oder zerstört werden können).
- Nicht-personenbezogene IDs sind zu vermeiden, da sie eine personenbezogene Auswertung unmöglich machen.
- Das Überschreiben eines bestimmten protokollierten Ereignisses durch ein gezieltes Auffüllen des Speichers der Protokolldaten mit "unverdächtigen" Daten muss zuverlässig verhindert werden.
- Die Entscheidung, welche Daten zu protokollieren sind, haben Datenschutz-/IT-Sicherheitsbeauftragte oder Applikationsverantwortliche in Übereinstimmung mit gesetzlichen Vorgaben (etwa Datenschutzgesetz (DSG 2000), BGBl. I Nr. 165/1999 i.d.g.F.) und der organisationsweiten IT-Sicherheitspolitik zu treffen. Dabei ist es wichtig, sich auf die tatsächlich relevanten Informationen zu beschränken, da ein zu großer Umfang an Daten die Auswertung der Daten erschweren oder sogar unmöglich machen kann.

SYS 10.2 Datenschutzrechtliche Aspekte bei der Erstellung von Protokolldateien

Relevanz: Umsetzung/Wartung; Anwender/innen;

Lt. § 14 (DSG 2000), BGBl. I Nr. 165/1999 i.d.g.F. (Datensicherheitsmaßnahmen) ist je nach Art der verwendeten personenbezogenen Daten und nach Umfang und Zweck der Verwendung, sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit sicherzustellen, dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind.

Unter anderem ist dazu Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können.

Protokoll- und Dokumentationsdaten dürfen nicht für Zwecke verwendet werden, die mit ihrem Ermittlungszweck - das ist die Kontrolle der Zulässigkeit der Verwendung des protokollierten oder dokumentierten Datenbestandes - unvereinbar sind. Unvereinbar ist insbesondere die Weiterverwendung zum Zweck der Kontrolle von Betroffenen, deren Daten im protokollierten Datenbestand enthalten sind, oder zum Zweck der Kontrolle jener Personen, die auf den protokollierten Datenbestand zugegriffen haben, aus einem anderen Grund als jenem der Prüfung ihrer Zugriffsberechtigung, es sei denn, dass es sich um die Verwendung zum Zweck der Verhinderung oder Verfolgung eines Verbrechens handelt, das mit mindestens fünfjähriger Freiheitsstrafe bedroht ist.

Aufbewahrungsfristen

Sofern gesetzlich nicht ausdrücklich anderes angeordnet ist, sind Protokoll- und Dokumentationsdaten drei Jahre lang aufzubewahren. Davon darf in jenem Ausmaß abgewichen werden, als der von der Protokollierung oder Dokumentation betroffene Datenbestand zulässigerweise früher gelöscht oder länger aufbewahrt wird (lt. § 14 (DSG 2000), BGBl. I Nr. 165/1999 i.d.g.F.).

Diese Pflichten gelten nur für den Gebrauch von personenbezogenen Daten. Protokollierungen von nicht-personenbezogenen Daten, wie z.B. die Installation eines Servers, Aufzeichnungen über den Datendurchsatz eines Systems, etc. sind nicht betroffen.

SYS 10.3 Kontrolle von Protokolldateien

Relevanz: Umsetzung/Wartung; Anwender/innen;

Die Protokollierung sicherheitsrelevanter Ereignisse ist als Sicherheitsmaßnahme nur wirksam, wenn die protokollierten Daten in regelmäßigen Abständen durch einen Revisor ausgewertet werden. Ist es personell oder technisch nicht möglich, die Rolle eines unabhängigen Revisors für Protokolldateien zu implementieren, kann ihre Auswertung auch durch den Administrator erfolgen. Für diesen Fall bleibt zu beachten, dass damit eine Kontrolle der Tätigkeiten des Administrators nur schwer möglich ist. Dem/der Datenschutz-/IT-Sicherheitsbeauftragten ist jedenfalls eine derartige Auswertung vorzulegen.

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

Je nach Art der Protokolldaten kann es sinnvoll sein, diese auf externen Datenträgern zu archivieren.

Da Protokolldateien in vielen Fällen personenbezogene Daten beinhalten, ist sicherzustellen, dass diese Daten nur für Zwecke, die mit ihrem Ermittlungszweck vereinbar sind, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes verwendet werden dürfen (vgl. §14 Z4 DSG 2000 (DSG 2000), BGBl. I Nr. 165/1999 i.d.g.F.).

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

- Liegen die Zeiten des An- und Abmeldens außerhalb der Arbeitszeit (Hinweis auf Manipulationsversuche)?
- Häufen sich fehlerhafte Anmeldeversuche (Hinweis auf den Versuch, Passwörter zu erraten)?
- Häufen sich unzulässige Zugriffsversuche (Hinweis auf Versuche zur Manipulation)?
- Gibt es auffällig große Zeitintervalle, in denen keine Protokolldaten aufgezeichnet wurden (Hinweis auf eventuell gelöschte Protokollsätze)?
- Ist der Umfang der protokollierten Daten zu groß (eine umfangreiche Protokolldatei erschwert das Auffinden von Unregelmäßigkeiten)?
- Gibt es auffällig große Zeitintervalle, in denen anscheinend kein Benutzerwechsel stattgefunden hat (Hinweis darauf, dass das konsequente Abmelden nach Arbeitsende nicht vollzogen wird)?
- Gibt es auffallend lange Verbindungszeiten in öffentliche Netze hinein?
- Wurde in einzelnen Netzsegmenten oder im gesamten Netz eine auffällig hohe Netzlast oder eine Unterbrechung des Netzbetriebes festgestellt (Hinweis auf Versuche, die Dienste des Netzes zu verhindern bzw. zu beeinträchtigen oder auf eine ungeeignete Konzeption bzw. Konfiguration des Netzes)?

Bei der Auswertung der Protokolldateien sollte besonderes Augenmerk auf alle Zugriffe gelegt werden, die unter Administratorkennungen durchgeführt wurden.

Wenn regelmäßig umfangreiche Protokolldateien ausgewertet werden müssen, ist es sinnvoll, ein Werkzeug zur Auswertung zu benutzen. Dieses Werkzeug sollte wählbare Auswertungskriterien zulassen und besonders kritische Einträge (z.B. mehrfacher fehlerhafter Anmeldeversuch) hervorheben.

Weiters ist zu beachten:

- Die Verantwortung für die Auswertung der Protokolldaten ist genau festzulegen.
- In besonders sicherheitskritischen Fällen sollte das Vier-Augen-Prinzip zur Anwendung kommen.
- Die Meldewege im Fall von Auffälligkeiten sind festzulegen.
- Es ist sicherzustellen, dass die Aktivitäten von Administratoren ausreichend kontrolliert werden können. Diese Sicherstellung kann durch technische oder organisatorische Maßnahmen erfolgen.

SYS 10.4 Rechtliche Aspekte bei der Erstellung und Auswertung von Protokolldateien zur E-Mail- und Internetnutzung

Relevanz: Management;

Die Überwachung des Fernmeldeverkehrs (Telefon. E-Mail etc.) durch den Arbeitgeber ist ein Problem, für das es derzeit noch keine klare Lösung gibt. Private Kommunikation genießt prinzipiell den Schutz des Fernmeldegeheimnisses und des Grundrechtes auf Datenschutz. Es muss aber auch gesagt werden, dass kein Recht der Arbeitnehmer/innen besteht, die vom Arbeitgeber zur Verfügung gestellten Ressourcen privat zu nutzen. Eine geringfügige private oder halbprivate Nutzung im Rahmen des normalen menschlichen Sozialverhaltens sollte zugelassen bzw. ignoriert werden. Ein totales Verbot privater Nutzung sollte nur in Extremfällen ausgesprochen werden (z.B. bei Behörden mit sehr hohen Ansprüchen an Sicherheit und Geheimhaltung).

Ein Arbeitgeber, der die private Nutzung von Internetdiensten einschränken will, sollte sich über die Gründe im Klaren sein.

- Der Hauptgrund werden die Kosten sein, die durch private Kommunikation verursacht werden, und zwar die direkten Kosten (Bandbreite, Speicherplatz) als auch der Verlust an Produktivität.
- Ein weiterer Grund für die Beschränkung privater E-Mail-Kommunikation kann im Schutz vor Viren, Trojanern und anderer schädlicher Software liegen.

Eine Vereinbarung zu diesem Thema ist wünschenswert. Gemäß §9 Abs.2 lit. f Bundes-Personalvertretungsgesetz, BGBl. Nr. 133/1967 i.d.g.F. ist bei der Einführung von Systemen zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten der Bediensteten, die über die Ermittlung von allgemeinen Angaben zur Person oder über die Ermittlung von fachlichen Voraussetzungen hinausgehen, mit dem Dienststellenausschuss das Einvernehmen herzustellen.

Gemäß §79c Beamten-Dienstrechtsgesetz 1979, BGBl. Nr.333/1979 i.d.g.F. §29l Vertragsbedienstetengesetz 1948, BGBl. Nr.86/1948 i.d.g.F. und §76g Richterdienstgesetz (RDG), BGBl. Nr.305/1961 i.d.g.F. ist die Einführung und Verwendung von Kontrollmaßnahmen und technischen Systemen, welche die Menschenwürde berühren, unzulässig, wobei die Frage, welche Maßnahmen die Menschenwürde berühren, interpretiert werden muss. Die Erläuterungen zu den Bestimmungen (1574 der Beilagen zu den Stenographischen Protokollen des Nationalrates XX. GP, NR: GP XX i.d.g.F.) verweisen auf die Judikatur zu §96 Arbeitsverfassungsgesetz, BGBl. Nr.22/1974 i.d.g.F.

Die Rechte des Arbeitgebers auf Schutz seiner EDV (insb. Gebrauch von Virenscannern) bleiben unberührt.

Die Gefahr von Virenbefall, Trojanern und anderer schädlicher Software lässt sich mit Hilfe geeigneter technischer Mittel stark reduzieren, insb. Virenscanner, Begrenzung des Rechts zur Installation ausführbarer Programme, Gebrauch von stabiler Systemsoftware, Einrichtung von kontrollierten Umgebungen zur Ausführung fragwürdiger Programme, etc.

Behörden, die im Rahmen des E-Governments tätig sind, werden rasch auf ein ernstes Problem stoßen: Den Nachweis von Zustellungen per E-Mail. Solange keine zuverlässigen Verfahren für E-Mail-Zustellbestätigungen existieren, begründet der protokollierte Postausgang zumindest den Anschein einer korrekten Versendung durch die Behörde. Der protokollierte Posteingang wiederum macht es unseriösen Elementen schwer, falsche Behauptungen aufzustellen (”Ich habe alles rechtzeitig mit E-Mail beantragt...”). Eine Aufzeichnung und Speicherung aller E-Mails (oder auch nur von Teilen, wie z.B. der Betreffzeile, Datum, Uhrzeit, Absender/in und Empfänger/in) kann die oben genannten Probleme verschärfen, aber auch die Beamtinnen und Beamten bei ihrer Tätigkeit unterstützen.

Falls ein dienstliches Interesse an der Verwendung von E-Mail für nicht unmittelbar dienstliche Zwecke besteht (z.B. Zusendung von Informationen durch die Personalvertretung), sollte derartige Mail von jeglicher Kontrolle ausgenommen werden. Weiters darf Mail an die Personalvertretung durch den Arbeitgeber nicht inhaltlich kontrolliert werden.

§26 Bundes-Personalvertretungsgesetz (PVG), BGBl. Nr. 133/1967 i.d.g.F. statuiert eine Geheimhaltungspflicht der Mitglieder der Personalvertretung über alle ihnen von einzelnen Bediensteten gemachten Mitteilungen, die der Sache nach oder auf Wunsch des/der Bediensteten vertraulich zu behandeln sind. Eine Erfassung von Telefondaten, mit der sich nachvollziehen lässt, mit wem ein Personalvertreter telefonisch in Kontakt war, widerspricht daher dem Datenschutzgesetz (Entscheidung der Datenschutzkommission vom 6.Oktober 1998, Zahl 120.599/8-DSK/98). Diese Entscheidung lässt sich auch auf E-Mail übertragen.

SYS 10.5 Audit und Protokollierung der Aktivitäten im Netz

Relevanz: Umsetzung/Wartung;

Eine angemessene Durchführung von Protokollierung, Audit und Revision ist ein wesentlicher Faktor der Netzsicherheit.

Protokollierung:

Eine Protokollierung innerhalb eines Netzmanagementsystems oder an bestimmten aktiven Netzkomponenten erlaubt es, gewisse (im Allgemeinen zu definierende) Zustände für eine spätere Auswertung abzuspeichern. Typische Fälle, die protokolliert werden können, sind z.B. die übertragenen fehlerhaften Pakete an einer Netzkomponente, ein unautorisierter Zugriff auf eine Netzkomponente oder die Performance eines Netzes zu bestimmten Zeiten. Eine Auswertung solcher Protokolle mit geeigneten Hilfsmitteln erlaubt beispielsweise einen Rückschluss, ob die Bandbreite des Netzes den derzeitigen Anforderungen genügt, oder die Erkennung von systematischen Angriffen auf das Netz.

Bei der Protokollierung fallen zumeist sehr viele Einträge an, so dass diese oft nur mit Hilfe eines Werkzeuges sinnvoll ausgewertet werden können.

Audit:

Unter einem Audit wird die Verwendung eines Dienstes verstanden, der insbesondere sicherheitskritische Ereignisse betrachtet. Dies kann online oder offline erfolgen. Bei einem Online-Audit werden die Ereignisse mit Hilfe eines Tools (z.B. einem Netzmanagementsystem) in Echtzeit betrachtet und ausgewertet. Bei einem Offline-Audit werden die Daten protokolliert oder aus einer bestehenden Protokolldatei extrahiert.

Beim Audit liegt die Fokussierung auf der Überwachung von sicherheitskritischen Ereignissen. Zusätzlich werden beim Audit häufig auch Daten über Nutzungszeiträume und anfallende Kosten erhoben.

Dabei sind für ein Audit insbesondere folgende Vorkommnisse von Interesse:

- Daten über die Betriebsdauer von IT-Systemen (wann wurde welches IT-System ein- bzw. wieder ausgeschaltet?),
- Zugriffe auf aktive Netzkomponenten (wer hat sich wann angemeldet?),
- sicherheitskritische Zugriffe auf Netzkomponenten und Netzmanagementkomponenten mit oder ohne Erfolg,
- Verteilung der Netzlast über die Betriebsdauer eines Tages oder eines Monats und die allgemeine Performance des Netzes.

Weiterhin sollten folgende Vorkommnisse protokolliert werden:

- Hardware-Fehlfunktionen, die zu einem Ausfall eines IT-Systems führen können,
- unzulässige Änderungen der IP-Adresse eines IT-Systems (in einem TCP/IP-Umfeld).

Ein Audit kann sowohl online als auch offline betrieben werden. Bei einem Online-Audit werden entsprechend kategorisierte Ereignisse direkt dem Auditor mitgeteilt, der ggf. sofort Maßnahmen einleiten kann. Dafür müssen Ereignisse in geeignete Kategorien eingeteilt werden, damit der zuständige Administrator oder Auditor auf wichtige Ereignisse sofort reagieren kann und nicht unter einer Flut von Informationen den Überblick verliert. Dabei ist auch zu überlegen, ob eine Rollentrennung erforderlich ist.

Bei einem Offline-Audit werden die Daten aus den Protokolldateien oder speziellen Auditdateien mit Hilfe eines Werkzeuges für Auditzwecke aufbereitet und durch den Auditor überprüft. Im letzteren Fall können Maßnahmen zur Einhaltung oder Wiederherstellung der Sicherheit nur zeitverzögert eingeleitet werden. Im Allgemeinen wird eine Mischform aus Online- und Offline-Audit empfohlen. Dabei werden für das Online-Audit die sicherheitskritischen Ereignisse gefiltert und dem Auditor sofort zur Kenntnis gebracht. Zusätzlich werden weniger kritische Ereignisse offline ausgewertet.

Revision:

Bei der Revision werden die beim (Offline-) Audit gesammelten Daten von einem oder mehreren unabhängigen Mitarbeiter/innenn (4-Augen-Prinzip) überprüft, um Unregelmäßigkeiten beim Betrieb der IT-Systeme aufzudecken und die Arbeit der Administratoren zu kontrollieren. Die mit einem Netzmanagementsystem möglichen Protokollierungs- und Audit-Funktionen sind in einem sinnvollen Umfang zu aktivieren. Neben Performance-Messungen zur Überwachung der Netzlast sind dabei insbesondere die Ereignisse (Events) auszuwerten, die von einem Netzmanagementsystem generiert werden, oder spezifische Datensammler einzusetzen, mit denen sicherheitskritische Ereignisse überwacht und ausgewertet werden können.

Auf keinen Fall dürfen Benutzer-Passwörter im Rahmen eines Audits oder einer Protokollierung gesammelt werden. Dadurch wird ein hohes Sicherheitsrisiko erzeugt, falls es zu einem unberechtigten Zugriff auf diese Informationen kommt. Ob falsch eingegebene Passwörter, die sich von den gültigen Passwörtern meist nur um ein Zeichen bzw. um eine Vertauschung zweier Zeichen unterscheiden, protokolliert werden, ist im Einzelfall zu entscheiden.

Es muss weiterhin festgelegt werden, wer die Protokolle und Audit-Daten auswertet. Hierbei muss eine angemessene Trennung zwischen Ereignisverursacher und -auswerter (z.B. Administrator und Auditor) vorgenommen werden. Weiterhin ist darauf zu achten, dass die datenschutzrechtlichen Bestimmungen eingehalten werden.

Die Protokoll- oder Auditdateien müssen regelmäßig ausgewertet werden. Sie können sehr schnell sehr umfangreich werden. Um die Protokoll- oder Auditdateien auf ein auswertbares Maß zu beschränken, sollten die Auswertungsintervalle daher angemessen, aber dennoch so kurz gewählt werden, dass eine sinnvolle Auswertung möglich ist.

SYS 10.6 Intrusion Detection Systeme

Relevanz: Umsetzung/Wartung;

Aufgabe von Intrusion Detection Systemen ist die Überwachung bzw. Analyse des Datenverkehrs bzw. der Aktivitäten auf IT-Systemen, mit dem Ziel, Eindringversuche zu erkennen, weiterzumelden und gegebenenfalls Gegenmaßnahmen einzuleiten.

Dies umfasst folgende Teilaufgaben:

- *Erfassung von Ereignissen:*
  Sammlung der wesentlichen Ereignisdaten aus Netzpaketen oder Protokolldateien
- *Analyse der erfassten Ereignisse:*
  Untersuchung der gespeicherten Aktivitäten auf Auffälligkeiten (z.B. anormales Verhalten von Benutzerinnen/Benutzern (”Anomalie Intrusion Detection Systeme”) oder bekannte Befehlsmuster (”Misuse Intrusion Detection Systeme”))
- *Speicherung der analysierten Daten*
- *Einleitung von Gegenmaßnahmen:*
  Generierung von Warnmeldungen und Setzen von Gegenmaßnahmen

Im Unterschied zu Firewalls, die die Anbindung eines Netzwerkes an ein Fremdnetz (etwa Internet) absichern, unterstützen Intrusion Detection Systeme die Erkennung unberechtigter Zugriffsversuche sowohl externer als auch interner Benutzer/innen innerhalb eines lokalen Netzes.

Intrusion Detection Systeme können andere Sicherheitsmaßnahmen, wie Authentisierung, Zugriffsschutzsysteme und Firewalls nicht ersetzen, sie können jedoch zu einer weiteren Erhöhung der Sicherheit, insbesondere in sensiblen Bereichen, beitragen.

5.11 Kryptographische Maßnahmen

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

Der Einsatz kryptographischer Verfahren kann die Gesamtsicherheit eines IT-Systems beträchtlich erhöhen.

Kryptographische Verfahren leisten etwa:

Vertraulichkeitsschutz durch Verschlüsselung

Die Vertraulichkeit übertragener oder gespeicherter Information kann durch geeignete Verschlüsselung sichergestellt werden. Das entscheidende Merkmal eines Verschlüsselungsverfahrens ist die Güte des Algorithmus sowie der Schlüsselauswahl.

Integritätsschutz durch MACs oder Digitale Signaturen

Schutz gegenüber Manipulationen bieten etwa Verfahren, die unter Verwendung eines symmetrischen Verschlüsselungsalgorithmus aus der zu übermittelnden Information einen so genannten Message Authentication Code (MAC) (auch Modification Detection Code (MDC) oder Message Integrity Code (MIC)) erzeugen.

Andere Verfahren bedienen sich eines asymmetrischen Verschlüsselungsalgorithmus in Kombination mit einer Hash-Funktion und erzeugen eine “Digitale Signatur”. Die jeweiligen erzeugten “Fingerabdrücke” (MAC, Digitale Signatur) werden zusammen mit der Information an den/die Empfänger/in übertragen und können von diesem/dieser überprüft werden.

Nichtabstreitbarkeit durch Elektronische Signaturen

Elektronische Signaturen sollen ein Pendant zur handschriftlichen Unterschrift für digitale Dateien und Nachrichten darstellen.

Sie beruhen auf asymmetrischen Verfahren. Die wesentliche Voraussetzung für elektronische Signaturen ist, dass jede/r Teilnehmer/in ein nur ihm/ihr bekanntes Geheimnis besitzt, mit dem er/sie zu beliebigen Dateien eine elektronische Signatur bilden kann. Anhand von öffentlichen Informationen muss es möglich sein, diese elektronische Signatur zu überprüfen.

In den nachfolgenden Maßnahmenbeschreibungen wird die Kenntnis kryptographischer Grundbegriffe vorausgesetzt. Andernfalls sei hier auf die entsprechenden Ausführungen in [BSI GSHB] (Maßnahme M 3.23 „Einführung in kryptographische Grundbegriffe“) bzw. die umfangreiche Fachliteratur zu diesem Thema verwiesen.

SYS 11.1 Entwicklung eines Kryptokonzepts

Relevanz: Management; Umsetzung/Wartung;

Aufgrund der Vielfalt kryptographischer Problemstellungen und unterschiedlicher Einflussfaktoren gibt es auch vielfältige Lösungsansätze und Realisierungsmöglichkeiten. Um den benötigten Grad an Sicherheit zu erreichen ist es erforderlich, ein Kryptokonzept zu entwickeln, das in das IT-Sicherheitskonzept der Behörde bzw. des Unternehmens integriert wird.

Die Auswahl geeigneter kryptographischer Komponenten muss auf diesem Konzept basieren.

Ein möglicher Aufbau eines Kryptokonzepts ist in Anhang C.11 Inhaltsverzeichnis Kryptokonzept (Muster) beispielhaft aufgezeigt.

Einzelne Punkte dieses Konzepts werden in den nachfolgenden Maßnahmenbeschreibungen näher ausgeführt.

Bei der Erstellung eines Kryptokonzeptes handelt es sich nicht um eine einmalige Aufgabe, sondern um einen dynamischen Prozess. Ein Kryptokonzept muss daher regelmäßig den aktuellen Gegebenheiten angepasst werden.

SYS 11.2 Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte

Relevanz: Umsetzung/Wartung;

Um bei der Verarbeitung und Übertragung sensitiver Informationen zu realistischen, verlässlichen und anwendungsgerechten Bedarfsanforderungen und Rahmenbedingungen für den Einsatz kryptographischer Verfahren und Produkte zu kommen, müssen zunächst die schützenswerten Daten identifiziert und bewertet werden.

Identifikation der zu schützenden Daten

Zunächst muss festgestellt werden, für welche Aufgaben kryptographische Verfahren eingesetzt werden sollen, und welche Daten damit gesichert werden sollen.

Der Einsatz kryptographischer Verfahren kann aus verschiedenen Gründen erforderlich sein, etwa:

- zum Schutz der Vertraulichkeit bzw. der Integrität von Daten,
- zur Authentisierung,
- für Sende- oder Empfangsnachweise.

Je nach Einsatzzweck können verschiedene kryptographische Methoden wie z.B. Verschlüsselung oder Digitale Signaturen sinnvoll sein (s.o.).

Um festzustellen, welche kryptographischen Verfahren bzw. Produkte benötigt werden und welche Daten damit zu schützen sind, sollte zunächst die aktuelle IT-Struktur ermittelt werden.

Ermittelt werden sollte,

- welche IT-Systeme es gibt, auf denen Daten verarbeitet bzw. gespeichert (PCs, Laptops, Server, ...) oder mit denen Daten übermittelt werden (Bridge, Router, Gateway, Firewall, ..) und
- welche Übertragungswege es gibt. Dazu sollte die logische und physikalische Vernetzungsstruktur erfasst werden (siehe auch SYS 6.3 „Ist-Aufnahme der aktuellen Netzsituation“).

Schutzbedarf der Daten (Vertraulichkeit, Integrität, Authentizität, Nichtabstreitbarkeit)

Es sollten alle Anwendungen bzw. Daten ermittelt werden, bei denen ein besonderer Anspruch an Vertraulichkeit, Integrität, Authentizität bzw. Nichtabstreitbarkeit besteht. Allerdings werden nicht nur für IT-Systeme, Anwendungen oder Informationen mit höherem Schutzbedarf kryptographische Produkte benötigt, sondern auch für solche mit mittlerem Schutzbedarf.

Beispiele für Daten mit besonderem Vertraulichkeitsanspruch sind

- personenbezogene Daten,
- Passwörter und kryptographische Schlüssel,
- Daten, aus denen ein Konkurrenzunternehmen finanzielle Gewinne ziehen könnte,
- Daten, ohne deren Vertraulichkeit die Aufgabenerfüllung gefährdet ist (z.B. Ermittlungsergebnisse),
- Daten, deren Veröffentlichung eine Rufschädigung verursachen könnte.

Beispiele für Daten mit besonderem Integritätsanspruch sind

- finanzwirksame Daten, durch deren Manipulation finanzielle Schäden entstehen können,
- Informationen, deren verfälschte Veröffentlichung Regressforderungen nach sich ziehen könnte,
- Daten, deren Verfälschung zu einer verminderten Produktqualität führen kann.

Ein Beispiel für Anwendungen mit besonderem Anspruch an Authentizität sind Remote-Zugriffe.

Ein Beispiel für Daten mit besonderem Anspruch an Nichtabstreitbarkeit sind Bestellungen oder Reservierungen, bei denen der Besteller identifizierbar sein sollte.

Als Ergebnis der Schutzbedarfsfeststellung ist festzulegen, welche Anwendungen oder Daten kryptographisch gesichert werden sollen. Diese Festlegung kann später noch verfeinert werden und sollte regelmäßig überarbeitet werden.

Als Resultat ergibt sich somit ein Überblick über alle Speicherorte und Übertragungsstrecken, die kryptographisch gesichert werden müssen.

Über die sicherheitstechnischen Anforderungen hinaus sind bei der Entwicklung eines Kryptokonzeptes und dem Einsatz kryptographischer Produkte auch noch eine Reihe anderer Aspekte von Bedeutung:

- *Technische Aspekte:*
  Dazu zählen etwa Fragen nach der physischen Sicherheit der Einsatzumgebung und Performance-Anforderungen.

- *Personelle und organisatorische Aspekte:*
  Dazu zählen Benutzerfreundlichkeit, Zumutbarkeit und Zuverlässigkeit der kryptographischen Verfahren und Produkte sowie eventueller zusätzlicher Schulungs- und Personalbedarf.
- *Wirtschaftliche Aspekte,*
  wie etwa einmalige Investitionskosten, laufende Kosten für Betrieb und Wartung sowie Lizenzgebühren.
- *Key Recovery:*
  Falls die zur Verschlüsselung benutzten Schlüssel verloren gehen, sind im Allgemeinen auch die damit geschützten Daten verloren. Viele Kryptoprodukte bieten daher Funktionen zur Datenwiedergewinnung für solche Fälle an. Solche Funktionen bringen aber auch Risiken mit sich: Wenn dadurch vertrauliche Schlüssel wiederhergestellt werden können, muss sichergestellt sein, dass dies nur Berechtigte können. Wenn es möglich ist, ohne Wissen der Original-Schlüsselbenutzerin bzw. des Original-Schlüsselbenutzers auf deren/dessen Daten zuzugreifen, hat diese/r keine Möglichkeit, böswillige Manipulationen zu beweisen. Der Einsatz von Key Recovery Mechanismen führt auch häufig aufgrund des entgegengebrachten Misstrauens zu Vorbehalten innerhalb des eigenen Unternehmens bzw. Behörde, aber auch bei den Kommunikationspartnern. Bei der Datenübertragung sollte daher generell auf Key Recovery verzichtet werden. Hierfür gibt es auch keine Notwendigkeit, da beim Schlüssel- oder Datenverlust diese einfach noch einmal ausgetauscht werden können. Bei der lokalen Speicherung von Daten sollte der Einsatz sorgfältig überlegt werden (siehe auch BCP 1.4 „Datensicherung bei Einsatz kryptographischer Verfahren“).
- *Lebensdauer von kryptographischen Verfahren:*
  Kryptographische Verfahren und Produkte müssen regelmäßig daraufhin überprüft werden, ob sie noch dem Stand der Technik entsprechen. Bereits bei der Auswahl kryptographischer Verfahren sollte daher eine zeitliche Grenze für deren Einsatz festgelegt werden. Zu diesem Zeitpunkt sollte noch einmal gründlich überdacht werden, ob die eingesetzten Kryptomodule noch den erwarteten Schutz bieten.
- *Gesetzliche Rahmenbedingungen:*
  Beim Einsatz kryptographischer Produkte sind diverse gesetzliche Rahmenbedingungen zu beachten. In einigen Ländern dürfen beispielsweise kryptographische Verfahren nicht ohne Genehmigung eingesetzt werden. Daher muss untersucht werden, ob innerhalb der zum Einsatzgebiet gehörenden Länder Einschränkungen beim Einsatz kryptographischer Produkte zu beachten sind und ob für in Frage kommende Produkte Exportbeschränkungen beachtet werden müssen (z.B. lt. Außenhandelsgesetz 1995, BGBl. Nr.172/1995 i.d.g.F.) (siehe SYS 11.4 „Auswahl eines geeigneten kryptographischen Produktes“).

SYS 11.3 Auswahl eines geeigneten kryptographischen Verfahrens

Relevanz: Umsetzung/Wartung;

Kriterien für die Auswahl eines kryptographischen Verfahrens sind:

- *Mechanismenstärke / Schlüssellänge:*
  Ein wesentliches Kriterium für die Auswahl von kryptographischen Verfahren stellt ihre kryptographische Stärke dar. Bei symmetrischen Verfahren stellt eine ausreichend große Schlüssellänge eine notwendige - wenn auch nicht hinreichende - Bedingung für die Sicherheit dar. Je größer die verwendete Schlüssellänge bei einem kryptographischen Verfahren ist, desto länger dauert die Berechnung des Schlüssels durch eine Brute-Force-Attacke. Andererseits werden die Verfahren bei der Verwendung längerer Schlüssel langsamer, so dass immer zu überlegen ist, welche Schlüssellänge unter Nutzen-/Leistungsgesichtspunkten angemessen ist. Als Faustregel für gute Verfahren und mittleren Schutzbedarf gilt derzeit, dass die eingesetzten Schlüssel mindestens 100 Bit lang sein sollten (vgl. Signaturverordnung (SigV), BGBl. II Nr. 30/2000 i.d.g.F.). Bei Verwendung von Blockchiffren sollten größere, strukturierte Datenmengen nicht im ECB-Modus verschlüsselt werden. Stattdessen sollten dazu der CBC-Modus oder der CFB-Modus verwendet werden. Mindestens eine dieser Betriebsarten sollte daher implementiert sein. Bei asymmetrischen Verfahren sollte die Mechanismenstärke so gewählt werden, dass die Lösung der zu Grunde liegenden mathematischen Probleme zum Brechen des Verfahrens einen unvertretbar großen bzw. praktisch unmöglichen Rechenaufwand erfordert (die zu wählende Mechanismenstärke hängt daher vom aktuellen Stand der Algorithmik und der Rechentechnik ab). Gegenwärtig kann man davon ausgehen, dass mit Modullängen von 1024 Bit bei RSA bzw. Untergruppenordnungen in der Größe von 160 Bit bei ElGamal-Verfahren auf einer geeigneten elliptischen Kurve ausreichende Sicherheit für *mittleren Schutzbedarf* erreicht wird (Quelle: [BSI GSHB] Ausgaben Juli 1999 / Oktober 2000, Maßnahme M 2.164). Zu beachten ist, dass für bestimmte Anforderungen u.U. größere Schlüssellängen erforderlich sind; so sind etwa laut derzeit gültiger Signaturverordnung (SigV), BGBl. II Nr. 30/2000 i.d.g.F. für sichere elektronische Signaturen Schlüssellängen von 1023 Bit für RSA und DSA erforderlich. Grundsätzlich sollten nur Algorithmen eingesetzt werden, die veröffentlicht sind, von einem breiten Fachpublikum intensiv untersucht wurden und von denen keine Sicherheitslücken bekannt sind. Vor der Verwendung von unbekannten Algorithmen aus Quellen, deren kryptographische Kompetenz nicht ausreichend nachgewiesen ist, kann nur gewarnt werden.
- *Symmetrische, asymmetrische oder hybride Verfahren?*
  Aus Performancegründen werden für Verschlüsselungszwecke keine reinen Public-Key-Implementierungen eingesetzt. Alle gängigen Implementierungen von Public-Key-Kryptographie nutzen hybride Verfahren. In Anwendungen mit großen oder offenen Nutzergruppen empfiehlt sich meist die Verwendung eines hybriden Verfahrens (wegen der Vorzüge für das Schlüsselmanagement). Bei kleinen, geschlossenen Nutzergruppen (insbesondere natürlich bei einem/einer einzelnen Benutzer/in) kann man sich auf symmetrische Verfahren beschränken. Bei Einsatz hybrider Verfahren ist es sinnvoll, die Stärken des symmetrischen und des asymmetrischen Anteils aufeinander abzustimmen. Da mit dem asymmetrischen Verfahren vor einem Schlüsselwechsel in der Regel viele Schlüssel für das symmetrische Verfahren verschlüsselt werden (”Überschlüsselung”), sollte der asymmetrische Algorithmus eher etwas stärker ausgelegt werden.

- *Realisierbarkeit von technischen Anforderungen*
  Die Chiffrieralgorithmen müssen so beschaffen sein, dass die technischen Anforderungen, insbesondere die geforderte Performance, durch eine geeignete Implementation erfüllt werden können. Hierunter fallen Anforderungen an die Fehlerfortpflanzung (z.B. falls über stark rauschende Kanäle gesendet wird), aber auch Anforderungen an Synchronisationsoverhead und Zeitverzögerung (z.B. falls "Echtzeit"-Verschlüsselung von großen Datenmengen erforderlich ist).

SYS 11.4 Auswahl eines geeigneten kryptographischen Produktes

Relevanz: Umsetzung/Wartung;

Aufgrund des breiten Spektrums kryptographischer Anwendungen können im Folgenden lediglich grundsätzliche Empfehlungen zur Auswahl von kryptographischen Produkten gegeben werden, die im konkreten Fall zu detaillieren sind.

Funktionalität

Das ausgewählte Produkt muss die von dem/der Anwender/in spezifizierte Funktionalität aufweisen.

Es muss insbesondere:

- die geforderten kryptographischen Grunddienste leisten,
- evtl. besonderen Anforderungen durch die Einsatzumgebung genügen (z.B. Single-User/Multi-User-PC, LAN-Umgebung, WAN-Anbindung),
- die geforderten technischen Leistungsmerkmale aufweisen (z.B. Durchsatzraten),
- die geforderten Sicherheitsfunktionalitäten aufweisen, insbesondere müssen die eingesetzten kryptographischen Mechanismen die erforderliche Stärke aufweisen.

Interoperabilität

Das ausgewählte Produkt wird in der Regel in eine bestehende IT-Umgebung eingefügt.

Es muss dort möglichst interoperabel sein. Die Einhaltung interner Standards ist nötig, um die Interoperabilität mit dem bereits vorhandenen IT-System bzw. Systemkomponenten zu gewährleisten. Die Anwendung internationaler Standards für kryptographische Techniken sollte selbstverständlich sein, sie erleichtert auch eine Sicherheitsevaluierung der kryptographischen Komponenten.

Wirtschaftlichkeit

Das ausgewählte Produkt sollte möglichst wirtschaftlich sein.

Dabei müssen Anschaffungskosten, Stückzahlen, Kosten für Wartung und Produktpflege, aber auch Einsparungen durch etwaige Rationalisierungseffekte berücksichtigt werden.

Zertifizierte Produkte

Die "Information Technology Security Evaluation Criteria" ([ITSEC]) bzw. die "Common Criteria" ([Common Criteria]) bieten einen Rahmen, innerhalb dessen die Sicherheitsfunktionalitäten eines IT-Produktes durch Anlegen von etablierten Kriterien in eine genau spezifizierte Hierarchie von Sicherheitsstufen eingeordnet werden können.

Die Informationssicherheitsbehörden mehrerer Staaten haben jeweils ein nationales Zertifizierungsschema nach diesen Kriterien aufgebaut.

Der Einsatz eines zertifizierten Produktes bietet die Gewähr, dass die Sicherheitsfunktionalität dieses Produktes unabhängig geprüft wurde und den im Evaluationslevel spezifizierten Standard nicht unterschreitet (siehe auch ENT 3.1 „Beachtung des Beitrags der Zertifizierung für die Beschaffung").

Importprodukte

In mehreren Staaten unterliegt der Export von starker Kryptographie starken Beschränkungen.

Insbesondere wird die Stärke von an sich starken Verschlüsselungsprodukten künstlich (durch Reduzierung der Schlüsselmannigfaltigkeit) herabgesetzt. Solche künstlich geschwächten Verfahren erreichen i.d.R. nicht die für mittleren Schutzbedarf erforderliche Mechanismenstärke. Beim Einsatz von Importprodukten sollte immer darauf geachtet werden, ob sie den vollen Leistungsumfang bieten.

Grenzüberschreitender Einsatz

Viele Unternehmen und Behörden haben zunehmend das Problem, dass sie auch ihre internationale Kommunikation, z.B. mit ausländischen Tochterunternehmen, kryptographisch absichern wollen.

Hierfür muss zunächst untersucht werden,

- ob innerhalb der jeweiligen Länder Einschränkungen beim Einsatz kryptographischer Produkte zu beachten sind und
- ob für in Frage kommende Produkte Export- oder Importbeschränkungen bestehen.

Fehlbedienungs- und Fehlfunktionssicherheit

Das Gefährliche an kryptographischen Produkten ist, dass sie Anwender/innen in einer - mitunter trügerischen - Sicherheit wiegen.

Daher kommt Maßnahmen gegen Kompromittierungen durch Bedienungsfehler oder technisches Versagen besondere Bedeutung zu, da deren Folgen eine gravierende Gefährdung der Sicherheit darstellen können. Allerdings ist die Bandbreite bezüglich redundanter Systemauslegung und zusätzlicher Überwachungsfunktionen - und damit an Gerätekosten - groß, sodass hier die Maßnahmen im Einzelfall in Abhängigkeit von den Anforderungen festzulegen sind.

Implementierung in Software, Firmware oder Hardware

Kryptographische Algorithmen können sowohl in Software, in Firmware als auch in Hardware implementiert werden.

Softwarerealisierungen werden in der Regel vom Betriebssystem des jeweiligen IT-Systems gesteuert. Unter Firmware versteht man Programme und Daten, die permanent so in Hardware gespeichert sind, dass die Speicherinhalte nicht dynamisch verändert werden können, und die während ihres Ablaufs nicht modifiziert werden können. Bei Hardwarelösungen wird das kryptographische Verfahren direkt in Hardware realisiert, z.B. als separates Sicherheitsmodul oder als Einsteckkarte.

Softwarelösungen bieten den Vorteil, leicht anpassbar und kostengünstig zu sein. Hardwarerealisierungen bieten im Allgemeinen sowohl höhere Manipulationsresistenz (und damit Sicherheit) als auch höheren Datendurchsatz als Softwarerealisierungen, sie sind aber meist auch teurer.

Firmwarelösungen kann man als Kompromiss der beiden vorangegangenen Möglichkeiten verstehen. Die Vor- und Nachteile der jeweiligen Realisierung beziehen sich jedoch immer nur auf lokale Aspekte (dazu gehört vor allem das Schlüsselmanagement). Sind die Daten einmal verschlüsselt und befinden sie sich auf dem Kommunikationsweg, ist im Prinzip das Zustandekommen der Verschlüsselung nicht mehr relevant.

Ein Beispiel für (relativ) preiswerte, transportable und benutzerfreundliche Kryptomodule sind Chipkarten, die im Bereich der lokalen Verschlüsselung als sicheres Speichermedium für die kryptographischen Schlüssel oder im Bereich der Authentikation zur Passwort-Generierung und Verschlüsselung eingesetzt werden können.

SYS 11.5 Regelung des Einsatzes von Kryptomodulen

Relevanz: Umsetzung/Wartung; Anwender/innen;

Auch im laufenden Betrieb müssen eine Reihe von Sicherheitsanforderungen an den Einsatz von Kryptomodulen gestellt werden. Diese müssen adäquat in das technische und organisatorische Umfeld eingebunden sein, in dem sie eingesetzt werden.

Wichtige organisatorische Regelungen dafür sind:

- Es müssen Verantwortliche benannt werden, und zwar für die Erstellung des Kryptokonzeptes, für die Auswahl sowie für den sicheren Betrieb der kryptographischen Produkte.
- Es sind geeignete personelle Maßnahmen festzulegen bzw. durchzuführen (Schulung, Benutzer-Support, Vertretungsregelungen, Verpflichtungen, Rollenzuteilungen).
- Die Benutzer/innen sollten nicht nur im Umgang mit den von ihnen zu bedienenden Kryptomodulen geschult werden, sie sollten darüber hinaus für den Nutzen und die Notwendigkeit der kryptographischen Verfahren sensibilisiert werden und einen Überblick über kryptographische Grundbegriffe erhalten.
- Falls Probleme oder der Verdacht auf Sicherheitsvorfälle beim Einsatz von Kryptomodulen auftreten, muss klar definiert sein, was in solchen Fällen zu unternehmen ist. Alle Benutzer/innen müssen über die entsprechenden Verhaltensregeln und Meldewege informiert sein.

- Im Rahmen des Kryptokonzeptes ist festzulegen, wer wann welche Kryptoprodukte benutzen muss bzw. darf und welche Randbedingungen dabei zu beachten sind (z.B. Schlüsselhinterlegung).
- Der korrekte Einsatz der Kryptomodule sollte regelmäßig überprüft werden. Ebenso ist regelmäßig zu hinterfragen, ob die eingesetzten kryptographischen Verfahren noch dem Stand der Technik entsprechen.
- Abhängig von den definierten Verfügbarkeitsanforderungen sollten Ersatz-Kryptomodule vorrätig gehalten werden, um einen reibungslosen Betrieb zu gewährleisten. Dies ist insbesondere dort wichtig, wo der Zugriff auf verschlüsselte Daten von der Funktionsfähigkeit eines einzelnen Kryptomoduls abhängt, z.B. bei der Datenarchivierung oder der ISDN-Verschlüsselung.

Zur Gewährleistung eines sicheren Betriebs der Kryptomodule sind folgende Maßnahmen zu setzen:

- Vor der Inbetriebnahme muss die optimale Konfiguration der Kryptomodule festgelegt werden, z.B. hinsichtlich Schlüssellänge, Betriebsmodi oder Kryptoalgorithmen.
- Die festgelegte Konfiguration muss dokumentiert sein, damit sie nach einem Systemversagen oder einer Neuinstallation schnell wieder eingerichtet werden kann.
- Für die Benutzer/innen müssen die Kryptoprodukte durch den Administrator so vorkonfiguriert sein, dass ohne weiteres Zutun der Benutzer/innen maximale Sicherheit erreicht werden kann.
- Bei komplexeren Kryptoprodukten müssen geeignete Handbücher verfügbar sein.
- Die Kryptomodule müssen sicher installiert und anschließend getestet werden.
- Die Anforderungen an die Einsatzumgebung müssen festgelegt sein, eventuell sind dafür ergänzende Maßnahmen im IT-Umfeld zu treffen.
- Umfang und Häufigkeit der Wartung sowie die Verantwortlichkeiten dafür sind festzulegen.

SYS 11.6 Physikalische Sicherheit von Kryptomodulen

Relevanz: Umsetzung/Wartung;

Wie in SYS 11.4 „Auswahl eines geeigneten kryptographischen Produktes“ beschrieben, können Kryptomodule in Software, Firmware oder Hardware realisiert sein. Letztere werden insbesondere dann gewählt, wenn das Kryptomodul besonders manipulationsresistent sein soll.

Hardware-Kryptomodule sollten unter Verwendung von physikalischen Sicherheitsmaßnahmen oder unter Ausnutzung entsprechender Materialeigenschaften so konstruiert sein, dass ein unautorisierter physikalischer Zugriff auf Modulinhalte erfolgreich verhindert werden kann.

Möglichkeiten dazu sind etwa:

- die Verwendung von Passivierungsmaterialien,
- geeignete Tamperschutzmaßnahmen,
- mechanische Schlösser sowie
- automatische Löschung (Vernichtung) aller im Klartext enthaltenen sensitiven Schlüsseldaten und -parameter bei unbefugtem Öffnen des Gehäuses.

Durch den Einsatz von Sensoren und Überwachungseinrichtungen lässt sich sicherstellen, dass das Kryptomodul in seinem vorgesehenen Arbeitsbereich, etwa bzgl. Spannungsversorgung, Taktung, Temperatur, mechanische Beanspruchung und elektromagnetische Beeinträchtigung, betrieben wird.

Zur Aufrechterhaltung seiner beabsichtigten Funktionalität sollte das Kryptomodul Selbsttests initiieren und durchführen können. Diese Tests können sich auf folgende Bereiche erstrecken: Algorithmentests, Software und Firmwaretests, Funktionstests, statistische Zufallstests, Konsistenztests, Bedingungstests sowie Schlüsselgenerierungs- und -ladetests. Bei einem negativen Testergebnis sollte den Benutzerinnen bzw. Benutzern des Kryptomoduls eine entsprechende Fehlermeldung signalisiert und ein entsprechender Fehlerzustand eingenommen werden. Erst nach Behebung der Fehlerursache(n) darf eine Freischaltung aus diesem Fehlerzustand möglich sein.

Beim Einsatz von Softwareprodukten muss die physikalische Sicherheit des Kryptomoduls durch das jeweilige IT-System bzw. dessen Einsatzumgebung geleistet werden. Eine Softwarelösung sollte Selbsttests durchführen können, um Modifikationen durch Trojanische Pferde oder Viren erkennen zu können.

SYS 11.7 Key-Management

Relevanz: Umsetzung/Wartung; Anwender/innen;

Die Verwendung kryptographischer Sicherheitsmechanismen (z.B. Verschlüsselung, digitale Signatur) setzt die vertrauliche, integere und authentische Erzeugung, Verteilung und Installation von geeigneten Schlüsseln voraus. Schlüssel, die Unbefugten zur Kenntnis gelangt sind, bei der Verteilung verfälscht worden sind oder gar aus unkontrollierter Quelle stammen, können den kryptographischen Sicherheitsmechanismus genauso kompromittieren wie qualitativ schlechte Schlüssel, die auf ungeeignete Weise erzeugt worden sind. Qualitativ gute Schlüssel werden in der Regel unter Verwendung geeigneter Schlüsselgeneratoren erzeugt.

Für das Schlüsselmanagement sind folgende Punkte zu beachten:

Schlüsselgenerierung

Die Auswahl der Schlüssel muss sich am eingesetzten Verfahren orientieren.

Schlüssel dürfen nicht leicht erratbar oder rekonstruierbar sein. Für eine “gute” Schlüsselwahl eignen sich insbesondere Zufallszahlengeneratoren. Auch muss sichergestellt werden, dass bei der Installation des Verschlüsselungsverfahrens etwaige voreingestellte Schlüssel geändert werden.

Schlüsseldiversifizierung

Kryptographische Schlüssel sollten möglichst nur für einen Einsatzzweck dienen.

Insbesondere sollten für die Verschlüsselung immer andere Schlüssel als für die Signaturbildung benutzt werden. Dies ist sinnvoll,

- damit bei der Offenlegung eines Schlüssels nicht alle Verfahren betroffen sind,
- um Abhängigkeiten zwischen Schlüsseln bzw. erzeugten Daten zu vermeiden,
- da es manchmal erforderlich sein kann, Schlüssel weiterzugeben (Vertretungsfall),
- da es unterschiedliche Zyklen für den Schlüsselwechsel geben kann.

Schlüsselverteilung / Schlüsselaustausch

Kryptographische Kommunikationsbeziehungen können nur dann funktionieren, wenn die Kommunikationspartner über aufeinander abgestimmte kryptographische Schlüssel verfügen.

Dazu müssen alle Kommunikationspartner mit den dazu erforderlichen Schlüsseln versorgt werden. Zur Schlüsselverteilung und zum Schlüsselaustausch können unterschiedliche Verfahren verwendet werden.

Unter Schlüsselverteilung wird hier die initiale Versorgung der Kommunikationspartner mit Grundschlüsseln verstanden. Die Schlüssel werden dazu von einer meist zentralen Schlüsselerzeugungsstelle (z.B. einem Trust Center) an die einzelnen Kommunikationspartner übermittelt. Die Verteilung der Schlüssel sollte auf geeigneten Datenträgern (z.B. Chipkarten) oder über Kommunikationsverbindungen (z.B. LAN, WAN) vertraulich (z.B. verschlüsselt), integer (z.B. MAC-gesichert) und authentisch (z.B. digital signiert) erfolgen. Die unbefugte Kenntnisnahme bzw. Verfälschung der Schlüssel muss verhindert oder wenigstens erkannt werden können.

Mit Schlüsselaustausch wird die Schlüsseleinigungsprozedur zwischen zwei Kommunikationspartnern auf einen Sitzungsschlüssel (Session Key) bezeichnet. Der Session Key ist ein Schlüssel, der nur eine begrenzte Zeit, etwa für die Dauer einer Kommunikationsverbindung, verwendet wird.

Schlüsselinstallation und -speicherung

Der Vertraulichkeitsschutz durch Verschlüsselung kann nur dann umfassend erreicht werden, wenn die verwendeten kryptographischen Schlüssel geheim gehalten werden können.

Bieten die IT-Systeme, auf denen das Verschlüsselungsverfahren eingesetzt ist, keinen ausreichenden Zugriffsschutz für die Schlüssel, sollten diese nicht auf diesem IT-System gespeichert werden. Besser ist eine bedarfsorientierte manuelle Eingabe oder die Auslagerung der Schlüssel auf einen externen Datenträger. Aus Sicherheitsgründen bieten sich hier insbesondere Chipkarten an.

Auf jeden Fall muss sichergestellt werden, dass bei der Installation des Verschlüsselungsverfahrens voreingestellte Schlüssel geändert werden.

Schlüsselarchivierung

Für Archivierungszwecke sollte das kryptographische Schlüsselmaterial auch außerhalb des Kryptomoduls in verschlüsselter Form speicherbar und gegebenenfalls wieder einlesbar sein.

Die kryptographischen Schlüssel können ihrerseits wieder - unter einem so genannten Masterkey oder Key-Encrypting-Key (KEK) - verschlüsselt werden. Der KEK muss entsprechend sicher (z.B. auf einer im Safe deponierten Chipkarte gespeichert) aufgehoben werden. Empfehlenswert ist die Splittung des KEK in zwei oder mehrere Teilschlüssel, sodass zur Rekonstruktion des KEK zwei oder mehrere Personen gleichzeitig anwesend sein müssen.

Im Bereich der öffentlichen Verwaltung wird zur Verschlüsselung die Verwendung von Verschlüsselungszertifikaten empfohlen, wobei alle Zertifikate innerhalb einer Organisationseinheit das gleiche Schlüsselpaar verwenden, sodass eine separate Schlüsselhinterlegung nicht notwendig wird. Es ist somit nur mehr das innerhalb der Organisationseinheit gemeinsame Schlüsselpaar geeignet zu archivieren. [IKTB-181202-1]

Zugriffs- und Vertretungsregelung

In der Sicherheitspolitik sollten Fragen bzgl. der Zugriffs- und Vertretungsrechte geregelt sein.

Entsprechende Mechanismen müssen vom Schlüsselmanagement und von den einzusetzenden Kryptomodulen/-geräten unterstützt werden (z.B. Schlüsselhinterlegung für den Fall, dass ein/e Mitarbeiter/in das Unternehmen verlässt oder wegen Krankheit längere Zeit ausfällt).

Wird innerhalb einer Organisationseinheit der öffentlichen Verwaltung ein und dasselbe Schlüsselpaar zur Verschlüsselung verwendet, so werden die Vertretungsregeln damit umsetzbar und eine Schlüsselhinterlegung innerhalb einer Einheit wird obsolet. [IKTB-181202-1]

Schlüsselwechsel

Die verwendeten Schlüssel sind abhängig von der Häufigkeit ihres Einsatzes, von dem relevanten Bedrohungspotential und der Sicherheit ihrer lokalen Aufbewahrung hinreichend oft präventiv zu wechseln.

Besteht der Verdacht, dass ein verwendeter Schlüssel kompromittiert wurde, so ist dieser Schlüssel nicht mehr zu verwenden und alle Beteiligten sind zu informieren. Bereits mit diesem Schlüssel verschlüsselte Informationen sind zu entschlüsseln und mit einem anderen Schlüssel zu verschlüsseln.

Außerbetriebnahme

Nicht mehr benötigte Schlüssel (z.B. Schlüssel, deren Gültigkeitsdauer abgelaufen ist) sind auf sichere Art zu löschen bzw. zu vernichten (z.B. durch mehrfaches Löschen/Überschreiben und/oder mechanische Zerstörung des Datenträgers).

Auf Produkte mit unkontrollierbarer Schlüsselablage sollte generell verzichtet werden.

SYS 11.8 Einsatz elektronischer Signaturen

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

Elektronische Signaturen stellen ein Pendant zur eigenhändigen Unterschrift für digitale Dateien und Nachrichten dar.

Sie leisten im Wesentlichen zwei Aufgaben:

- *Authentifizierung:*
  Es kann eindeutig verifiziert werden, ob eine bestimmte Person eine bestimmte elektronische Signatur erzeugt hat.
- *Überprüfung der Integrität der signierten Daten:*
  Es ist eindeutig überprüfbar, ob die Daten, an die eine elektronische Signatur angehängt wurde, identisch sind mit den Daten, die tatsächlich signiert wurden.

Elektronische Signaturen gewährleisten *nicht* die Vertraulichkeit von Daten, hierzu sind zusätzliche Verschlüsselungsmaßnahmen erforderlich.

Der Einsatz elektronischer Signaturen empfiehlt sich vor allem in offenen Systemen, in denen a priori kein gegenseitiges Vertrauen zwischen den Kommunikationsteilnehmern vorausgesetzt werden kann, aber verbindliche, authentische Kommunikation erforderlich ist.

Für Behörden wird im Bereich der elektronischen Signaturen die Amtssignatur mit entsprechender Bildmarke verwendet [IKTB-090204-03], [IKTB-240304-03].

Der rechtliche Rahmen für die Erstellung und Verwendung digitaler Signaturen sowie die Erbringung von Signatur- und Zertifizierungsdiensten wird in Österreich durch das Bundesgesetz über elektronische Signaturen - Signaturgesetz - (SigG), BGBl. I Nr. 190/1999 i.d.g.F. geregelt. Dieses sowie die zugehörige Signaturverordnung (SigVO), BGBl. II Nr. 30/2000 i.d.g.F. ist am 1.1.2000 in Kraft getreten.

Das Signaturgesetz regelt u.a.:

- die Rechtswirkungen elektronischer und sicherer elektronischer Signaturen,
- die Tätigkeit der Zertifizierungsanbieter,
- die Aufsicht,
- technische Sicherheitserfordernisse,
- Rechte und Pflichten der Anwender/innen sowie
- die Frage der Anerkennung ausländischer Zertifikate.

Nähere Anforderungen an die technischen Komponenten und Verfahren etc. werden in der Signaturverordnung geregelt.

Aufsichtsstelle ist lt. §13 Signaturgesetz (SigG), BGBl. I Nr. 190/1999 i.d.g.F. die Telekom-Control-Kommission (§110 Telekommunikationsgesetz (TKG), BGBl. I Nr. 100/1997 i.d.g.F.), die sich bei der Durchführung der Aufsicht der Rundfunk und Telekom Regulierungs-GmbH (RTR) [Anmerkung: früher: Telekom Control GmbH] (§108 Telekommunikationsgesetz (TKG), BGBl. I Nr. 100/1997 i.d.g.F.) bedienen kann.

Als erste Bestätigungsstelle lt. §19 Signaturgesetz (SigG), BGBl. I Nr. 190/1999 i.d.g.F. wurde durch Verordnung des Bundeskanzlers vom 2.2.2000 der Verein “Zentrum für sichere Informationstechnologie - Austria (A-SIT)” (Verordnung - A-Sit, BGBl. II Nr. 31/2000 i.d.g.F.) anerkannt.

Adressen und Homepages s. Anhang D.

SYS 11.9 Zertifizierungsdienste

Relevanz: Umsetzung/Wartung; Anwender/innen;

Zertifikate können einerseits zur Verschlüsselung aber andererseits auch zur Authentisierung verwendet werden. Demnach unterscheiden sich auch die Vorgaben und Anforderungen an die ausstellenden Zertifizierungsdienste.

Im Rahmen des IKT-Board Beschlusses vom 11.März 2003 [IKTB-110303-1] wurde die Kennzeichnung von Sicherheitszertifikaten beschlossen. Zur eindeutigen Erkennung von Zertifikaten für Signatur und Server wurde der Object Identifier für .gv.at mit der Arbeitsgruppe der Länder abgestimmt. Zur Stärkung des Vertrauens und zur nachweisbaren Sicherheit wird empfohlen, die Server für Anwendungen des E-Government automatisiert erkennbar zu machen. Dies erfordert die Anwendung der "Richtlinien für Zertifikate für das E-Government" [IKT-ZERT]. Diese Kennung wurde auch im internationalen Kennungsschema (Zertifikatsattribute) festgelegt.

Im IKT-Board Beschluss vom 3.Mai 2005 [IKTB-030505-01-] werden für Anwendungen in der Bundesverwaltung je nach Anwendungsgebiet drei Arten von Zertifikaten unterschieden.

- Amtssignatur (automatisch ausgehende Erledigungen und Bescheide)
- Signatur mit der Bürgerkarte/Dienstkarte (Identifikation der Organverwalter und gegebenenfalls, wie die Amtssignatur, für individuelle einzelne Erledigungen)
- Signatur im Rahmen des E-Mailverkehrs

Des Weiteren wurde in [IKTB-110303-2] für eine automatisierte Vernetzung von E-Government-Anwendungen ein eindeutiges Kennzeichen für Organisationseinheiten der öffentlichen Verwaltung (VKZ) empfohlen. Da bereits eine Reihe von Schlüsselsystemen für Teilbereiche der öffentlichen Verwaltung besteht, soll ein Überbau über bestehende Systeme geschaffen werden.

Das Kennzeichen soll für folgende Bereiche verwendet werden:

- Portalverbund
- Vernetzung von Verfahrensinformationen
- Verzeichnisdienste
- Elektronische Signatur (Zeichnungsberechtigungen)

Die Verwaltung des Kennzeichens für Teilbereiche der dargestellten Organisationen soll durch diese selbst dezentral erfolgen können.

6 Aufrechterhaltung der Sicherheit im laufenden Betrieb

Der IT-Sicherheitsprozess endet nicht mit der Umsetzung von Maßnahmen. Umfassendes IT-Sicherheitsmanagement beinhaltet nicht zuletzt auch die Aufgabe, die IT-Sicherheit im laufenden Betrieb aufrechtzuerhalten. Ein IT-Sicherheitskonzept ist kein statisches, unveränderbares Dokument, sondern muss stets auf seine Wirksamkeit, Aktualität und die Umsetzung in der täglichen Praxis überprüft werden. Weiters muss eine angemessene Reaktion auf sicherheitsrelevante Ereignisse gewährleistet sein.

Ziel aller Follow-Up-Aktivitäten muss es sein, das erreichte Sicherheitsniveau aufrecht zu erhalten bzw. weiter zu erhöhen. Verschlechterungen der Wirksamkeit von Sicherheitsmaßnahmen - sei es durch eine Veränderung der Bedrohungslage oder durch falsche Verwendung der implementierten Sicherheitsmaßnahmen - sollen erkannt und entsprechende Gegenmaßnahmen eingeleitet werden.

Die Verantwortlichkeiten für diese Aktivitäten müssen im Rahmen der organisationsweiten IT-Sicherheitspolitik bzw. der einzelnen IT-Systemsicherheitspolitiken festgelegt werden. Als Richtlinie kann auch hier gelten, dass die Verantwortung für systemspezifische Maßnahmen bei den einzelnen Bereichs-IT-Sicherheitsbeauftragten liegen sollte, die Verantwortung für organisationsweite IT-Sicherheitsmaßnahmen sowie die Gesamtverantwortung bei der bzw. beim Datenschutz-/IT-Sicherheitsbeauftragten.

Von besonderer Bedeutung für die Aufrechterhaltung oder weitere Erhöhung eines einmal erreichten Sicherheitsniveaus ist eine permanente Sensibilisierung aller betroffenen Mitarbeiter/innen für Fragen der IT-Sicherheit (vgl. dazu auch Kap. Sicherheitssensibilisierung und -schulung).

6.1 Wartung

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

Als vorbeugende Maßnahme, um IT-Systeme vor Störungen zu bewahren, ist die ordnungsgemäße Durchführung von Wartungsarbeiten von besonderer Bedeutung.

Dabei umfasst der Begriff Wartung

im Falle von Hardware (Hardware-Wartung):

- Instandhaltung (vorbeugende Wartung zur Aufrechterhaltung der Betriebstüchtigkeit) und
- Instandsetzung (Behebung von Störungen und Fehlern zur Wiederherstellung der Betriebstüchtigkeit) durch Reparatur und Ersatz schadhafter IT-Komponenten,

im Falle von Software

- die Behebung von Störungen bzw. Hilfe bei deren Umgehung und
- die Beratung der Auftraggeberin bzw. des Auftraggebers beim Einsatz der IT-Komponenten, sowie allenfalls, abhängig von den vertraglichen Vereinbarungen,
- die Behebung von Fehlern,
- die Einrichtung und den Betrieb einer Hotline,
- Weiterentwicklung und notwendige Anpassungen.

Richtlinien für Allgemeine Vertragsbedingungen für die Wartung von IT-Komponenten werden in den AVB-IT [AVB-IT] gegeben. Dort findet sich auch eine Vorgabe für die Klassifizierung von Fehlern und die davon abgeleiteten Maßnahmen. Die AVB-IT sehen vor (s. Anhang C):

Fehlerklasse 1: “kritisch”
Fehlerklasse 2: “schwer”
Fehlerklasse 3: “leicht”
Fehlerklasse 4: “trivial”

BET 1.1 Regelungen für Wartungsarbeiten im Haus

Relevanz: Umsetzung/Wartung; Anwender/innen;

Für Wartungsarbeiten im Hause sind eine Reihe von Vorkehrungen und Regelungen zu treffen, von denen die wichtigsten im Folgenden zusammengefasst werden. Besonderes Augenmerk ist diesen Maßnahmen zu schenken, wenn die Arbeiten durch Externe durchgeführt werden.

- Ankündigung der Maßnahme gegenüber den betroffenen Mitarbeiterinnen und Mitarbeitern.
- Wartungstechniker/innen müssen sich auf Verlangen ausweisen.
- Arbeiten - insbesondere wenn sie von Externen durchgeführt werden - sind so weit zu beaufsichtigen, dass beurteilt werden kann, ob während der Arbeit nicht-autorisierte Handlungen vollzogen werden und ob der Wartungsauftrag ausgeführt wurde.
- Der Zugriff auf Daten durch den/die Wartungstechniker/in ist so weit wie möglich zu vermeiden. Falls erforderlich, d.h. abhängig von den Anforderungen der Informationssicherheitspolitik, sind Speichermedien ev. vorher auszubauen oder zu löschen (nach einer kompletten Datensicherung). Falls das Löschen nicht möglich ist (z.B. auf Grund eines Defektes), sind die Arbeiten durch autorisierte Mitarbeiter/innen genau zu beobachten bzw. es sind besondere vertragliche Vereinbarungen zu treffen.
- Die dem/der Wartungstechniker/in eingeräumten Zutritts- und Zugriffsrechte sind auf das notwendige Minimum zu beschränken und nach den Arbeiten zu widerrufen bzw. zu löschen.
- Nach der Durchführung von Wartungsarbeiten sind - je nach “Eindringtiefe” des Wartungspersonals - Passwort-Änderungen erforderlich. Im PC-Bereich sollte ein Viren-Check durchgeführt werden.
- Die durchgeführten Wartungsarbeiten sind zu dokumentieren (Datum, betroffene IT-Komponenten, Fehlerklasse, Dauer des Ausfalls, Art und Ursache der Störung, Art der Behebung, Name des Wartungstechnikers bzw. der Wartungstechnikerin, ...). Ein Muster für einen entsprechenden Störungsbericht findet sich im Anhang zu den AVB-IT.

Folgende Regelungen sollten vertraglich festgelegt werden (vgl. dazu auch AVB-IT [AVB-IT]):

- Verpflichtung zur Geheimhaltung von Daten und Einhaltung der von der Auftraggeberin bzw. vom Auftraggeber bekannt gegebenen Sicherheitsstandards.
- Einhaltung aller Vorschriften gemäß Datenschutzgesetz in der geltenden Fassung, insbesondere Verpflichtung auf §15 Datenschutzgesetz (DSG 2000), BGBl. I Nr. 165/1999 i.d.g.F..
- Verpflichtung, ersetzte IT-Komponenten so zu bearbeiten, dass die auf ihnen enthaltenen Informationen nicht mehr lesbar sind, oder diese nach Vereinbarung unter Aufsicht zu zerstören. Die erfolgte Löschung oder Zerstörung ist auf Wunsch der Auftraggeberin bzw. des Auftraggebers in jedem Einzelfall schriftlich zu bestätigen.

- Verpflichtung, Daten, die im Rahmen der Wartung extern gespeichert wurden, nach Abschluss der Arbeiten sorgfältig zu löschen.
- Festlegung der Pflichten und Kompetenzen des externen Wartungspersonals.

BET 1.2 Regelungen für externe Wartungsarbeiten

Relevanz: Umsetzung/Wartung;

Zusätzlich zu den in BET 1.1 Regelungen für Wartungsarbeiten im Haus angeführten Maßnahmen, die sinngemäß auch für die Wartung außer Haus gelten, sind eine Reihe von weiteren Maßnahmen zu treffen, die im Folgenden kurz angeführt werden.

Werden IT-Systeme zur Wartung außer Haus gegeben, sind alle vertraulichen oder geheimen Daten, die sich auf Datenträgern befinden, in Abstimmung mit der bestehenden Informationssicherheitspolitik vorher physikalisch zu löschen bzw. die Datenträger zu entfernen. Ist dies nicht möglich, weil auf Grund eines Defekts nicht mehr auf die Datenträger zugegriffen werden kann, sind die mit der Reparatur beauftragten Unternehmen auf die Einhaltung der erforderlichen IT-Sicherheitsmaßnahmen zu verpflichten.

Protokollierung:
Werden Wartungsarbeiten extern durchgeführt, so sollte zusätzlich protokolliert werden:

- welche IT-Systeme oder Komponenten wann an wen zur Reparatur gegeben wurden,
- wer dies veranlasst hat,
- zu welchem Zeitpunkt die Reparatur abgeschlossen sein sollte und
- wann das Gerät wieder zurückgebracht wurde.

Um dies gewährleisten zu können, ist eine Kennzeichnung der IT-Systeme oder Komponenten erforderlich, aus der zum einem hervorgeht, welcher Organisation diese gehören, und zum anderen eine eindeutige Zuordnung innerhalb der Organisation möglich ist.

Weiters ist zu beachten:

- Bei Versand oder Transport der zu reparierenden IT-Komponenten sollte darauf geachtet werden, dass Beschädigungen und Diebstahl vorgebeugt wird. Befinden sich auf den IT-Systemen noch sensitive Informationen, müssen sie entsprechend geschützt transportiert werden, also z.B. in verschlossenen Behältnissen oder durch Kuriere. Weiters müssen Nachweise über den Versand (Begleitzettel, Versandscheine) und den Eingang beim Empfänger bzw. bei der Empfängerin (Empfangsbestätigung) geführt und archiviert werden.
- Bei IT-Systemen, die durch Passwörter geschützt sind, müssen je nach Umfang der Reparaturarbeiten und der Art der Passwortabsicherung alle oder einige Passwörter entweder bekannt gegeben oder auf festgelegte Einstellungen wie “REPARATUR” gesetzt werden, damit die Wartungstechniker/innen auf die Geräte zugreifen können.
- Nach der Rückgabe der IT-Systeme oder Komponenten sind diese auf Vollständigkeit zu überprüfen. *Alle* Passwörter sind zu ändern. PC-Datenträger sind nach der Rückgabe mittels eines aktuellen Viren-Suchprogramms auf Viren zu überprüfen. Alle Dateien oder Programme, die sich auf dem reparierten Gerät befinden, sind auf Integrität zu überprüfen.

BET 1.3 Fernwartung

Relevanz: Umsetzung/Wartung;

Die Fernwartung von IT-Systemen über ein Modem birgt besondere Sicherheitsrisiken. Aus Sicherheitsgründen ist es sinnvoll, auf externe Fernwartung zu verzichten. Ist dies nicht möglich, so sind zusätzliche Sicherungsmaßnahmen unumgänglich.

Das zu wartende IT-System einschließlich des eingesetzten Modems muss die folgenden Sicherheitsfunktionen realisieren:

- Der Aufbau der Verbindung für eine Fernwartung sollte immer vom lokalen IT-System initiiert werden. Dies kann durch Anruf des zu wartenden IT-Systems bei der Fernwartungsstelle oder über einen automatischen Rückruf (Callback) realisiert werden.
- Das externe Wartungspersonal muss sich zu Beginn der Wartung authentisieren. Werden dabei Passwörter unverschlüsselt übertragen, sollten Einmalpasswörter benutzt werden.
- Alle Tätigkeiten bei der Durchführung der Fernwartung müssen auf dem zu wartenden IT-System protokolliert werden.

Darüber hinaus können am zu wartenden IT-System noch weitere Funktionalitäten implementiert werden, wie etwa:

- Verhängen einer Zeitsperre bei fehlerhaften Zugangsversuchen,
- Sperren der Fernwartung im Normalbetrieb und explizite Freigabe für eine genau definierte Zeitspanne,
- Einschränkung der Rechte des Wartungspersonals. Das Wartungspersonal sollte nicht die vollen Administrator-Rechte besitzen, sondern nur auf die Daten und Verzeichnisse Zugriff haben, die aktuell von der Wartung betroffen sind.
- Auf dem IT-System sollte für das Wartungspersonal eine eigene Benutzerkennung existieren, unter der möglichst alle Wartungsarbeiten durchgeführt werden.
- Wird die Verbindung zur Fernwartungsstelle auf irgendeine Weise unterbrochen, so muss der Zugriff auf das System durch einen “Zwangslogout” beendet werden.

Die Fernwartung sollte lokal durch IT-Experten bzw. IT-Expertinnen beobachtet werden. Auch wenn die Fernwartung eingesetzt wird, weil intern das Know-how oder die Kapazität nicht verfügbar ist, kann das Wartungspersonal nicht unbeaufsichtigt gelassen werden (siehe auch BET 1.1 Regelungen für Wartungsarbeiten im Haus). Bei Unklarheiten über die Vorgänge sollte die lokale IT-Expertin bzw. der lokale IT-Experte sofort nachfragen. Es muss jederzeit die Möglichkeit geben, die Fernwartung lokal abzubrechen.

Werden während der Wartung Daten oder Programme auf dem lokalen IT-System angelegt, so muss dies deutlich erkennbar und nachvollziehbar sein, also z.B. darf dies nur in besonders markierten Verzeichnissen oder unter bestimmten Benutzerkennungen erfolgen.

Analog zu BET 1.2 Regelungen für externe Wartungsarbeiten sind auch für Fernwartung mit externem Wartungspersonal vertragliche Regelungen über die Geheimhaltung von Daten zu treffen. Insbesondere ist festzulegen,

- dass Daten, die im Rahmen der Wartung extern gespeichert wurden, nach Abschluss der Arbeiten sorgfältig gelöscht werden,
- dass die Vorschriften des DSG 2000 über den internationalen Datenverkehr (§ 13) (DSG 2000), BGBl. I Nr. 165/1999 i.d.g.F. eingehalten werden,
- welche Pflichten und Kompetenzen das externe Wartungspersonal hat.

BET 1.4 Wartung und administrativer Support von Sicherheitseinrichtungen

Relevanz: Management; Umsetzung/Wartung;

Viele Sicherheitsmaßnahmen erfordern zur Gewährleistung ihrer einwandfreien Funktionsfähigkeit Wartung und administrativen Support. Zu diesen Aufgaben zählen etwa die regelmäßige Auswertung und Archivierung von Protokollen, Backup, Restore und Maintenance von sicherheitsrelevanten Komponenten, die Überprüfung der Parametereinstellungen und eventueller Rechte auf mögliche nicht-autorisierte Änderungen, die Reinitialisierung von Startwerten oder Zählern sowie Updates der Sicherheitssoftware, wenn verfügbar (besonders, aber nicht ausschließlich, im Bereich Virenschutz) u.v.a.m.

Alle Wartungs- und Supportaktivitäten sollten nach einem detailliert festgelegten Plan erfolgen und regelmäßig durchgeführt werden.

Die Wartung von Sicherheitseinrichtungen hat in Abstimmung mit den Verträgen, die mit den Lieferfirmen geschlossen wurden, zu erfolgen und darf nur durch dafür autorisierte Personen vorgenommen werden.

Die Kosten für Wartungs- und Supportaufgaben können im Einzelfall beträchtlich sein und sollten daher bereits bei der Auswahl der Sicherheitsmaßnahmen bekannt sein und in den Entscheidungsprozess mit einfließen.

Um die Aufrechterhaltung eines einmal erreichten Sicherheitsniveaus zu gewährleisten, ist sicherzustellen, dass

- die erforderlichen finanziellen und personellen Ressourcen zur Wartung von IT-Sicherheitseinrichtungen zur Verfügung stehen,
- organisatorische Regelungen existieren, die die Aufrechterhaltung der IT-Sicherheitsmaßnahmen im laufenden Betrieb ermöglichen und unterstützen,
- die Verantwortungen im laufenden Betrieb klar zugewiesen werden,
- die Maßnahmen regelmäßig daraufhin geprüft werden, ob sie wie beabsichtigt funktionieren und
- Maßnahmen verstärkt werden, falls sich neue Schwachstellen zeigen.

Alle Wartungs- und Supportaktivitäten im IT-Sicherheitsbereich sollten protokolliert werden. Der regelmäßigen Auswertung dieser Protokolle kommt besondere Bedeutung für die gesamte IT-Sicherheit zu.

6.2 Security Compliance Checking und Monitoring

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

Zur Gewährleistung eines angemessenen und gleich bleibenden Sicherheitsniveaus ist dafür Sorge zu tragen, dass alle Maßnahmen so eingesetzt werden, wie es im IT-Sicherheitskonzept und im IT-Sicherheitsplan vorgesehen ist. Dies muss für alle IT-Systeme, -Projekte und Applikationen sichergestellt sein.

Weiters sind die getroffenen Maßnahmen regelmäßig auf Übereinstimmung mit gesetzlichen und betrieblichen Vorgaben zu überprüfen.

Security Compliance Checks sollten zu folgenden Zeitpunkten bzw. bei Eintreten folgender Ereignisse durchgeführt werden:

- *für neue IT-Systeme oder relevante neue Anwendungen:*
  nach der Implementierung
- *für bereits in Betrieb befindliche IT-Systeme oder Applikationen:*
  nach einer bestimmten, in der IT-Systemsicherheitspolitik vorzugebenden Zeitspanne (z.B. jährlich) sowie bei signifikanten Änderungen.

BET 2.1 Einhaltung von rechtlichen und betrieblichen Vorgaben

Relevanz: Umsetzung/Wartung; Anwender/innen;

Es ist dafür Sorge zu tragen, dass alle gesetzlichen und betrieblichen Vorgaben eingehalten werden.

Dazu ist laufend zu überprüfen,

- ob die Systeme allen gesetzlichen und betrieblichen Vorgaben entsprechen (insbesondere Beachtung neuer gesetzlicher Bestimmungen!) sowie
- ob die Vorgaben im laufenden Betrieb auch tatsächlich umgesetzt und eingehalten werden.

Wichtige Vorgaben ergeben sich beispielsweise aus:

- Datenschutzgesetz 2000 (DSG2000), BGBl. I Nr. 165/1999 i.d.g.F.
- Einhaltung von gesetzlichen Aufbewahrungs- und Löschfristen
- Urheberrecht und Wettbewerbsgesetze (etwa Verhindern von unbefugtem Kopieren von Software)

sowie

- 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. Gesicherte Anbindung an Fremdnetze (Internet-Sicherheit))

BET 2.2 Überprüfung auf Einhaltung der Sicherheitspolitiken

Relevanz: Management; Umsetzung/Wartung;

Es sollte regelmäßig überprüft werden,

- ob alle Sicherheitsmaßnahmen und -vorgaben, die in der organisationsweiten IT-Sicherheitspolitik sowie in den relevanten IT-Systemsicherheitspolitiken vorgesehen sind, vollständig und korrekt umgesetzt sind,
- der korrekte Einsatz der implementierten Sicherheitsmaßnahmen gewährleistet ist (Stichproben!) und
- die organisatorischen Sicherheitsvorgaben im täglichen Betrieb eingehalten und akzeptiert werden.

Diese Überprüfungen erfordern profundes Know-how über die zu prüfenden Systeme und die eingesetzten Sicherheitsmaßnahmen sowie mögliche Bedrohungen und sollten daher nur von erfahrenen und vertrauenswürdigen Personen durchgeführt werden.

Im Folgenden werden einige Maßnahmen aus dem Bereich Security Compliance Checking detaillierter behandelt, eine vollständige Auflistung ist in diesem Rahmen aber nicht möglich und sinnvoll, die Vorgehensweise muss vielmehr speziell auf das betreffende System abgestimmt werden.

BET 2.3 Auswertung von Protokolldateien

Relevanz: Umsetzung/Wartung;

Die Protokollierung sicherheitsrelevanter Ereignisse ist als Sicherheitsmaßnahme nur wirksam, wenn die protokollierten Daten auch ausgewertet werden. Daher sind Protokolldateien in regelmäßigen Abständen durch eine Revisorin bzw. einen Revisor auszuwerten.

Ist es technisch nicht möglich, die Rolle einer unabhängigen Revisorin bzw. eines unabhängigen Revisors für Protokolldateien zu implementieren, kann die Auswertung der Protokolldateien auch durch die Systemadministration erfolgen. Für diesen Fall bleibt zu beachten, dass damit eine Kontrolle der Tätigkeiten der Systemadministration nur schwer möglich ist. Das Ergebnis der Auswertung sollte daher dem/der Datenschutz-/IT-Sicherheitsbeauftragten, dem/der Applikations-/Projektverantwortlichen oder einem/einer anderen besonders zu bestimmenden Mitarbeiter/in vorgelegt werden.

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

Beinhalten die Protokolldateien personenbezogene Daten, so ist sicherzustellen, dass diese Daten nur zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes verwendet werden dürfen (vgl. dazu Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999 i.d.g.F.).

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

- Liegen die Zeiten des An- und Abmeldens außerhalb der Arbeitszeit (Hinweis auf Manipulationsversuche)?
- Häufen sich fehlerhafte Anmeldeversuche (Hinweis auf den Versuch, Passworte zu erraten)?
- Häufen sich unzulässige Zugriffsversuche (Hinweis auf Versuche zur Manipulation)?
- Gibt es auffällig große Zeitintervalle, in denen keine Protokolldaten aufgezeichnet wurden (Hinweis auf eventuell gelöschte Protokollsätze)?
- Ist der Umfang der protokollierten Daten zu groß (eine umfangreiche Protokolldatei erschwert das Auffinden von Unregelmäßigkeiten)?
- Gibt es auffällig große Zeitintervalle, in denen anscheinend kein Benutzerwechsel stattgefunden hat (Hinweis darauf, dass das konsequente Abmelden nach Arbeitsende nicht vollzogen wird)?

Weiters ist zu beachten:

- Müssen regelmäßig umfangreiche Protokolldateien ausgewertet werden, ist es sinnvoll, ein Werkzeug zur Auswertung zu benutzen. Dieses Werkzeug sollte wählbare Auswertungskriterien zulassen und besonders kritische Einträge (z.B. mehrfacher fehlerhafter Einlog-Versuch) hervorheben.
- Besonders sicherheitskritische Protokolldaten sollten unter Anwendung des Vier-Augen-Prinzips ausgewertet werden.
- Die Befugnisse der Systemadministration sind klar festzulegen; es ist dafür Sorge zu tragen, dass auch die Systemadministration ausreichend kontrolliert werden kann.
- Auffälligkeiten sind dem IT-Sicherheitsmanagement zu berichten (vgl. auch Incident Handling)

BET 2.4 Kontrolle bestehender Verbindungen

Relevanz: Umsetzung/Wartung;

Alle Netzwerkkomponenten sind einer (zumindest stichprobenartigen) Sichtprüfung zu unterziehen.

Dabei ist auf folgende Punkte zu achten:

- Spuren von gewaltsamen Öffnungsversuchen an verschlossenen Verteilern,
- Aktualität der im Verteiler befindlichen Dokumentation,
- Übereinstimmung der tatsächlichen Beschaltungen und Rangierungen mit der Dokumentation,
- Unversehrtheit der Kurzschlüsse und Erdungen nicht benötigter Leitungen und
- unzulässige Einbauten/Veränderungen.

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

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

Weiters ist zu beachten:

- Der Meldeweg für festgestellte Unregelmäßigkeiten ist festzulegen.
- Festgestellte Unregelmäßigkeiten müssen dokumentiert und verfolgt werden.
- Es ist festzulegen, wer für die Beseitigung von Unregelmäßigkeiten verantwortlich ist.

BET 2.5 Durchführung von Sicherheitskontrollen in Client-Server-Netzen

Relevanz: Umsetzung/Wartung; Anwender/innen;

Die folgenden Punkte sollten - abhängig von den Sicherheitsanforderungen und den technischen Möglichkeiten des betrachteten Systems - auf Server-Ebene regelmäßig auf Einhaltung und Effektivität kontrolliert werden.

- *System-Sicherheits-Einstellungen* Die Korrektheit aller sicherheitsrelevanten Systemeinstellungen ist regelmäßig zu kontrollieren.
- *Benutzung von privilegierten Benutzeraccounts* Die Benutzung privilegierter Benutzeraccounts, also von Accounts mit erweiterten Rechten und Berechtigungen wie etwa der Systemadministration, ist regelmäßig durch Überprüfung der entsprechenden Protokolleinträge zu überprüfen.
- *Fehlgeschlagene Zugriffsversuche (Berechtigungsverstöße)* Sofern Zugriffe auf Dateien aufgezeichnet werden, ist das Protokoll zumindest wöchentlich, bei Bedarf auch öfter, auf das Vorliegen fehlgeschlagener Zugriffsversuche zu überprüfen. Werden Berechtigungsverstöße festgestellt, ist die Ursache zu ermitteln.
- *Systemintegrität* Die Systemintegrität ist regelmäßig zu überprüfen; insbesondere sind die Daten der letzten Veränderung sowie die Zugriffsrechte der wichtigen Systemdateien zu überprüfen und mit den Werten, die unmittelbar nach der Installation des Systems sowie bei der jeweils vorherigen Überprüfung gegeben waren, zu vergleichen.
- *Unbenutzte Benutzeraccounts* Es ist sicherzustellen, dass die Berechtigungen ehemaliger Benutzer/innen sofort deaktiviert und nach einer geeigneten Übergangszeit (ca. ½ Jahr) vom System gelöscht werden. Die Liste der definierten Benutzer/innen ist regelmäßig zu überprüfen, um sicherzustellen, dass nur aktive Beschäftigte auf dem System arbeiten.
- *Benutzer- und Gruppenberechtigungen* Es sollte überprüft werden, ob Programmierer/innen Zugriff auf Produktionsbibliotheken haben. Weiterhin ist die Gruppenmitgliedschaft zu überprüfen, wenn sich die Mitgliedschaft oder Aufgabe einer Benutzerin oder eines Benutzers ändert, und es sollte regelmäßig überprüft werden, ob Anhäufungen von Benutzerrechten existieren. Die Systemadministration sollte außerdem in regelmäßigen Abständen die Benutzer/innen mit Spezialberechtigungen mit den organisatorischen Vorgaben abgleichen.
- *Berechtigungskontrolle* Es ist sicherzustellen, dass die Eigentümer/innen von Dateien und Verzeichnissen ihre Verpflichtung verstehen, anderen Benutzerinnen und Benutzern nur dann Zugriff zu gewähren, wenn dies erforderlich ist.

Es sind Prozeduren bzw. Verfahren zu entwickeln für den Fall, dass Abweichungen von den festgelegten Einstellungen auftreten. Diese Prozeduren müssen folgende Punkte enthalten:

- wer wird wann informiert,
- Begründung für die eventuelle Wahl abweichender Einstellungen und Angabe, ob hierdurch möglicherweise eine Sicherheitslücke entsteht,
- Schritte zur Behebung der Sicherheitslücke,
- Schritte zur Identifizierung der Ursache der Sicherheitslücke.

BET 2.6 Kontrollgänge

Relevanz: Umsetzung/Wartung;

Eine Maßnahme kann nur so gut wirken, wie sie auch tatsächlich umgesetzt wird. Kontrollgänge bieten ein einfaches und wirksames Mittel, die Umsetzung von Maßnahmen und die Einhaltung von Auflagen und Anweisungen zu überprüfen.

Die Kontrollgänge sollen nicht dem Finden von Tätern bzw. Täterinnen dienen, um diese zu bestrafen. Sinn der Kontrollen soll es in erster Linie sein, erkannte Nachlässigkeiten möglichst sofort zu beheben (Fenster zu schließen, unbefugtes Offenhalten von Türen in Sicherheitsbereichen zu verhindern, Unterlagen in Aufbewahrung zu nehmen etc.). In zweiter Linie können Ursachen für diese Nachlässigkeiten erkannt und evtl. in der Zukunft vermieden werden.

Die Kontrollgänge sollten durchaus auch während der Dienstzeit erfolgen und zur Information der Mitarbeiter/innen über das Wie und Warum von Regelungen genutzt werden. So werden sie von allen Beteiligten eher als Hilfe denn als Gängelung angesehen.

BET 2.7 Fortlaufende Überwachung der IT-Systeme (Monitoring)

Relevanz: Umsetzung/Wartung;

Monitoring ist eine laufende Aktivität mit dem Ziel, zu überprüfen, ob das IT-System, seine Benutzer/innen und die Systemumgebung das im IT-Sicherheitsplan festgelegte Sicherheitsniveau beibehalten. Dazu wird ein Plan für eine kontinuierliche Überwachung der IT-Systeme im täglichen Betrieb erstellt.

Wo technisch möglich und sinnvoll, sollte das Monitoring durch die Ermittlung von Kennzahlen unterstützt werden, die eine rasche und einfache Erkennung von Abweichungen von den Sollvorgaben ermöglichen. Solche Kennzahlen können beispielsweise die Systemverfügbarkeit, die Zahl der Hacking-Versuche über Internet oder die Wirksamkeit des Passwortmechanismus betreffen.

Da alle Änderungen der potentiellen Bedrohungen, Schwachstellen, zu schützenden Werte und Sicherheitsmaßnahmen möglicherweise signifikante Auswirkungen auf das Gesamtrisiko haben können, ist eine fortlaufende Überwachung dieser Bereiche erforderlich. Dies sind insbesondere:

Wert der zu schützenden Objekte:

Sowohl die Werte von Objekten als auch, daraus resultierend, die Sicherheitsanforderungen an das Gesamtsystem können im Laufe des Lebenszyklus eines IT-Projektes oder -Systems erheblichen Änderungen unterliegen.

Mögliche Gründe dafür sind eine Änderung der IT-Sicherheitsziele, die Installation neuer Applikationen oder die Verarbeitung von Daten einer höheren Sicherheitsklasse auf existierenden Systemen oder Änderungen in der HW-Ausstattung.

Bedrohungen und Schwachstellen:

Organisatorisch oder technologisch (hier insbesondere durch neue Technologien in der Außenwelt) bedingt können sowohl die Wahrscheinlichkeit des Eintritts einer Bedrohung als auch die potentielle Schadenshöhe im Laufe der Zeit starken Änderungen unterliegen und sind daher regelmäßig zu evaluieren.

Es ist wichtig, neue potentielle Schwachstellen so früh wie möglich zu erkennen und abzusichern.

Sicherheitsmaßnahmen:

Die Wirksamkeit der implementierten Sicherheitsmaßnahmen ist laufend zu überprüfen.

Es ist sicherzustellen, dass sie einen angemessenen und den Vorgaben der IT-Systemsicherheitspolitik entsprechenden Schutz bieten. Änderungen in den Werten der bedrohten Objekte, den Bedrohungen und den Schwachstellen, aber auch durch den Einsatz neuer Technologien, können die Wirksamkeit der Sicherheitsmaßnahmen nachhaltig beeinflussen.

Durch ein kontinuierliches Monitoring soll die Leitung der Institution ein klares Bild darüber bekommen, was durch die IT-Sicherheitsmaßnahmen erreicht wurde (Soll-/Ist-Vergleich), und ob die Ergebnisse den Sicherheitsanforderungen der Institution genügen. Weiters soll eine Beurteilung des Erfolges der einzelnen Maßnahmen erfolgen.

6.3 Change Management

Relevanz: Management; Umsetzung/Wartung;

Aufgabe des Change Managements ist es, neue Sicherheitsanforderungen zu erkennen, die sich aus Änderungen am IT-System ergeben. Sind signifikante Hardware- oder Softwareänderungen in einem IT-System geplant, so sind die Auswirkungen auf die Gesamtsicherheit des Systems zu untersuchen.

Im Rahmen des Konfigurationsmanagements ist sicherzustellen, dass Änderungen an einem IT-System nicht zu einer Verringerung der Effizienz von einzelnen Sicherheitsmaßnahmen und damit einer Gefährdung der Gesamtsicherheit führen.

BET 3.1 Reaktion auf Änderungen am IT-System

Relevanz: Management; Umsetzung/Wartung;

Es ist dafür Sorge zu tragen, dass auf alle sicherheitsrelevanten Änderungen angemessen reagiert wird.

Dazu gehören zum Beispiel:

- Änderungen des IT-Systems (neue Applikationen, neue Hardware, neue Netzwerkverbindungen, ...),
- Änderungen in der Aufgabenstellung oder in der Wichtigkeit der Aufgabe für die Institution,
- Änderungen in der Benutzerstruktur (neue, etwa externe oder anonyme, Benutzergruppen),
- räumliche Änderungen, z.B. nach einem Umzug,
- Änderungen in der Bewertung der eingesetzten IT, der notwendigen Vertraulichkeit, Integrität oder Verfügbarkeit und
- Änderungen bei Bedrohungen oder Schwachstellen.

Alle Änderungen und die dazugehörigen Entscheidungsgrundlagen sind schriftlich zu dokumentieren.

Abhängig von der Bedeutung des Systems und dem Grad der Änderung kann eine neuerliche Durchführung vorangegangener Aktivitäten im Sicherheitsprozess erforderlich werden. Dies soll das folgende, dem 1.Teil des vorliegenden Handbuches, Kap. 2 [KIT S01], entnommene Bild verdeutlichen:

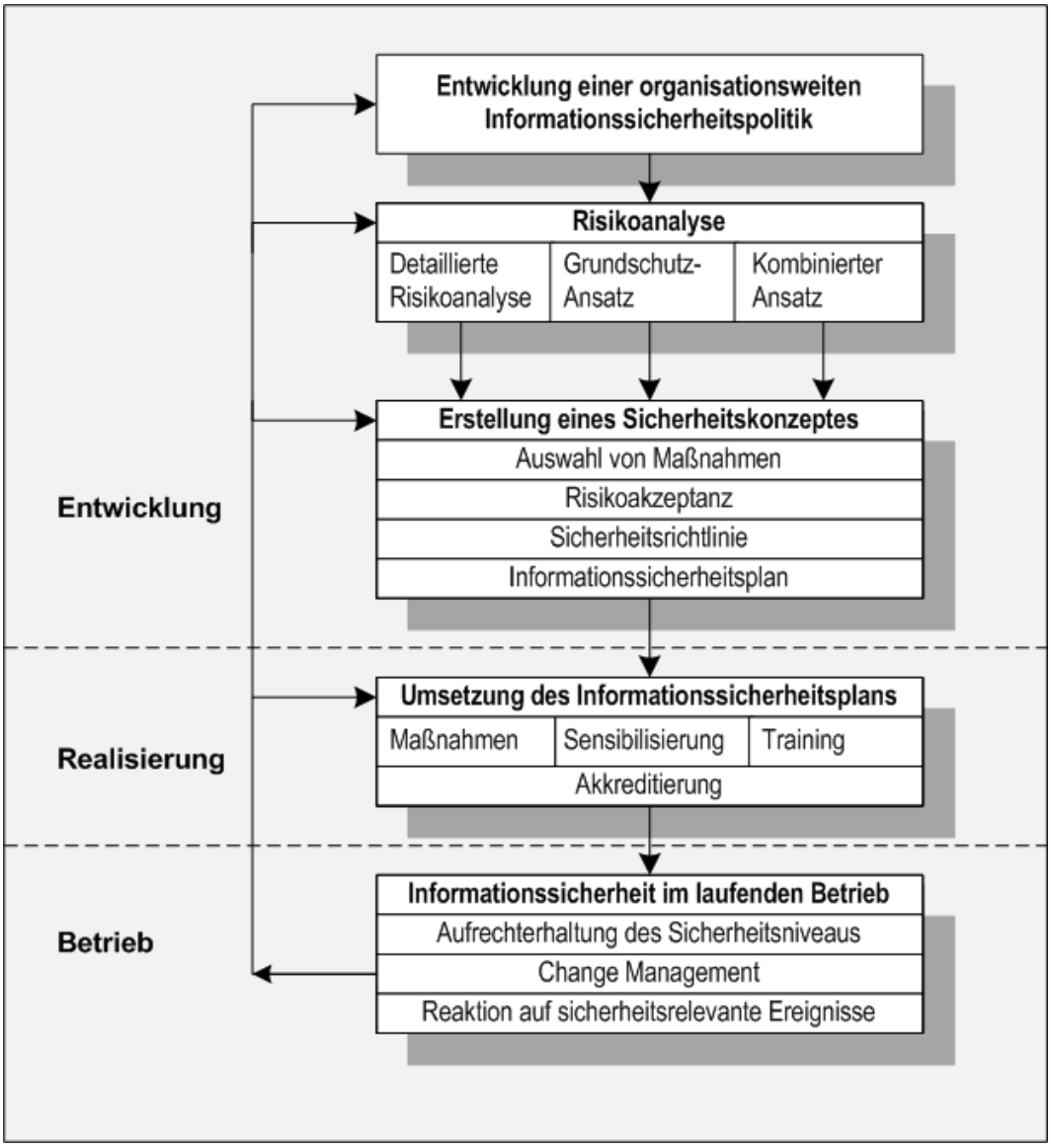

Abbildung 7: Aktivitäten im Rahmen des Informationssicherheitsmanagements

Eine Änderung des IT-Systems oder seiner Einsatzbedingungen kann also

- Änderungen in der Umsetzung des Informationssicherheitsplans
- die Erstellung eines neuen Sicherheitskonzeptes
- eine neue Risikoanalyse oder sogar
- die Überarbeitung der organisationsweiten Informationssicherheitspolitik

erforderlich machen.

BET 3.2 Software-Änderungskontrolle

Relevanz: Umsetzung/Wartung;

Software-Änderungskontrolle (Software Change Control) ist der Teil des Change Managements, der sich auf die Gewährleistung der Integrität von Software bei Änderungen bezieht.

- Es ist sicherzustellen, dass nur abgenommene und freigegebene Software installiert wird (vgl. ENT 1.7 Abnahme und Freigabe von Software),
- die freigegebene Software(version) nur unverändert installiert werden kann (vgl. ENT 1.9 Sicherstellen der Integrität von Software),
- Installation und Konfiguration entsprechend den Installationsanweisungen erfolgen (vgl. ENT 1.8 Installation und Konfiguration von Software) und
- Standardsoftware einer Lizenzverwaltung und Versionskontrolle unterliegt (vgl. ENT 1.10 Lizenzverwaltung und Versionskontrolle von Standardsoftware)

Für komplexe Eigenentwicklungen empfiehlt sich die Erstellung eines "Software-Pflege- und Änderungskonzeptes" (SWPÄ-Konzept, vgl. BET 3.3 Software-Pflege- und -Änderungskonzept (SWPÄ-Konzept)).

BET 3.3 Software-Pflege- und -Änderungskonzept (SWPÄ-Konzept)

Relevanz: Umsetzung/Wartung;

Unter Software-Pflege und -Änderung sind alle Maßnahmen zu verstehen, die ergriffen werden,

- um eine zur Benutzung freigegebene Programmausstattung funktionsfähig zu erhalten, ohne dass Spezifikationen geändert oder erweitert werden (Software-Pflege),
- um eine Änderung oder Erweiterung der Spezifikationen in einer zur Benutzung freigegebenen Programmausstattung zu berücksichtigen (Software-Änderung).

(Definition lt. [IT-BVM]) - In den [IT-BVM] werden die inhaltlichen Anforderungen an ein SWPÄ-Konzept gegeben.

Diese umfassen u.a.

- Beschreibung der SWPÄ-Organisation (SWPÄ-Team, Aufgaben und Verantwortlichkeiten)
- Beschreibung des SWPÄ-Prozesses (Beantragung, Analyse und Klassifikation von Änderungen, Konfigurationsverwaltung, Verteilung von Datenträgern, Installation)
- Planung der SWPÄ-Bereitschaft (Schaffung der personellen und technischen Voraussetzungen, Ausbildung, entwicklungsbegleitende Maßnahmen)

6.4 Reaktion auf sicherheitsrelevante Ereignisse (Incident Handling)

Relevanz: Management; Umsetzung/Wartung;

Unter sicherheitsrelevanten Ereignissen sind alle Vorkommnisse zu verstehen, die Sicherheitsprobleme aufdecken oder nach sich ziehen. Dazu zählen etwa Einbruchsversuche in das System (Hacking), das Auftreten von Viren oder das Ausspähen von Passwörtern.

Auch bei Vorhandensein wirksamer Sicherheitsmaßnahmen und eines hohen Sicherheitsniveaus ist das Auftreten solcher Ereignisse nicht gänzlich zu verhindern. Jede Institution muss ein vitales Interesse daran haben, dass auf sicherheitsrelevante Ereignisse so schnell und effektiv wie möglich reagiert wird. Darüber hinaus können und sollen Informationen über derartige Vorkommnisse der Vorbeugung künftiger Schadensereignisse dienen.

Daher sind alle Mitarbeiter/innen über ihre Verantwortung bei Eintreten sicherheitsrelevanter Ereignisse, die vorgesehenen Meldewege und zu setzenden Aktionen zu unterrichten.

BET 4.1 Erstellung eines Incident Handling Plans

Relevanz: Management; Umsetzung/Wartung;

Zur Sicherstellung einer angemessenen Behandlung von sicherheitsrelevanten Ereignissen ist es empfehlenswert, detaillierte Vorgaben in Form eines " Incident Handling Planes " (IHP) auszuarbeiten und allen Mitarbeiterinnen und Mitarbeitern bekannt zu machen.

Der IHP legt in schriftlicher Form und verbindlich fest:

- wie auf sicherheitsrelevante Ereignisse zu reagieren ist,
- Verantwortlichkeiten für die Meldung bzw. Untersuchung sicherheitsrelevanter Vorfälle,
- die einzuhaltenden Meldewege,
- ob und in welcher Form schadensbehebende oder schadensvorbeugende Maßnahmen zu ergreifen sind und die Verantwortlichkeiten hierfür,
- die Protokollierung und Dokumentation sicherheitsrelevanter Vorfälle sowie
- die Ausbildung von Personen, die sicherheitsrelevante Vorfälle behandeln bzw. Gegenmaßnahmen treffen müssen.

Darüber hinaus muss auch geregelt sein, wer für Kontakte mit anderen Organisationen verantwortlich ist, um Informationen über bekannte Sicherheitslücken einzuholen oder um Informationen über aufgetretene Sicherheitslücken weiterzugeben. Es ist dafür Sorge zu tragen, dass evtl. mitbetroffene Stellen schnellstens informiert werden.

BET 4.2 Einrichtung von CERTs

Relevanz: Management;

Ein CERT (Computer Emergency Response Team) ist eine Gruppe von Personen, die

- die Ursachen und Auswirkungen von sicherheitsrelevanten Vorfällen untersucht,
- Vorfälle aufzeichnet und auswertet,
- Hilfestellung bei der Behandlung von sicherheitsrelevanten Vorfällen gibt.

Ob innerhalb einer Institution ein (oder ev. auch mehrere) CERT(s) eingerichtet wird, hängt in erster Linie von der Größe dieser Institution und der erwarteten Anzahl und Schwere der Vorfälle ab. In kleineren Institutionen wird eine Behandlung und Aufzeichnung der sicherheitsrelevanten Vorfälle durch eine in der IT-Sicherheitspolitik zu benennende Person - dies wird im Allgemeinen der/die Datenschutz-/IT-Sicherheitsbeauftragte sein - angemessen sein, in großen oder besonders sicherheitssensiblen Institutionen ist die Einrichtung von CERTs zu empfehlen.

Darüber hinaus besteht auch die Möglichkeit, institutionsübergreifende CERTs einzurichten, die es ermöglichen, Daten über sicherheitsrelevante Vorfälle auszutauschen und damit auf eine breitere Information, etwa über die Häufigkeit des Eintretens von Bedrohungen oder über neue Angriffe, zurückzugreifen. In diesem Fall sollten gemeinsame Protokollierungsvorgaben, Formulare, Bewertungsmethoden und Datenbankstrukturen erarbeitet werden, die den Austausch und die Auswertung von Information erleichtern.

7 Disaster Recovery und Business Continuity Planung

Ziel der Disaster Recovery Planung ist es, die Verfügbarkeit der wichtigsten Applikationen und IT-Systeme innerhalb eines definierten Zeitraumes zu gewährleisten sowie Vorkehrungen zur Schadensbegrenzung im Katastrophen- bzw. Notfall zu treffen.

Weiter gefasst ist der Begriff der Business Continuity Planung, der über die Disaster Recovery Planung hinaus auch alle Präventivmaßnahmen zur Vermeidung eines K-Falles umfasst. Ziel der Business Continuity Planung ist es, die Verfügbarkeit der wichtigsten Applikationen und Systeme innerhalb eines definierten Zeitraumes zu gewährleisten sowie Vorkehrungen zur Schadensbegrenzung im Katastrophenfall zu treffen (”Gewährleistung eines kontinuierlichen Geschäftsbetriebes”).

Disaster Recovery Planung stellt also ein Teilgebiet der Business Continuity Planung dar, in der Praxis werden beide Begriffe allerdings manchmal auch synonym verwendet. Oft findet man für Disaster Recovery Planung auch die Bezeichnung “Notfallvorsorge” sowie die eher älteren und heute seltener verwendeten Begriffe “Katastrophenplanung” (”K-Planung”) und “Backup-Planung” (hier besteht Verwechslungsgefahr mit dem “Backup” im Sinne einer regelmäßigen Datensicherung). Contingency Planning (”Ausweichplanung”) beschäftigt sich in erster Linie mit der Ausweichplanung für ev. Notfälle und stellt damit ein Teilgebiet der Disaster Recovery Planung dar (vgl. dazu Abschnitt 7.2 Strategie und Planung).

Im Rahmen der IT-Sicherheitspolitik sind die Verfügbarkeitsklassen für IT-Anwendungen und die diesen Anwendungen zugrunde liegenden IT-Systeme zu definieren (siehe BCP 2.1). Die Business Continuity Planung selbst ist nicht Bestandteil der IT-Sicherheitspolitik, sondern muss in den entsprechen den weiteren Aktivitäten erfolgen.

7.1 Datensicherung

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

Unabdingbare Voraussetzung für jeden Business Continuity Plan ist die Planung und Durchführung einer ordnungsgemäßen Datensicherung.

BCP 1.1 Regelmäßige Datensicherung

Relevanz: Umsetzung/Wartung; Anwender/innen;

Zur Vermeidung von Datenverlusten müssen regelmäßige Datensicherungen durchgeführt werden. In den meisten Rechnersystemen können diese weitgehend automatisiert erfolgen. Es sind Regelungen zu treffen, welche Daten von wem wann gesichert werden. Empfehlenswert ist die Erstellung eines Datensicherungskonzeptes (vgl. BCP 1.2 Entwicklung eines Datensicherungskonzeptes).

Abhängig von der Menge und Wichtigkeit der laufend neu gespeicherten Daten und vom möglichen Schaden bei Verlust dieser Daten ist Folgendes festzulegen:

- *Umfang der zu sichernden Daten:*
  Am einfachsten ist es, Partitionen bzw. Verzeichnisse festzulegen, die bei der regelmäßigen Datensicherung berücksichtigt werden. Eine geeignete Differenzierung kann die Übersichtlichkeit vergrößern sowie Aufwand und Kosten sparen helfen. Z.B.: Sicherung der selbsterstellten Dateien und der individuellen Konfigurationsdateien.
- *Zeitintervall:*
  z.B. täglich, wöchentlich, monatlich
- *Zeitpunkt:*
  z.B. nachts, freitags abends
- *Anzahl der aufzubewahrenden Generationen:*
  z.B. Bei täglicher Komplettsicherung werden die letzten sieben Sicherungen aufbewahrt, außerdem die Freitagabend-Sicherungen der letzten zwei Monate.
- *Speichermedien (abhängig von der Datenmenge):*
  z.B. Bänder, Kassetten, Disketten, Spiegelplatte,
- Wiederaufbereitung der Datenträger (Löschung vor Wiederverwendung)
- Zuständigkeit für die Durchführung (Systemadministration, Benutzer/in)
- Zuständigkeit für die Überwachung der Sicherung, insbesondere bei automatischer Durchführung (Fehlermeldungen, verbleibender Platz auf den Speichermedien)
- Dokumentation der erstellten Sicherungen (Datum, Art der Durchführung der Sicherung, gewählte Parameter, Beschriftung der Datenträger)

Wegen des großen Aufwands können Komplettsicherungen in der Regel höchstens einmal täglich durchgeführt werden. Die seit der letzten Sicherung erstellten Daten können nicht wiedereingespielt werden. Daher und zur Senkung der Kosten sollen zwischen den Komplettsicherungen regelmäßig inkrementelle Sicherungen durchgeführt werden, das heißt, nur die seit der letzten Komplettsicherung neu erstellten Daten werden gesichert. Werden zwischen zwei Komplettsicherungen mehrere inkrementelle Sicherungen durchgeführt, können auch jeweils nur die seit der letzten inkrementellen Sicherung neu erstellten Daten gesichert werden.

Eine inkrementelle Sicherung kann häufiger erfolgen, zum Beispiel sofort nach Erstellung wichtiger Dateien oder mehrmals täglich. Die Vereinbarkeit mit dem laufenden Betrieb ist sicherzustellen.

Für eingesetzte Software ist in der Regel die Aufbewahrung der Originaldatenträger und deren Sicherungskopien ausreichend. Sie braucht dann von der regelmäßigen Datensicherung nicht erfasst zu werden.

Alle Benutzer/innen sollten über die Regelungen zur Datensicherung informiert sein, um ggf. auf Unzulänglichkeiten (zum Beispiel zu geringes Zeitintervall für ihren Bedarf) hinweisen oder individuelle Ergänzungen vornehmen zu können (zum Beispiel zwischenzeitliche Spiegelung wichtiger Daten auf der eigenen Platte). Auch die Information der Benutzer/innen darüber, wie lange die Daten wiedereinspielbar sind, ist wichtig. Werden zum Beispiel bei wöchentlicher Komplettsicherung nur zwei Generationen aufbewahrt, bleiben in Abhängigkeit vom Zeitpunkt des Verlustes nur zwei bis drei Wochen Zeit, um die Wiedereinspielung vorzunehmen.

Falls bei vernetzten Rechnern nur die Server-Platten gesichert werden, ist sicherzustellen, dass die zu sichernden Daten regelmäßig von den Benutzerinnen und Benutzern oder automatisch dorthin überspielt werden.

BCP 1.2 Entwicklung eines Datensicherungskonzeptes

Relevanz: Umsetzung/Wartung;

Die Verfahrensweise der Datensicherung wird von einer großen Zahl von Einflussfaktoren bestimmt. Das IT-System, das Datenvolumen, die Änderungsfrequenz der Daten und die Verfügbarkeitsanforderungen sind einige dieser Faktoren. Im Datensicherungskonzept gilt es, eine Lösung zu finden, die diese Faktoren berücksichtigt und gleichzeitig unter Kostengesichtspunkten wirtschaftlich vertretbar ist. Diese Lösung muss auch jederzeit aktualisierbar und erweiterbar sein. Weiters ist dafür Sorge zu tragen, dass alle betroffenen IT-Systeme im Datensicherungskonzept berücksichtigt werden und das Konzept stets den aktuellen Anforderungen entspricht.

Ein möglicher Aufbau eines Datensicherungskonzeptes ist in Anhang C angeführt.

Einzelne Punkte eines Datensicherungskonzeptes werden in den nachfolgenden Maßnahmen näher ausgeführt.

Für die Gewährleistung einer funktionierenden Datensicherung müssen praktische Übungen zur Datenrestaurierbarkeit verpflichtend vorgesehen sein (siehe BCP 3.2 Übungen zur Datenrekonstruktion).

BCP 1.3 Festlegung des Minimaldatensicherungskonzeptes

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

Für eine Organisation ist festzulegen, welche Minimalforderungen zur Datensicherung eingehalten werden müssen. Damit können viele Fälle, in denen eingehende Untersuchungen und die Erstellung eines Datensicherungskonzeptes zu aufwendig sind, pauschal behandelt werden. Weiterhin ist damit eine Grundlage gegeben, die generell für alle IT-Systeme gültig ist und damit auch für neue IT-Systeme, für die noch kein Datensicherungskonzept erarbeitet wurde. Ein Beispiel soll dies erläutern.

Minimaldatensicherungskonzept (Beispiel):

- *Software:*
  Sämtliche Software, also sowohl Eigenentwicklungen als auch Standardsoftware, ist einmalig mittels einer Vollsicherung zu sichern.
- *Systemdaten:*
  Systemdaten sind mindestens einmal monatlich mit einer Generation zu sichern.
- *Anwendungsdaten:*
  Alle Anwendungsdaten sind mindestens einmal monatlich mittels einer Vollsicherung im Drei-Generationen-Prinzip zu sichern.
- *Protokolldaten:*
  Sämtliche Protokolldaten sind mindestens einmal monatlich mittels einer Vollsicherung im Drei-Generationen-Prinzip zu sichern.

BCP 1.4 Datensicherung bei Einsatz kryptographischer Verfahren

Relevanz: Umsetzung/Wartung;

Beim Einsatz kryptographischer Verfahren darf die Frage der Datensicherung nicht vernachlässigt werden. Neben der Frage, wie sinnvollerweise eine Datensicherung der verschlüsselten Daten erfolgen sollte, muss auch überlegt werden, ob und wie die benutzten kryptographischen Schlüssel gespeichert werden sollen. Daneben ist es auch zweckmäßig, die Konfigurationsdaten der eingesetzten Kryptoprodukte zu sichern.

Datensicherung der Schlüssel

Es muss sehr genau überlegt werden, ob und wie die benutzten kryptographischen Schlüssel gespeichert werden sollen, da jede Schlüsselkopie eine potentielle Schwachstelle ist.

Trotzdem kann es aus verschiedenen Gründen notwendig sein, kryptographische Schlüssel zu speichern.

Es gibt unterschiedliche Methoden der Schlüsselspeicherung:

- die Speicherung zu Transportzwecken auf einem transportablen Datenträger, z.B. Diskette, Chipkarte (dient vor allem zur Schlüsselverteilung bzw. zum Schlüsselaustausch, siehe SYS 11.7 Key-Management),
- die Speicherung in IT-Komponenten, die dauerhaft auf kryptographische Schlüssel zugreifen müssen, also z.B. zur Kommunikationsverschlüsselung,
- die Schlüsselhinterlegung als Vorbeugung gegen Schlüsselverlust oder im Rahmen von Vertretungsregelungen.

Hierbei ist grundsätzlich zu beachten:

- Kryptographische Schlüssel sollten so gespeichert bzw. aufbewahrt werden, dass Unbefugte sie nicht unbemerkt auslesen können. Beispielsweise könnten Schlüssel in spezieller Sicherheitshardware gespeichert werden, die die Schlüssel bei Angriffen automatisch löscht. Falls sie in Software gespeichert werden, sollten sie auf jeden Fall in verschlüsselter Form gespeichert werden. Hierbei ist zu bedenken, dass die meisten Standardanwendungen, bei denen Schlüssel oder Passwörter in der Anwendung gespeichert werden, dies im Allgemeinen mit leicht zu brechenden Verfahren tun. Als weitere Variante kann auch das Vier-Augen-Prinzip bei der Schlüsselspeicherung benutzt werden, also die Speicherung eines Schlüssels in Schlüsselhälften oder Schlüsselteilen.
- Von Kommunikationsschlüsseln und anderen kurzlebigen Schlüsseln sollten keine Kopien erstellt werden. Damit eine unautorisierte Nutzung ausgeschlossen ist, sollten auch von privaten Signaturschlüsseln im Allgemeinen keine Kopien existieren. Falls jedoch für die Schlüsselspeicherung eine reine Softwarelösung gewählt wurde, d.h. wenn keine Chipkarte o.ä. verwendet wird, ist das Risiko des Schlüsselverlustes (etwa durch Bitfehler oder Festplattendefekt) erhöht. In diesem Fall ist es unter Umständen weniger aufwendig, eine ausreichend gesicherte Möglichkeit der Schlüsselhinterlegung zu schaffen, als bei jedem Schlüsselverlust alle Kommunikationspartner zu informieren.
- Von langlebigen Schlüsseln, die z.B. zur Archivierung von Daten oder zur Generierung von Kommunikationsschlüsseln eingesetzt werden, sollten auf jeden Fall Sicherungskopien angefertigt werden.

Datensicherung der verschlüsselten Daten

Besondere Sorgfalt ist bei der Datensicherung von verschlüsselten Daten bzw. beim Einsatz von Verschlüsselung während der Datenspeicherung notwendig. Treten hierbei Fehler auf, sind nicht nur einige Datensätze, sondern meist alle Daten unbrauchbar.

Die Langzeitspeicherung von verschlüsselten oder signierten Daten bringt viele zusätzliche Probleme mit sich. Hierbei muss nicht nur sichergestellt werden, dass die Datenträger regelmäßig aufgefrischt werden und jederzeit noch die technischen Komponenten zum Verarbeiten dieser zur Verfügung stehen, sondern auch, dass die verwendeten kryptographischen Algorithmen und die Schlüssellänge noch dem Stand der Technik entsprechen. Bei der langfristigen Archivierung von Daten kann es daher sinnvoller sein, diese unverschlüsselt zu speichern und dafür entsprechend sicher zu lagern, also z.B. in Tresoren.

Die verwendeten Kryptomodule sollten vorsichtshalber immer archiviert werden, da die Erfahrung zeigt, dass auch noch nach Jahren Daten auftauchen, die nicht im Archiv gelagert waren.

Datensicherung der Konfigurationsdaten der eingesetzten Produkte

Bei komplexeren Kryptoprodukten sollte nicht vergessen werden, deren Konfigurationsdaten zu sichern. Die gewählte Konfiguration sollte dokumentiert sein, damit sie nach einem Systemversagen oder einer Neuinstallation schnell wieder eingerichtet werden kann.

BCP 1.5 Geeignete Aufbewahrung der Backup-Datenträger

Relevanz: Umsetzung/Wartung;

Backup-Datenträger unterliegen besonderen Anforderungen hinsichtlich ihrer Aufbewahrung:

- Der Zugriff auf diese Datenträger darf nur befugten Personen möglich sein, so dass eine Entwendung ausgeschlossen werden kann.
- Ein ausreichend schneller Zugriff im Bedarfsfall muss gewährleistet sein.
- Für den Katastrophenfall müssen die Backup-Datenträger räumlich getrennt vom Rechner - auf jeden Fall in einem anderen Brandabschnitt, wenn möglich disloziert - aufbewahrt werden.

Zu beachten sind auch die Anforderungen aus SYS 2.2 Datenträgerverwaltung.

Je nach Anforderungen und geforderte Ausfallsicherheit (Katastrophenvorsorge – vgl. BCP 2.1) kann es notwendig sein das Datenarchiv an einem gänzlich anderen Ort zu halten. Damit wird sichergestellt, dass der Datenbestand eines derartigen Notfallarchivs nicht aufgrund der gleichen Schadensursache zerstört wird, und dass im Falle der Unzugänglichkeit der Infrastruktur (beispielsweise aufgrund von Verschüttungen, o.ä.) der Datensicherungsbestand zur Verfügung steht.

BCP 1.6 Sicherungskopie der eingesetzten Software

Relevanz: Umsetzung/Wartung;

Von den Originaldatenträgern von Standardsoftware bzw. von der Originalsoftware bei Eigenentwicklungen ist eine Sicherungskopie zu erstellen, von der bei Bedarf die Software wieder eingespielt werden kann. Die Originaldatenträger und die Sicherungskopien sind getrennt voneinander aufzubewahren. Es ist darauf zu achten, dass der physikalische Schreibschutz des Datenträgers ein versehentliches Löschen oder Überschreiben der Daten verhindert.

Ein unerlaubter Zugriff, z.B. zur Erstellung einer Raubkopie, muss ausgeschlossen sein.

BCP 1.7 Beschaffung eines geeigneten Datensicherungssystems

Relevanz: Umsetzung/Wartung;

Ein Großteil der Fehler, die beim Erstellen oder Restaurieren einer Datensicherung auftreten, sind Fehlbedienungen. Daher sollte bei der Beschaffung eines Datensicherungssystems nicht allein auf dessen Leistungsfähigkeit geachtet werden, sondern auch auf seine Bedienbarkeit und insbesondere auf seine Toleranz gegenüber Benutzerfehlern.

Bei der Auswahl von Sicherungssoftware sollte darauf geachtet werden, dass sie die folgenden Anforderungen erfüllt:

- Die Datensicherungssoftware sollte ein falsches Medium ebenso wie ein beschädigtes Medium im Sicherungslaufwerk erkennen können.
- Sie sollte mit der vorhandenen Hardware problemlos zusammenarbeiten.
- Es sollte möglich sein, Sicherungen automatisch zu vorwählbaren Zeiten bzw. in einstellbaren Intervallen durchführen zu lassen, ohne dass hierzu manuelle Eingriffe (außer dem eventuell notwendigen Bereitstellen von Sicherungsdatenträgern) erforderlich wären.
- Es sollte möglich sein, einen oder mehrere ausgewählte Benutzerinnen oder Benutzer automatisch über das Sicherungsergebnis und eventuelle Fehlermeldungen per E-Mail oder ähnliche Mechanismen zu informieren. Die Durchführung von Datensicherungen inklusive des Sicherungsergebnisses und möglicher Fehlermeldungen sollten in einer Protokolldatei abgespeichert werden.
- Die Sicherungssoftware sollte die Sicherung des Backup-Mediums durch ein Passwort oder, je nach Vertraulichkeitsanforderungen, durch Verschlüsselung unterstützen. Weiters sollte sie in der Lage sein, die gesicherten Daten in komprimierter Form abzuspeichern.
- Durch Vorgabe geeigneter Include- und Exclude-Listen bei der Datei- und Verzeichnisauswahl sollte genau spezifiziert werden können, welche Daten zu sichern sind und welche nicht. Es sollte möglich sein, diese Listen zu Sicherungsprofilen zusammenzufassen, abzuspeichern und für spätere Sicherungsläufe wieder zu benutzen.
- Es sollte möglich sein, die zu sichernden Daten in Abhängigkeit vom Datum ihrer Erstellung bzw. ihrer letzten Modifikation auszuwählen.
- Die Sicherungssoftware sollte die Erzeugung logischer und physischer Vollkopien sowie inkrementeller Kopien (Änderungssicherungen) unterstützen.
- Die zu sichernden Daten sollten auch auf Festplatten und Netzlaufwerken abgespeichert werden können.

- Die Sicherungssoftware sollte in der Lage sein, nach der Sicherung einen automatischen Vergleich der gesicherten Daten mit dem Original durchzuführen und nach der Wiederherstellung von Daten einen entsprechenden Vergleich zwischen den rekonstruierten Daten und dem Inhalt des Sicherungsdatenträgers durchzuführen.
- Bei der Wiederherstellung von Dateien sollte es möglich sein auszuwählen, ob die Dateien am ursprünglichen Ort oder auf einer anderen Platte bzw. in einem anderen Verzeichnis wiederhergestellt werden. Ebenso sollte es möglich sein, das Verhalten der Software für den Fall zu steuern, dass am Zielort schon eine Datei gleichen Namens vorhanden ist. Dabei sollte man wählen können, ob diese Datei immer, nie oder nur in dem Fall, dass sie älter als die zu rekonstruierende Datei ist, überschrieben wird, oder dass in diesem Fall eine explizite Anfrage erfolgt.

Falls mit dem eingesetzten Programm die Datensicherung durch ein Passwort geschützt werden kann, sollte diese Option genutzt werden.

BCP 1.8 Datensicherung bei mobiler Nutzung eines IT-Systems

Relevanz: Umsetzung/Wartung; Anwender/innen;

IT-Systeme im mobilen Einsatz (z.B. Laptops, Notebooks) sind in aller Regel nicht permanent in ein Netz eingebunden. Der Datenaustausch mit anderen IT-Systemen erfolgt üblicherweise über Datenträger oder über temporäre Netzanbindungen. Letztere können beispielsweise durch Remote Access oder direkten Anschluss an ein LAN nach Rückkehr zum Arbeitsplatz realisiert sein. Anders als bei stationären Clients ist es daher bei mobilen IT-Systemen meist unvermeidbar, dass Daten zumindest zeitweise lokal anstatt auf einem zentralen Server gespeichert werden. Dem Verlust dieser Daten muss durch geeignete Datensicherungsmaßnahmen vorgebeugt werden.

Generell bieten sich folgende Verfahren zur Datensicherung an:

Datensicherung auf externen Datenträgern:

Der Vorteil dieses Verfahrens ist, dass die Datensicherung an nahezu jedem Ort und zu jeder Zeit erfolgen kann. Nachteilig ist, dass ein geeignetes Laufwerk und genügend Datenträger mitgeführt werden müssen und dass für den/die Benutzer/in zusätzlicher Aufwand für die ordnungsgemäße Handhabung der Datenträger entsteht.

Die Datenträger sollten eine ausreichende Speicherkapazität besitzen, so dass der/die Benutzer/in nicht mehrere Datenträger pro Sicherungsvorgang in das Laufwerk einlegen muss. Bei unverschlüsselter Datenhaltung ergibt sich außerdem die Gefahr, dass Datenträger abhanden kommen und dadurch sensitive Daten kompromittiert werden können. Die Datenträger und das mobile IT-System sollten möglichst getrennt voneinander aufbewahrt werden, damit bei Verlust oder Diebstahl des IT-Systems die Datenträger nicht ebenfalls abhanden kommen.

Nach Rückkehr zum Arbeitsplatz müssen die Datensicherungen auf den Datenträgern in das Backup-System oder in das Produktivsystem bzw. die zentrale Datenhaltung der Organisation eingebracht werden.

Datensicherung über temporäre Netzverbindungen

Wenn die Möglichkeit besteht, das IT-System regelmäßig an ein Netz anzuschließen, beispielsweise über Remote Access, kann die Sicherung der lokalen Daten auch über die Netzanbindung erfolgen. Vorteilhaft ist hier, dass der/die Benutzer/in keine Datenträger verwalten und auch kein entsprechendes Laufwerk mitführen muss. Weiterhin lässt sich das Verfahren weitgehend automatisieren, beispielsweise kann die Datensicherung beim Einsatz von Remote Access nach jedem Einwahlvorgang automatisch gestartet werden.

Entscheidend bei der Datensicherung über eine temporäre Netzverbindung ist, dass deren Bandbreite für das Volumen der zu sichernden Daten ausreichen muss. Die Datenübertragung darf nicht zu lange dauern und nicht zu übermäßigen Verzögerungen führen, wenn der/die Benutzer/in gleichzeitig auf entfernte Ressourcen zugreifen muss. Bei gängigen Zugangstechnologien (z.B. ISDN, Modem, Mobiltelefon) bedeutet dies, dass nur geringe Datenmengen pro Sicherungsvorgang transportiert werden können. Einige Datensicherungsprogramme bieten daher die Möglichkeit an, lediglich Informationen über die Änderungen des Datenbestands seit der letzten Datensicherung über die Netzverbindung zu übertragen. In vielen Fällen kann hierdurch das zu transportierende Datenvolumen stark reduziert werden.

Eine wichtige Anforderung an die zur Datensicherung verwendete Software ist, dass unerwartete Verbindungsabbrüche erkannt und ordnungsgemäß behandelt werden. Die Konsistenz der gesicherten Daten darf durch Verbindungsabbrüche nicht beeinträchtigt werden.

Bei beiden Verfahren zur Datensicherung ist es wünschenswert, das Volumen der zu sichernden Daten zu minimieren. Neben dem Einsatz verlustfreier Kompressionsverfahren, die in viele Datensicherungsprogrammen integriert sind, können auch inkrementelle oder differentielle Sicherungsverfahren zum Einsatz kommen Hierdurch erhöht sich jedoch u.U. der Aufwand für die Wiederherstellung einer Datensicherung.

BCP 1.9 Verpflichtung der Mitarbeiter/innen zur Datensicherung

Relevanz: Umsetzung/Wartung; Anwender/innen;

Da die Datensicherung eine wichtige IT-Sicherheitsmaßnahme darstellt, sollten die betroffenen Mitarbeiter/innen - vorzugsweise in schriftlicher Form - zur Einhaltung des Datensicherungskonzeptes bzw. des Minimaldatensicherungskonzeptes verpflichtet werden. Eine regelmäßige Motivation zur Datensicherung und Kontrolle auf Einhaltung ist empfehlenswert.

7.2 Strategie und Planung

Relevanz: Management; Umsetzung/Wartung; Anwender/innen;

BCP 2.1 Definition von Verfügbarkeitsklassen

Relevanz: Management; Umsetzung/Wartung;

Um den Verfügbarkeitsanspruch von IT-Anwendungen einer Organisation darstellen zu können, sind im Rahmen der IT-Sicherheitspolitik entsprechende Verfügbarkeitsklassen zu definieren (vgl. dazu auch Teil 1 des vorliegenden Sicherheitshandbuches [KIT S01]).

Nachfolgend ein Beispiel für ein solches Klassifizierungsschema – basierend auf den Katastrophenvorsorge- und Ausfallssicherheitsüberlegungen im IT-Bereich des Bundeskanzleramtes [KFall]:

- *Betriebsverfügbarkeitskategorie 1 – Keine Vorsorge (unkritisch):*
  Für die IT-Anwendung werden keine besonderen Vorkehrungen getroffen. Es ist ein Datenverlust bzw. Ausfall der IT-Anwendung unbestimmter Dauer denkbar. Eine Behinderung in der Wahrnehmung der Aufgaben der betroffenen Verwaltungsstelle entsteht durch den Ausfall bzw. Datenverlust nicht.
- *Betriebsverfügbarkeitskategorie 2 – Offline Sicherung:*
  Es sind die gängigen Sicherungsmaßnahmen für die IT-Anwendung vorgesehen, ein Datenverlust ist auszuschließen. Die IT-Anwendung kann bei technischen Problemen erst nach deren Behebung am ursprünglichen Produktivsystem in Betrieb genommen werden. Die Sicherung wird an einen externen Ort ausgelagert.
- *Betriebsverfügbarkeitskategorie 3 – Redundante Infrastruktur:*
  Die Infrastruktur für die IT-Anwendung ist derart ausgelegt, dass bei Ausfall einer IT-Komponente der Betrieb durch redundante Auslegung ohne Unterbrechung fortgesetzt werden kann.
- *Betriebsverfügbarkeitskategorie 4 – Redundante Standorte:*
  Die IT-Infrastruktur sowie die darauf aufsetzende IT-Anwendung ist auf zwei Standorte verteilt, so dass bei Betriebsunterbrechung des einen Standortes die IT-Anwendung uneingeschränkt am zweiten Standort weiter betrieben werden kann.

Zusätzlich zu den vier genannten Kategorien ist noch die Zusatzqualität „K-Fall Sicher“ definiert, welche auch die Anforderungen in Katastrophenfällen berücksichtigt:

- *K-Fall sicher (K2 bis K4):*
  Die IT-Anwendung ist derart konzipiert, dass zumindest ein Notbetrieb in einer Zero-Risk-Umgebung möglich ist. Dazu werden die Daten je nach Aktualisierungsgrad laufend in die Zero-Risk-Umgebung transferiert und der Betrieb der IT-Anwendung derart gestaltet, dass ein Wiederaufsetzen eines definierten Notbetriebes in der Zero-Risk-Umgebung umgehend möglich ist. Eine Einbindung der Zero-Risk-Umgebung in den Normalbetrieb ist je nach Sensibilität vorgesehen.

In Summe ergibt eine derartige Einstufung die Verfügbarkeitsklassen 1 bis 4 und K2 bis K4. Die Zusatzoption „K-Fall sicher“ in Verbindung mit Betriebsverfügbarkeitskategorie 1 ist nicht sinnvoll.

BCP 2.2 Erstellung einer Übersicht über Verfügbarkeitsanforderungen

Relevanz: Umsetzung/Wartung;

Für die in einem IT-System betriebenen IT-Anwendungen und deren Daten sind die Verfügbarkeitsanforderungen festzustellen. Da eine IT-Anwendung nicht zwingend jeden Bestandteil des IT-Systems benötigt, sind die Verfügbarkeitsanforderungen der IT-Anwendungen auf die wesentlichen Komponenten des IT-Systems abzubilden.

Das Ergebnis dieser Arbeit kann in Form einer Übersicht dargestellt werden, wie das nachfolgende Beispiel illustrieren soll:

IT-Anwendung	Verfügbarkeitsklasse (lt. Beispiel in BCP 2.1)	IT-System	IT-Komponente
Prozessleitsystem	Kategorie 3, K-Fall Sicher (K3)	Prozessleitrechner	Host Prozessleitsystem
			Datenhaltung
			...
		Netzwerk	Leitungen
			Routing-Devices
			...
Zugangssystem	Kategorie 2	Rechensystem Zugangssystem	Host Zugangssystem
			Datenhaltung
			...
		Netzwerk	Leitungen
			Routing Devices
			...

Tabelle 7: Verfügbarkeitsklassen der Anwendung

Die zu fordernde Betriebsverfügbarkeit der Systeme und Komponenten wird durch deren Anwendung definiert. Demnach wurde in obiger Tabelle vordergründig die Verfügbarkeit der einzelnen Anwendungen aufgeführt und in weiterer Folge alle zur Ausführung der Anwendung notwendigen Komponenten und Systeme aufgelistet. Über die Identifikation der Komponenten lassen sich gemeinsam genutzte Systemteile identifizieren und deren Verfügbarkeitskategorie festlegen. Die Anwendung mit höchster Kategorie ist dabei bestimmend, wie in folgender Tabelle dargestellt:

IT-System	IT-Komponente	Verfügbarkeitsklasse (lt. Beispiel in BCP 2.1)	Bestimmende Anwendung
Rechensystem Zugangssystem	Host Zugangssystem	Kategorie 2	Zugangssystem
	Datenhaltung	Kategorie 3, K-Fall sicher (K3)	Prozessleitsystem
	...	...	...
Prozessleitrechner	Host Prozessleitsystem	Kategorie 3, K-Fall sicher (K3)	Prozessleitsystem
	Datenhaltung	Kategorie 3, K-Fall sicher (K3)	Prozessleitsystem
	...	...	...
Netzwerk	Leitungen	Kategorie 3, K-Fall sicher (K3)	Prozessleitsystem
	Routing-Devices	Kategorie 3, K-Fall sicher (K3)	Prozessleitsystem
	...	...	...

Tabelle 8: Verfügbarkeitsklassen der Systeme und Komponenten

Dies ist wie folgt zu interpretieren: Die IT-Komponente Host im IT-System “Zentralsystem” hat auf Grund der IT-Anwendung Buchhaltung eine maximal tolerierbare Ausfallzeit von 3 Stunden und ist daher der Verfügbarkeitsklasse 2 zuzuordnen.

Eine praktikable Vorgehensweise ist es, zu den einzelnen IT-Anwendungen den zuständigen Applikationsverantwortlichen nach den tolerierbaren Ausfallzeiten der benutzten IT-Komponenten zu befragen, um danach die Ergebnisse nach IT-System und Komponenten geordnet in der Tabelle aufzuführen. Die Anforderungen an die Verfügbarkeit sind zu begründen, sofern dies nicht schon an anderer Stelle geschehen ist. Die Verfügbarkeitsanforderungen sind von der Behörden- bzw. Unternehmensleitung zu bestätigen.

Die Tabelle ist regelmäßig zu überprüfen und gegebenenfalls zu aktualisieren.

Die Übersicht erleichtert es, die besonders zeitkritischen Komponenten des IT-Systems zu extrahieren, für die die Notfallvorsorge unumgänglich ist. Bei Ausfall einer Komponente gibt diese Übersicht Auskunft über die betroffenen IT-Anwendungen und deren Verfügbarkeitsanforderungen.

Bei Ausfall einer Komponente des IT-Systems ermöglicht diese Übersicht weiters eine schnelle Aussage, ab wann ein Notfall vorliegt. Nicht jeder Teil- oder Gesamtausfall des Systems stellt einen Notfall dar. Oftmals lassen sich Ausfälle des IT-Systems durch geplante Maßnahmen, z.B. Ersatzbeschaffung, auch in kurzer Zeit beheben. Der Notfall tritt erst dann ein, wenn ein Zustand erreicht wird, bei dem innerhalb der geforderten Zeit eine Wiederherstellung der Verfügbarkeit nicht möglich ist und sich daraus ein sehr hoher Schaden ergibt.

Dass ein Notfall auch bei Ausfall einer besonders zeitkritischen Komponente nicht zwingend eintreten muss, lässt sich anhand des Ersatzbeschaffungsplans (siehe BCP 2.10 Ersatzbeschaffungsplan) und der Untersuchung über interne und externe Ausweichmöglichkeiten (vgl. BCP 2.7 Untersuchung interner und externer Ausweichmöglichkeiten) ersehen.

BCP 2.3 Benennung einer/eines Notfall-Verantwortlichen

Relevanz: Management;

Schon bei Eintritt eines Ereignisses, in dessen Folge der Notfall entstehen könnte, sind die erforderlichen Maßnahmen zu ergreifen, die zu einer Schadensreduzierung führen.

Für die autorisierte und rechtzeitige Einleitung von Notfallmaßnahmen bedarf es der Benennung einer/eines Notfall-Verantwortlichen. Die Behörden- bzw. Unternehmensleitung muss die Notfall-Verantwortliche bzw. den Notfall-Verantwortlichen sowohl für die Entscheidung autorisieren, ob ein Notfall eingetreten ist, als auch für die Einleitung erforderlicher Notfallmaßnahmen.

BCP 2.4 Erstellung eines Disaster Recovery Handbuches

Relevanz: Umsetzung/Wartung;

In einem Disaster Recovery Handbuch (auch als Notfall-Handbuch bezeichnet) sind alle Maßnahmen, die nach Eintritt eines notfallauslösenden Ereignisses zu ergreifen sind, und alle dazu erforderlichen Informationen zu dokumentieren. Das Disaster Recovery Handbuch ist so zu gestalten, dass eine sachverständige Dritte bzw. ein sachverständiger Dritter in der Lage ist, die im Handbuch spezifizierten Notfallmaßnahmen durchzuführen.

In Anhang C wird beispielhaft ein umfassendes Inhaltsverzeichnis eines Disaster Recovery Handbuches zur Orientierung aufgeführt. Welche Teile dieses Vorschlags übernommen werden können, ist abhängig von der vorhandenen System- und Anwendungsdokumentation und kann daher nur individuell entschieden werden.

Das Disaster Recovery Handbuch ist durch die Leitung der Organisation in Kraft zu setzen und muss nach Bedarf aktualisiert werden. Die Verfügbarkeit des Disaster Recovery Handbuches ist von zentraler Bedeutung. Deshalb ist ein aktuelles Exemplar extern auszulagern. Zusätzlich ist das Disaster Recovery Handbuch allen im Handbuch genannten Personen oder Organisationseinheiten zur Kenntnis zu bringen.

Die Ausgestaltung wichtiger Inhalte ist den nachfolgenden Maßnahmenbeschreibungen zu entnehmen.

BCP 2.5 Definition des eingeschränkten IT-Betriebs (Notlaufplan)

Relevanz: Umsetzung/Wartung;

Für den Fall, dass Teile des IT-Systems ausfallen, ist zu untersuchen, ob ein eingeschränkter IT-Betrieb notwendig und möglich ist. Um bei einem eingeschränkten IT-Betrieb möglichst viele IT-Anwendungen betreiben zu können, ist die für jede einzelne IT-Anwendung zur Verfügung gestellte Kapazität auf das notwendige Maß zu reduzieren.

Für den eingeschränkten IT-Betrieb muss festgelegt werden, welche IT-Anwendungen mit welcher Priorität betrieben werden. Dies ist schriftlich zu fixieren (Notlaufplan).

Auch manuelle Ersatzverfahren können geeignet sein, um die Verfügbarkeitsanforderungen einer IT-Anwendung zu senken. Die für den Einsatz eines manuellen Ersatzverfahrens erforderlichen Hilfsmittel (Formulare, Papierlisten, Mikrofiche) müssen dazu allerdings bereitgehalten werden.

Die qualitativen und quantitativen Vorgaben für den eingeschränkten IT-Betrieb sind mit den Fachbereichen abzusprechen.

BCP 2.6 Regelung der Verantwortung im Notfall

Relevanz: Management;

Für den Zeitraum von Eintritt des schädigenden Ereignisses bis zur vollständigen Wiederherstellung der Verfügbarkeit kann eine zeitlich befristete Notfall-Organisation erforderlich sein.

Es müssen Verantwortliche bestimmt sein, die befugt sind zu entscheiden, ob ein Notfall eingetreten ist, und die die entsprechenden Maßnahmen des Disaster Recovery Handbuchs einleiten (siehe BCP 2.3 Benennung einer/eines Notfall-Verantwortlichen). Die an der Durchführung der Maßnahmen im Bereich der Notfallvorsorge beteiligten Organisationseinheiten müssen befugt sein, die ihnen übertragenen Aufgaben eigenverantwortlich durchzuführen. Die hierzu erforderlichen Regelungen sind schriftlich festzuhalten. Dieses “Notfall-Organigramm” muss von der Leitung der Organisation autorisiert werden.

BCP 2.7 Untersuchung interner und externer Ausweichmöglichkeiten

Relevanz: Management; Umsetzung/Wartung;

Um Kapazitätsengpässe im eingeschränkten IT-Betrieb zu vermeiden, sind interne und externe Ausweichmöglichkeiten zu untersuchen.

Bei der Untersuchung von Ausweichmöglichkeiten ist insbesondere auf die technischen Anforderungen an das Ausweich-IT-System zu achten. Kompatibilität und ausreichende Kapazitätsreserven des Ausweich-IT-Systems sind Grundvoraussetzung für dessen Benutzung.

Zunächst steht die interne Verlagerung von IT-Anwendungen von einem IT-System auf ein anderes IT-System im Vordergrund (z.B. Ausweichen auf den Entwicklungsrechner, wenn der Produktionsrechner ausfällt). Externe Ausweichmöglichkeiten sind dann heranzuziehen, wenn mit internen Ausweichmöglichkeiten die Verfügbarkeitsanforderungen nicht mehr oder nicht wirtschaftlich erfüllt werden können. Dabei ist dafür Sorge zu tragen, dass die Integrität und Vertraulichkeit der ausgelagerten IT-Anwendungen und Daten gewährleistet wird.

Ebenso sind Ausweichmöglichkeiten für nicht IT-spezifische Komponenten zu berücksichtigen. So sind beispielsweise im Bereich der Infrastruktur Ausweichmöglichkeiten für IT-Räume in Betracht zu ziehen.

Auf Basis des IKT-Board Beschlusses [IKTB-170902-4] sind für Organisationen der öffentlichen Verwaltung einheitliche Kriterien für Ausweichsysteme und für die Krisensicherung empfohlen. Dazu sind Kriterienkataloge anzuwenden, die mit den jeweiligen entsprechenden Ressorts abgestimmt worden sind. Die Ausweichstandorte werden in Bezug auf die Erfüllung der Klassen des Kriterienkataloges klassifiziert.

Die Konfiguration, Kapazität und Kompatibilität von internen und externen Ausweichmöglichkeiten sind dem aktuellen Verfahrensstand anzupassen.

BCP 2.8 Alarmierungsplan

Relevanz: Umsetzung/Wartung; Anwender/innen;

Ein Alarmierungsplan enthält eine Beschreibung der Meldewege, über den bei Eintritt eines Notfalls die zuständigen Personen oder Organisationseinheiten zu informieren sind. Die Alarmierung kann z.B. über Telefon, Fax, Funkrufdienste oder Kurier erfolgen. Beschrieben werden muss, wer wen benachrichtigt, wer ersatzweise zu benachrichtigen ist bzw. wie bei Nichterreichen zu verfahren ist. Zu diesem Zweck sind evtl. Adress- und Telefonlisten zu führen. Wird eine Evakuierung des Gebäudes nötig bzw. ist dieses nicht betretbar (Brand-, Bombenalarm, ...), müssen entsprechende Treffpunkte vereinbart sein.

Der Alarmierungsplan muss sämtlichen Notfall-Verantwortlichen zur Verfügung stehen, darüber hinaus an zentraler Stelle redundant vorgehalten werden (z.B. Portier, Bewachungspersonal). Die im Alarmierungsplan genannten Personen müssen den sie betreffenden Teil kennen. Allen Mitarbeiterinnen und Mitarbeitern müssen die Ansprechpartner/innen bekannt sein, denen das Eintreten eines evtl. notfallauslösenden Ereignisses gemeldet werden kann.

Es kann verschiedene Alarmierungspläne für unterschiedliche Schadensfälle geben (Feuer, Wasser, DFÜ-Ausfall). Dann muss darauf geachtet werden, dass alle Schadensfälle abgedeckt sind.

Mit der Erstellung eines Alarmierungsplans sollte auch die Festlegung eines Ruf- oder Bereitschaftsdienstes erwogen werden.

Der Alarmierungsplan ist immer aktuell zu halten und regelmäßig zu testen.

BCP 2.9 Erstellung eines Wiederanlaufplans

Relevanz: Umsetzung/Wartung;

Für einen geregelten Wiederanlauf nach Ausfall einer IT-Komponente sind folgende Informationen zu dokumentieren (siehe Beispiel in Anhang C.13 Inhaltsverzeichnis Disaster Recovery Handbuch (Muster)):

- Wiederbeschaffungsmöglichkeiten, zum Beispiel die Nutzung eines Testrechners für den Echtbetrieb oder die Ersatzbeschaffung (siehe BCP 2.10 Ersatzbeschaffungsplan),
- interne/externe Ausweichmöglichkeiten für IT-Anwendungen (siehe BCP 2.7 Untersuchung interner und externer Ausweichmöglichkeiten) sind aufzuzählen,
- DFÜ-Versorgung für den Notbetrieb, um die minimal notwendigen Datenübertragungen zu gewährleisten,
- die im eingeschränkten IT-Betrieb (siehe BCP 2.5 Definition des eingeschränkten IT-Betriebs (Notlaufplan)) laufenden IT-Anwendungen sowie

- Systemstart der IT-Komponente und Einbindung in das IT-System.

Um den Anforderungen an die Verfügbarkeit (siehe BCP 2.2 Erstellung einer Übersicht über Verfügbarkeitsanforderungen) der einzelnen IT-Anwendungen gerecht zu werden, ist eine Reihenfolge für den Wiederanlauf der IT-Anwendungen festzulegen.

Die für den Wiederanlauf einer IT-Anwendung erforderlichen Schritte sind im Disaster Recovery Handbuch aufzuzeigen. Beispiele für solche Schritte sind:

- Aufbau und Installation der notwendigen Hardware-Komponenten,
- Einspielen der Systemsoftware,
- Einspielen der Anwendungssoftware,
- Bereitstellen der notwendigen Daten einschließlich Konfigurationsdateien,
- Wiederanlauf.

Eine revisionsfähige Protokollierung des Wiederanlaufs ist zu gewährleisten.

Der Wiederanlaufplan ist durch Notfallübungen (sowohl bei internen als auch bei externen Ausweichmöglichkeiten) auf seine Durchführbarkeit zu testen. Insbesondere ist bei der Durchführung solcher Übungen der ausschließliche Einsatz der Software und Daten zu testen, die in internen oder externen Sicherungsarchiven aufbewahrt werden.

Der Wiederanlauf kann, je nach Umfang der betriebenen IT-Anwendungen, mit erheblichem Zeitaufwand verbunden sein. Der Zeitaufwand für die mit dem Wiederanlauf verbundenen Maßnahmen kann durch solche Übungen ermittelt werden und ist bei der Überarbeitung des Wiederanlaufplans zu berücksichtigen.

BCP 2.10 Ersatzbeschaffungsplan

Relevanz: Umsetzung/Wartung;

Bei Ausfall einzelner Teile des IT-Systems ist neben der Reparatur die Ersatzbeschaffung zunächst die Maßnahme, die am zielgerichtetsten die Wiederherstellung der Verfügbarkeit verfolgt.

Um den Vorgang der Ersatzbeschaffung zu beschleunigen, ist die Erstellung eines Ersatzbeschaffungsplans sinnvoll. Dieser muss für jede wichtige IT-Komponente Angaben machen über:

- Bezeichnung der IT-Komponente (Name, Geräte-Nr., Beschaffungsdatum),
- Hersteller,
- Lieferant,
- Lieferzeit und
- Dauer der Reinstallation.

Ersatzbeschaffungsmaßnahmen müssen neben der Wiederherstellung der Verfügbarkeit des IT-Systems auch der Fortentwicklung der Informationstechnik Rechnung tragen. Entsprechen eingesetzte Teile des IT-Systems nicht mehr dem Stand der Technik, so darf eine Ersatzbeschaffung nicht ausschließlich darauf gerichtet sein, den alten Zustand wiederherzustellen. Dies erfordert eine regelmäßige Überarbeitung des Ersatzbeschaffungsplans. Der Bezug zur Betriebsmittelverwaltung ist zu beachten (vgl. SYS 2.1 Betriebsmittelverwaltung).

BCP 2.11 Lieferantenvereinbarungen

Relevanz: Umsetzung/Wartung;

Bei Kauf von Informationstechnik ergibt sich für den/die IT-Betreiber/in die Notwendigkeit, Ersatzbeschaffungsmaßnahmen zu planen. Von besonderer Bedeutung beim Kauf sind eine vom Hersteller oder Lieferanten zugesicherte Nachkaufgarantie, Ersatzteillieferung, garantierte Lieferzeiten, die Garantiezeit bei auftretenden Mängeln sowie der angebotene Support.

Miet- bzw. Leasingverträge müssen Regelungen über schadensvorbeugende Wartungsarbeiten und die Anforderungen an die Beseitigung von Störungen oder Schäden beinhalten.

Im Gegensatz zum Kauf von Informationstechnik ist bei deren Miete oder Leasing eine Vielzahl von Risiken über den Vermieter bereits abgesichert. In der Regel schließt ein/e Vermieter/in eine Feuerversicherung für die vermietete Informationstechnik ab, die von der Mieterin bzw. vom Mieter durch den Mietvertrag mitbezahlt wird. Somit ist bei Miete oder Leasing von Informationstechnik auf die nicht vom Vertrag abgedeckten Versicherungslücken zu achten.

BCP 2.12 Abschließen von Versicherungen

Relevanz: Management; Umsetzung/Wartung;

Das trotz aller informationstechnischen, baulichen und organisatorischen Maßnahmen verbleibende Restrisiko kann durch entsprechende Versicherungen abgedeckt werden.

Für Bundesbehörden ist der Abschluss von Versicherungen zwar unüblich, dennoch sollen die prinzipiellen Möglichkeiten im Folgenden angeführt werden.

Da die herkömmlichen Geschäftsversicherungen gegen Feuer, Diebstahl oder Sturm nur bestimmte Gefahren abdecken (”Ausschnittsdeckung”), nicht aber die spezifischen Risiken im Bereich der Datenverarbeitung, kann der Abschluss eigener DV-Versicherungen notwendig werden.

Im Folgenden werden derzeit in Österreich angebotene Sparten von Computer-Versicherungen kurz erörtert. Da die Versicherungsbedingungen von den einzelnen Anbietern individuell festgelegt werden können, sind Details zu den einzelnen Sparten, ihrem Deckungsumfang und ihren Besonderheiten den konkreten Versicherungsbedingungen und -verträgen zu entnehmen. (Unverbindliche) Empfehlungen werden in den unten angeführten Musterbedingungen gegeben. Generell ist beim Abschluss von DV-Versicherungen auf Grund der Komplexität der Materie eine intensive Zusammenarbeit mit den Versicherungsgesellschaften anzustreben, um eine optimale Risikoabdeckung zu gewährleisten.

Elektronik-Sachversicherung

Dies ist die eigentliche Geräte-Versicherung. Ihr liegen als Musterbedingung die “Allgemeinen Bedingungen für die Versicherung von elektronischen Datenverarbeitungsanlagen” (ADVB) zugrunde. Versicherte Gefahren und Schäden sind hier unvorhergesehen und plötzlich eintretende Beschädigung oder Zerstörung sowie der Verlust der versicherten Sachen etwa durch Bedienungsfehler, Fahrlässigkeit oder Sabotage (sofern die durch vorangeführte Gefahren verursachten Beschädigungen visuell ohne Hilfsmittel erkennbar sind), Wasser oder Feuchtigkeit, Brand, Blitzschlag, Explosionen, Diebstahl u.a. (Details siehe Artikel 2, §1 der ADVB).

Bei Abschluss der Versicherung ist insbesondere zu klären, welche Gegenstände versichert sind, und ob Voraussetzungen für bestimmte Leistungen bestehen, wie z.B. der Abschluss eines Wartungsvertrages.

Festzusetzen sind weiters die Versicherungssumme, die Angleichung der Versicherungssumme, der Versicherungsort, Selbstbehalte sowie mögliche Ausschlüsse und Erweiterungen. Es wird grundsätzlich der Neuwert (eventuell unter Abzug eines Selbstbehaltes) ersetzt.

Informationsverlust- und Datenträger-Versicherung

Die Informationsverlust- und Datenträger-Versicherung (vgl. auch “Allgemeine Bedingungen für die Informationsverlust- und Datenträger-Versicherung elektronischer Datenverarbeitungsanlagen” (ADVBID)) versichert die in der Polizze angeführten Datenträger und die auf ihnen befindlichen Daten unter den im Antrag angegebenen Betriebs- und Aufbewahrungsverhältnissen. Die Daten sind nur insoweit versichert, als sie wiederbeschaffbar und für den/die Versicherungsnehmer/in erforderlich sind.

Ersetzt werden die Kosten für die Wiederherstellung von in Verlust geratenen Datenbeständen sowie der Wert zerstörter oder verlorener Datenträger.

Es ist jedoch zu beachten, dass diese Leistungen an eine Reihe von Bedingungen geknüpft sind.

Mehrkosten-Versicherung

Diese Versicherung deckt die Mehrkosten, die bei Störung bzw. Ausfall der DV-Anlage infolge eines durch die Sachversicherung gedeckten Schadensereignisses bei Weiterführung des Betriebes - etwa in einem Back-Up-Rechenzentrum - entstehen. Musterbedingungen sind die “Allgemeinen Bedingungen für die Mehrkosten-Versicherung elektronischer Datenverarbeitungsanlagen” (ADVBM).

Betriebsunterbrechungs-Versicherung

Die Computer-Betriebsunterbrechungs-Versicherung deckt den Ertragsausfall ab, den ein Unternehmen infolge eines ersatzpflichtigen Sachschadens erleidet.

Es gibt jedoch eine Reihe von Einschränkungen für die Ersatzleistung. Besondere Beachtung ist der Abgrenzung zur Feuer-Betriebsunterbrechungsversicherung zu schenken.

Computer-Missbrauchversicherung

Die Computer-Missbrauchversicherung bietet Schutz gegen Schäden infolge von Computerkriminalität.

BCP 2.13 Redundante Leitungsführung

Relevanz: Umsetzung/Wartung;

Bei der redundanten Leitungsführung werden zwischen geeigneten Punkten im Netz neben den im normalen Betrieb genutzten Leitungen zusätzliche Verbindungen eingerichtet. Diese sollten über eine andere Trasse und wenn möglich von anderen Postknoten geführt werden. Dadurch besteht die Möglichkeit, bei Störungen auf die redundante Verbindung umzuschalten. Diese Umschaltung kann automatisch oder von Hand erfolgen. Die automatische Umschaltung ist an einer Stelle anzuzeigen, die die Störungsbeseitigung auf der normalen Leitung veranlasst.

Die Funktionsfähigkeit von redundanten Leitungen ist in sinnvollen Zeitabständen durch tatsächliche Nutzung auf ihre Funktionsfähigkeit hin zu überprüfen. Die Dimensionierung, die Prüfintervalle und die grundsätzliche Notwendigkeit von redundanten Leitungen sind direkt von den Verfügbarkeitsanforderungen an das Netz abhängig. Ebenso muss man das Verhältnis der Bereitstellungszeit der redundanten Leitung zur Wiederherstellungszeit der normalen Leitung berücksichtigen. Es ist allerdings von entscheidender Bedeutung, ob es sich um Leitungen im öffentlichen Bereich oder im privaten Bereich handelt.

Bei Leitungen im öffentlichen Bereich hat der/die Benutzer/in keinen Einfluss auf deren Schutz. Das öffentliche Netz stellt grundsätzlich eine ausreichende Zahl von redundanten Leitungen zur Verfügung. Meistens reicht es aus, bei Ausfall einer Verbindung (gleichgültig ob Festverbindung oder Wählleitung) durch Aufbau einer Wählleitung die Verbindung wiederherzustellen. Die Schaltung von redundanten Festverbindungen ist in der Regel zu teuer und meistens verzichtbar.

In einem privaten Netz kann der/die Betreiber/in die Sicherheit von Leitungen wesentlich beeinflussen. Kostenüberlegungen führen meist dazu, dass es keine redundanten Leitungen gibt. In privaten Netzen verursachen redundante Leitungen jedoch außer den Herstellungskosten keine laufenden Ausgaben.

Neben der redundanten Auslegung der Kommunikationsverbindungen ist auch zu überlegen, ob - auch bei Vorhandensein einer zentralen Notstromversorgung - die Notwendigkeit einer redundanten Stromanbindung besteht.

BCP 2.14 Redundante Auslegung der Netzkomponenten

Relevanz: Umsetzung/Wartung;

An die Verfügbarkeit der zentralen Netzkomponenten müssen hohe Anforderungen gestellt werden, da in der Regel viele Benutzer/innen vom reibungslosen Funktionieren eines lokalen Netzes abhängig sind. Damit in einem Fehlerfall der Betrieb so schnell wie möglich wieder aufgenommen werden kann, ist in Abhängigkeit von den entsprechenden Verfügbarkeitsanforderungen im jeweiligen Bereich Redundanz zu schaffen, die einem Teil- oder Totalausfall der relevanten Netzkomponenten mit akzeptablem Aufwand vorbeugt.

Dabei gibt es zwei verschiedene Möglichkeiten, Redundanz zu erreichen:

- Die Netzkomponenten können redundant im Lager vorgehalten werden, um in einem Notfall kurzfristig einen Austausch durchführen zu können. Wird dies nicht beachtet, sind oft langwierige Beschaffungsvorgänge nötig, bevor die Störung behoben werden kann. Alternativ sind Wartungs- bzw. Lieferverträge mit den entsprechenden Herstellern abzuschließen, die einen schnellen Ersatz defekter Komponenten garantieren (s. auch BCP 2.10 Ersatzbeschaffungsplan). Danach können die gesicherten Konfigurationsdaten wieder eingespielt werden, um die Ausfallzeit der betroffenen Netzsegmente so gering wie möglich zu halten.
- Es ist weiterhin sinnvoll, bereits bei der Konzeption des Netzes eine redundante Auslegung der Netzkomponenten einzuplanen. So sollten alle zentralen Switches und je nach den verwendeten Protokollen alle Router zumindest doppelt in das Netz eingebunden sein, um die Anbindung der Server und die Verbindung zwischen den einzelnen Netzkomponenten redundant zu halten. Die korrekte Funktionsweise ist durch eine geeignete logische Netzkonfiguration zu gewährleisten.

Ist je nach Verfügbarkeitsanforderungen auch eine Redundanz im Endgeräte-Bereich nötig, so müssen zusätzlich alle Endgeräte mit zwei Netzadaptern ausgerüstet werden.

Es muss in jedem Fall anhand einer sorgfältigen Analyse festgestellt werden, welche konkreten Verfügbarkeitsanforderungen gegeben sind. Im Rahmen einer detaillierten Planung der System- und Netzarchitektur muss dann ein geeignetes Redundanzkonzept entwickelt werden, welches diesen Anforderungen genügt. In diesem Zusammenhang ist auch die Maßnahme BCP 2.13 Redundante Leitungsführung zu beachten.

7.3 Umsetzung und Test

Relevanz: Management; Umsetzung/Wartung;

BCP 3.1 Durchführung von Disaster Recovery Übungen

Relevanz: Management; Umsetzung/Wartung;

Disaster Recovery Übungen dienen der Prüfung der Wirksamkeit von Maßnahmen im Bereich der Notfallvorsorge. Einerseits wird durch eine Notfallübung der effektive und reibungslose Ablauf eines Disaster Recovery Planes erprobt und andererseits werden bisher unerkannte Mängel aufgedeckt.

Typische Übungen sind:

- die Durchführung einer Alarmierung,
- Durchführung von Brandschutzübungen,
- Funktionstests von Stromaggregaten,
- Wiederanlauf nach Ausfall einer ausgewählten IT-Komponente, wenn möglich unter Einbindung von (ausgewählten) IT-Anwenderinnen und IT-Anwendern und
- Wiedereinspielen von Datensicherungen (vgl. BCP 3.2 Übungen zur Datenrekonstruktion).

Die Ergebnisse einer Disaster Recovery Übung sind zu dokumentieren.

Disaster Recovery Übungen sind regelmäßig zu wiederholen. Da diese Übungen den normalen Betriebsablauf stören können, sollte die Häufigkeit an der Gefährdungslage orientiert sein, jedoch sollten die entsprechenden Disaster Recovery Übungen zumindest einmal jährlich stattfinden. Soweit erforderlich sind Schulungsmaßnahmen der Mitarbeiter/innen durchzuführen (Erste Hilfe, Brandbekämpfung etc.)

Vor Durchführung einer Disaster Recovery Übung ist das Einverständnis der Leitung der Organisation einzuholen.

Aufgedeckte Mängel müssen Konsequenzen, wie etwa eine Überarbeitung der Disaster Recovery Pläne, nach sich ziehen.

BCP 3.2 Übungen zur Datenrekonstruktion

Relevanz: Umsetzung/Wartung;

Durch technische Defekte, falsche Parametrisierung, eine unzureichende Datenträgerverwaltung oder die Nichteinhaltung von Regeln, die in einem Datensicherungskonzept gefordert werden, ist es möglich, dass eine Rekonstruktion eines Datenbestandes nicht durchführbar ist. Die Rekonstruktion von Daten mit Hilfe von Datensicherungsbeständen muss daher sporadisch, zumindest aber nach jeder Änderung des Datensicherungsverfahrens, getestet werden. Hierbei muss nachgewiesen werden, dass eine vollständige Datenrekonstruktion möglich ist.

Auf diese Weise kann zuverlässig ermittelt werden, ob

- die Datenrekonstruktion überhaupt möglich ist,
- die Verfahrensweise der Datensicherung praktikabel ist,
- eine ausreichende Dokumentation der Datensicherung vorliegt, damit ggf. auch ein/e Vertreter/in die Datenrekonstruktion vornehmen kann, und
- die erforderliche Zeit zur Datenrekonstruktion den Anforderungen an die Verfügbarkeit entspricht (siehe BCP 2.1 Definition von Verfügbarkeitsklassen und BCP 2.2 Erstellung einer Übersicht über Verfügbarkeitsanforderungen).

Bei Übungen zur Datenrekonstruktion sollte auch berücksichtigt werden, dass

- die Daten ggf. auf einem Ausweich-IT-System installiert werden müssen,
- für die Datensicherung und Datenrekonstruktion unterschiedliche Schreib-/Lesegeräte benutzt werden.

Es ist sicherzustellen, dass auch eine sachverständige Dritte bzw. ein sachverständiger Dritter die Datenrestaurierung anhand der vorhandenen Dokumentation durchführen kann.

Anhang A: Wichtige Normen

Im Folgenden werden eine Reihe von Normen angeführt, die für die einzelnen Themenbereiche von Interesse sein können. Auf Grund der Vielzahl von nationalen und internationalen Normen können im Rahmen dieses Handbuches keinesfalls alle Dokumente angegeben werden. Es empfiehlt sich daher bei eingehender Beschäftigung mit einem Themenbereich, weitere Recherchen, entweder ausgehend von den angeführten Normen oder über entsprechende Datenbanken oder Institutionen (z.B. ÖNORM), durchzuführen. Hier sei auch besonders auf die in Anhang D angegebenen Internet-Adressen verwiesen.

Normen sind einer laufenden Überprüfung und Weiterentwicklung unterworfen. Daher wurde in den nachfolgenden Zusammenstellungen auf eine Angabe von Status (z.B. Norm, Vornorm, ...) und Ausgabedatum verzichtet.

A 1 Brandschutz

ÖNORMEN:

B 3800	Brandverhalten von Baustoffen und Bauteilen
B 3850	Feuerschutzabschlüsse – Drehflügeltüren und -tore sowie Pendeltüren – Ein- und zweiflügelige Ausführung
B 3858	Türschlösser - Einsteckschlösser für Feuerschutzabschlüsse – Anforderungen und Prüfungen

EN 2	Brandklassen
EN 3	Tragbare Feuerlöscher
EN 54	Brandmeldeanlagen
F 2030	Kennzeichnung für den Brandschutz - Anforderungen, Ausführung, Verwendung und Anbringung
F 2031	Planzeichen für Brandschutzpläne
F 3140	Ionisationsrauchmelder - Strahlenschutzanforderungen
Z 1000 - 1	Sicherheitskennfarben und -kennzeichen - Begriffsbestimmungen, Anforderungen, Ausführungen
Z 1000 - 2	Sicherheitskennfarben und -kennzeichen - Sicherheits- und Gesundheitsschutzkennzeichen
Z 1000 - 1/AC1	Sicherheitskennfarben und -kennzeichen - Begriffsbestimmungen, Anforderungen, Ausführungen (Berichtigung)

TRVB Technische Richtlinie Vorbeugender Brandschutz

Die TRVB werden vom Österreichischen Bundesfeuerwehrverband und den Brandverhütungs-stellen der Länder herausgegeben.

Der Gruppenbuchstabe in der TRVB-Nummer bedeutet:

A = Allgemein
B = Bauwesen
C = Chemie
E = Elektrotechnik
F = Abwehrender Brandschutz
H = Heizungsanlagen, Feuerstätten
L = Landwirtschaft
N = Nutzung von Gebäuden und Gebäudeteilen
O = Organisation
S = Selbsttätige Brandschutzeinrichtungen

Auswahl aus den TRVB:

A 100/87	Brandschutzeinrichtungen - Rechnerischer Nachweis
A 101/67	Grundlagen für die Beurteilung der Brand- und Explosionsgefährlichkeit
E 102/83	Fluchtweg - Orientierungsbeleuchtung
B 109/98	Brennbare Stoffe im Bauwesen
O 119/88	Betriebsbrandschutz - Organisation
O 120/88	Betriebsbrandschutz - Eigenkontrolle
O 121/96	Brandschutzpläne
N 122/97	Erweiterte Automatische Löschhilfe
S 123/96	Brandmeldeanlagen
F 124/97	Erste und Erweiterte Löschhilfe
S 125/98	Rauch- und Wärmeabzugsanlagen
A 126/87	Brandschutztechnische Kennzahlen verschiedener Nutzungen, Lagerungen, Lagergüter
S 127/86	Sprinkleranlagen
F 128/90	Steigleitungen und Wandhydranten
F 134/87	Aufstellungsflächen für die Feuerwehr auf Grundstücken
S 140/96	CO2 - Löschanlagen
B 148/84	Feststellanlagen für Brand- und Rauchabschlüsse
S 151/94	Brandfallsteuerungen
S 152/95	Automatische Löschanlagen, gasförmige Löschmittel

A 2 Sicherheitstüren und einbruchhemmende Türen

ÖNORMEN:

B 5338	Einbruchhemmende Fenster, Türen und zusätzliche Abschlüsse - Allgemeine Festlegungen
B 5453	Einbruchhemmende Türen - Hauptschlösser
B 5455	Einbruchhemmende Türen - Schutzbeschläge für Hauptschlösser
B 5456	Einbruchhemmende Türen - Zusatzschlösser
B 5457	Einbruchhemmende Türen - Schließbleche für Hauptschlösser
B 5458	Einbruchhemmende Türen - Bänder und Bandsicherungen
B 3850	Brandschutztüren - Ein- und zweiflügelige Drehflügeltüren und -tore
B 3855	Rauchabschlüsse - Einflügelige und zweiflügelige Drehflügeltüren aus Stahl oder Holz
B 3858	Türschlösser - Einstemmschlösser (Einsteckschlösser) für Brandschutztüren

A 3 Wertbehältnisse

ÖNORMEN:

EN 1047-1	Wertbehältnisse - Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand - Datensicherungsschränke
EN 1047-2	Wertbehältnisse - Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand - Datensicherungsräume und Datensicherungscontainer
EN 1143	Wertbehältnisse - Anforderungen, Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Einbruchdiebstahl
ENV 1300	Wertbehältnisse - Klassifizierung von Hochsicherheitsschlössern nach ihrem Widerstandswert gegen unbefugtes Öffnen
EN 14450	Wertbehältnisse - Anforderungen, Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Einbruchdiebstahl - Sicherheitsschränke

A 4 Vernichtung von Akten und Daten

ÖNORMEN:

S 2109	Akten- und Datenvernichtung

A 5 Informationssicherheit und IT-Sicherheit

ISO-Normen:

ISO/IEC 7816	Identification cards - Integrated circuit(s) cards with contacts
ISO 9564	Banking - Personal Identification Number (PIN) management and security
ISO/IEC 9594	Information technology - Open Systems Interconnection - The Directory
ISO/IEC 9796	Information technology - Security techniques - Digital signature scheme giving message recovery
ISO/IEC 9797	Information technology - Security techniques - Message Authentication Codes (MACs)
ISO/IEC 9798	Information technology - Security techniques - Entity authentication
ISO/IEC 10116	Information technology - Modes of operation for an n-bit block cipher algorithm
ISO/IEC 10118	Information technology- Security techniques - Hash functions
ISO 10126	Banking - Procedures for message encipherment (wholesale)
ISO/IEC 10181	Information technology - Open systems interconnection - Security frameworks for open systems
ISO/IEC 10536	Identification cards - Contactless integrated circuit(s) cards - Close-coupled cards
ISO 11568	Banking - Key management (retail)
ISO/IEC 11770	Information technology - Security Techniques - Key Management
ISO/IEC TR 13335	Information technology - Guidelines for the management of IT Security
ISO/IEC 13335	Management of information and communications technology security
ISO 13491	Secure Cryptographic devices (retail)
ISO/TR 13569	Banking, securities and other financial services - Information security guidelines
ISO/IEC 13888	Information technology - Security techniques - Non-repudiation
ISO/IEC 14443	Identification cards - Contactless integrated circuit(s) cards - Proximity cards
ISO/IEC 14516	Information technology - Security techniques - Guidelines on the use and management of Trusted Third Party services
ISO/IEC 14888	Information technology - Security techniques - Digital signatures with appendix
ISO/IEC 15292	Information technology - Security techniques - Protection Profile registration procedures
ISO/IEC 15408	Information technology- Security techniques- Evaluation criteria for IT security
ISO/IEC TR 15443	Information technology - Security techniques - A framework for IT security assurance

ISO/IEC 15446	Information technology - Security techniques - Guide for the production of Protection Profiles and Security Targets
ISO/IEC 15693	Identification cards - Contactless integrated circuit(s) cards - Vicinity Cards
ISO/IEC 15816	Information technology - Security techniques - Security information objects for access control
ISO/IEC 15945	Information technology - Security techniques - Specification of TTP services to support the application of digital signatures
ISO/IEC 15946	Information technology - Security techniques - Cryptographic techniques based on elliptic curves
ISO/IEC TR 15947	Information technology - Security techniques – IT intrusion detection framework
ISO/IEC 18014	Information technology - Security techniques – Time-stamping services
ISO/IEC 18028	Information technology - Security techniques – IT network security
ISO/IEC 18031	Information technology - Security techniques – Random bit generation
ISO/IEC 18033	Information technology - Security techniques - Encryption algorithms
ISO/IEC 18043	Information technology - Security techniques - Selection, deployment and operations of intrusion detection systems
ISO/IEB TR 18044	Information technology - Security techniques – Information security incident management
ISO/IEC 17799	Information technology - Code of practice for information security management
ISO/IEC 19790	Information technology - Security techniques – Security requirements for cryptographic modules
ISO IEC/TR 19791	Information technology - Security techniques – Security assessment of operational systems
ISO/IEC 27001	Information technology - Security techniques – Information security management systems
ISO/IEC 27005	Information technology - Security techniques – Information security risk management (in Entwicklung)
ISO/IEC 21827	Information technology -- Systems Security Engineering -- Capability Maturity Model (SSE-CMM)
ISO/IEC 27799	Health informatics – Security management in health using ISO/IEC 17799

ÖNORMEN:

ONR 17700	Informationsverarbeitung - Sicherheitstechnische Anforderungen an Webapplikationen (ON-Regel)

Anhang B: Referenzdokumente

Nachfolgend werden die Dokumente angeführt, auf die im vorliegenden Sicherheitshandbuch direkt Bezug genommen wird. Dabei wird generell die Version angegeben, die bei Erstellung des Handbuches zugrunde gelegt wurde. Da die meisten der nachfolgend angeführten Dokumente regelmäßig oder bei Bedarf aktualisiert werden, empfiehlt es sich, stets auch auf die aktuelle Version eines Dokumentes zu achten.

Die mit (*) gekennzeichneten Dokumente können im Internet unter der Adresse www.cio.gv.at bezogen werden.

Postanschrift:
Bundeskanzleramt
Büro der Informationssicherheitskommission, Ballhausplatz 2, A-1014 Wien
E-Mail: i12@bka.gv.at

[AVB] Allgemeine Vertragsbedingungen der Republik Österreich, Teil des "Beschaffungshandbuches", Version Januar 2001; zum Zeitpunkt der Erstellung des vorliegenden Handbuches sind u.a. verfügbar: AVB Software AVB Softwareerstellung AVB Hardware AVB Wartung AVB Dienstleistungen AVB Projekt In Anhang C sind beispielhaft Auszüge aus den AVB angeführt

[BSI GSHB] Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn: "IT-Grundschutzhandbuch", Version 1999, Bundesanzeiger Verlagsges.mbH, ISBN 3-88784- 915-9, erscheint jährlich, http.//www.bsi.de

[Common Criteria] "Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik" (Common Criteria, CC); vgl. dazu auch ISO/IEC 15408; Die CC können von verschiedenen Servern und Mail-Boxen abgerufen werden, vgl. u.a.: http://csrc.nist.gov/cc/ und http://www.bsi.de/cc/

[IT-BVM] "Bundesvorgehensmodell (IT-BVM), Vorgehensmodell für die Entwicklung von IT-Systemen des Bundes", Version 1.0, April 1999, http://www.bv-modell.at

[ITSEC] Commission of the European Communities, Directorate-General XIII: "Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC)", Amt für Veröffentlichungen der Europäischen Gemeinschaften, Version 1.2 vom Juni 1991, ISBN 92-826-3003-X

[ITSEM] Commission of the European Communities, Directorate-General XIII: "Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM)", Amt für Veröffentlichungen der Europäischen Gemeinschaften, Version 1.0 vom September 1993, publ. 1994, ISBN 92-826-7078-2

[IKT-LDAP] Kooperation Bund / Länder / Gemeinden: "Spezifikation LDAP-gv.at", Version 2.0.1 vom Feber 2002

[ITU-T] International Telecommunications Union (ITU) - Telecommunications Standardization Sector (ITU-T)

[IKT-CLWLAN] Stabsstelle IKT-Strategie des Bundes: “Checkliste WLAN“, Version 1.0 vom Juni 2004.

[IKT-IPOL] Stabsstelle IKT-Strategie des Bundes, E-Government Bund-Länder-Gemeinden: "Internet-Policy", Version 1.0.2 vom Mai 2004

[IKT-MPOL] Stabsstelle IKT-Strategie des Bundes, E-Government Bund-Länder-Gemeinden: "E-Mail-Policy", Version 2.0.1 vom September 2004.

[IKT-MZERT] Stabsstelle IKT-Strategie des Bundes: "Richtlinien für E-Mail-Zertifikate in der Verwaltung", Version 1.0.1 vom Jänner 2003.

[IKT-PKI] Stabsstelle IKT-Strategie des Bundes: “ PKI in der Verwaltung - Allgemeine Richtlinien für den Einsatz von PKI in der Verwaltung“, Version 0.9 vom April 2003.

[IKT-PVP] Kooperation Bund / Länder / Gemeinden: "Portal Verbund Whitepaper", Version 1.0 vom Feber 2002

[IKT-SZERT] Stabsstelle IKT-Strategie des Bundes: "Richtlinien für Serverzertifikate", Version 1.0.4 vom April 2003.

[IKT-WLAN] Bundeskanzleramt, IT-Koordination: "Beachtens- und Wissenswertes zu WLANs in der Verwaltung", Version 1.3 vom Mai 2003

[IKT-ZERT] Bundeskanzleramt, IT-Koordination: "Object Identifier der öffentlichen Verwaltung", Version 1.0.2 vom Feber 2003

[KFall] Bundeskanzleramt: "Katastrophenvorsorge- und Ausfallssicherheitsüberlegungen im IT-Bereich", vom Oktober 2002

[KIT S01] Bundeskanzleramt, Büro der Informationssicherheitskommission: „Österreichisches Informationssicherheitshandbuch, Teil 1: Informationssicherheitsmanagement", Version 2.3 vom April 2007

[KIT S04] Bundeskanzleramt, IT-Koordination: "Richtlinien des Fachausschusses für Netzwerke der KIT zur gesicherten Anbindung an Fremdnetzwerke" ("AFNW-Richtlinien"), Version vom 1.9.2000, verfügbar über (*)

[KIT T05] Bundeskanzleramt, IT-Koordination: "Festlegung technischer Standards für Dokumentenübermittlung", Richtlinien Kommunikationsformate des Fachausschusses für Netzwerke, Version 1.1 vom 7.4.1999, verfügbar über (*)

[NSA-CIS2] National Security Agency (NSA) - System and Network Attack Center (SNAC), Router Security Configuration Guide, September 2002

[NSA-EEC1] National Security Agency (NSA) - System and Network Attack Center (SNAC), E-mail Security in the Wake of Recent Malicious Code Incidents, Jänner 2002

[NSA-SD2] National Security Agency (NSA) - System and Network Attack Center (SNAC), Guide to the Secure Configuration and Administration of iPlanet Web Server, Enterprise Edition 4.1, Juli 2001

[NSA-SD3] National Security Agency (NSA) - System and Network Attack Center (SNAC), Guide to the Secure Configuration and Administration of Microsoft Internet Information Server 4.0, März 2002

[NSA-SD4] National Security Agency (NSA) - System and Network Attack Center (SNAC), Guide to the Secure Configuration and Administration of Microsoft Internet Information Server 4.0, März 2002

[NSA-SD5] National Security Agency (NSA) - System and Network Attack Center (SNAC), Secure Configuration of the Apache Web Server, April 2001

[NSA-SD7] National Security Agency (NSA) - System and Network Attack Center (SNAC), The 60 Minute Network Security Guide, Juli 2002

[NSA-SD8] National Security Agency (NSA) - System and Network Attack Center (SNAC), Guide to Securing Microsoft Internet Explorer 5.5 Using Group Policy, Juli 2002

[NSA-SD10] National Security Agency (NSA) - System and Network Attack Center (SNAC), Guide to Securing Netscape Navigator 7.0, Dezember 2002

Anhang C: Muster für Verträge, Verpflichtungserklärungen und Inhaltsverzeichnisse

C.1 Sourcecodehinterlegung (Muster, aus AVB-IT)

Muster aus AVB-IT, Version 1.07, abgerufen am 4.Mai 2007 – Abschnitt 2.8:

Lieferung bzw. Hinterlegung des Sourcecodes von Softwarekomponenten

Der Sourcecode von Individualsoftware und individuellen Softwareanpassungen (inkl. Datenbankscripts oder Java-Scripts udgl.) ist auf einem Datenträger, der auf dem System des Auftraggebers gelesen werden kann, samt der dazugehörigen Dokumentation (Inhalt und Aufbau des Datenträgers, Programm und Datenflusspläne, Testverfahren, Testprogramme, Fehlerbehandlung usw.) mitzuliefern.

Bei Standardsoftware, die nicht im Einflussbereich des Auftragnehmers liegt, d.h. Standardsoftware, an der die Rechte am Sourcecode bei einem Dritten - meist dem Hersteller - liegen, kommt eine Sourcecode Hinterlegung nicht in Betracht.

Um bei Standardsoftware, die im Einflussbereich des Auftragnehmers liegt (mit Ausnahme eingebundener Drittprodukte), einschließlich aller ihrer Änderungen die weitere Fehlerbehebung und Wartung einschließlich aller Änderungen für den Fall der Handlungsunfähigkeit des Auftragnehmers und den Fall der Einstellung der Weiterentwicklung oder Wartung sicherzustellen, wird der Auftragnehmer die Software auf einem Datenträger, der auf dem System des Auftraggebers gelesen werden kann, im Sourcecode bereitstellen und in den Maschinencode übersetzen sowie die Installation auf dem System vornehmen. Nach der Installation wird dieser Datenträger mit dem Sourcecode samt der dazugehörigen Dokumentation (Inhalt und Aufbau des Datenträgers, Programm und Datenflusspläne, Testverfahren, Testprogramme, Fehlerbehandlung usw.) vom Auftragnehmer versiegelt und bei einer neutralen Stelle (insbesondere einem Notar, Rechtsanwalt) hinterlegt.

Die Kosten der Hinterlegung sind vom Auftraggeber zu tragen.

Der Datenträger muss die Software in den ursprünglichen Programmiersprachen zum Zeitpunkt der Installation einschließlich aller seitherigen Änderungen sowie die Dokumentation - soweit sie in maschinenlesbarer Form vorliegt - enthalten. Eine Dokumentation, die nicht maschinenlesbar vorliegt, ist in einer ohne Hilfsmittel lesbaren Kopie beizulegen. In jedem Fall jedoch ist eine ohne Hilfsmittel lesbare Aufstellung der hinterlegten Gegenstände und eine Anweisung, wie der Datenträger auf dem System des Auftraggebers gelesen und der Vertragsgegenstand installiert werden muss, beizulegen.

Die Hinterlegung bzw. Übergabe wird bei jeder Lieferung einer neuen Version der Software binnen 2 Monaten ab Einsatzbeginn der jeweils neuen Version wiederholt. Sollten mehrere Änderungen innerhalb von sechs Monaten erfolgen, ist die Hinterlegung jedoch nur einmal pro sechs Monate erforderlich.

Tritt beim Auftragnehmer Handlungsunfähigkeit ein oder stellt er trotz auftraggeberseitig ungekündigten Wartungsvertrages die Weiterentwicklung oder Wartung der Software ein, so ist der Auftraggeber berechtigt, die Siegel des hinterlegten Datenträgers zu brechen und den Vertragsgegenstand im Sourcecode samt der Dokumentation entweder einem sachkundigen

Unternehmen zu übergeben und dieses mit der weiteren Fehlerbehebung und Wartung des Vertragsgegenstandes zu beauftragen oder sie selbst durchzuführen.

Als Handlungsunfähigkeit gelten Liquidation, Eröffnung eines Konkursverfahrens oder Abweisung eines Konkursantrages mangels Masse oder zumindest zwei erfolglose Exekutionsversuche wider den Auftragnehmer.

Es gilt jedoch nicht als Handlungsunfähigkeit, wenn ein Dritter die Leistungen des Auftragnehmers in vollem Umfang übernimmt und der Auftraggeber dieser Vertragsübernahme zustimmt.

Anmerkung: Eine aktuelle Version der Allgemeinen Vertragsbedingungen der Republik Österreich für die Lieferung, Implementierung, Einführung und Wartung von IT-Systemen, Internetapplikationen bzw. sonstigen IT-Dienstleistungen, kurz AVB-IT, findet sich im Internet unter den Seiten der Bundesbeschaffung GmbH (BBG, vgl. Anhang B).

C.2 Musteranwendung MA002 Zutrittskontrollsysteme

(Muster, Auszug aus der Standard- und Muster-Verordnung 2004 (StMV 2004), BGBl. II Nr. 312/2004)

Zweck der Datenanwendung:

Kontrolle der Berechtigung des Zutritts zu Gebäuden und abgegrenzten Bereichen durch den Eigentümer oder Benutzungsberechtigten mit Hilfe von Anlagen, die personenbezogene Daten automationsunterstützt ermitteln und speichern, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in dieser Angelegenheit.

Rechtsgrundlagen der Anwendung sind insbesondere die folgenden Gesetze und Verordnungen (in der geltenden Fassung):

§ 96a Abs. 1 Z 1 ArbVG und § 9 Abs. 2 lit. f PVG

Höchstdauer der zulässigen Datenaufbewahrung:

Bis zum Ende der Zutrittsberechtigung und darüber hinaus solange als gesetzliche Aufbewahrungsfristen bestehen oder solange besondere Rechtsansprüche aus dem Arbeitsverhältnis gegenüber dem Arbeitgeber geltend gemacht werden können. Sofern keine besonderen Aufbewahrungsfristen bestehen, sollen die Daten sechs Monate nach Ende der Zutrittsberechtigung gelöscht werden.

Betroffene Personen-gruppen:	Nr:	Datenarten:	Empfängerkreise:
Zutrittsberechtigte:	01	Ordnungsnummer	---
	02	Bereichsspezifisches Personenkennzeichen (nur bei Dienstnehmern eines Auftraggebers des öffentlichen Bereiches): Personalverwaltung (PV)	1
	03	Vor- und Familienname, akad. Grad/Standesbezeichnung	---
	04	Geschlecht	---
	05	Beziehung des Betroffenen zum Auftraggeber (Mitarbeiter, Kunde, sonstiger Besucher)	---
	06	Telefon-, Faxnummer, und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikations-techniken ergeben, sofern dies zur raschen Verständigung des Betroffenen erforderlich ist	---
	07	Lichtbild des Betroffenen, sofern dies als zusätzliche Sicherheitsmaßnahme erforderlich ist	---
	08	Zutrittscode	---
	09	Vom Berechtigten einzugebender Berechtigungscode	---
	010	Daten der Zutrittsberechtigung, insbesonders die Bereiche und Zeiten, für die die Berechtigung gilt, die Sicherheitsstufe, ebenso besondere Befugnisse wie z.B. das Recht, mit einem Fahrzeug in den geschützten Bereich einzufahren	---
	11	Gültigkeitsdauer der Zutrittsberechtigung	---

C.3 Fehlerklassen Wartung (Muster, aus AVB Wartung)

Muster aus AVB-IT, Version 1.07, abgerufen am 4.Mai 2007 – Abschnitt 2.18:

Fehlerklassen

Die Zuordnung zu den Fehlerklassen erfolgt einvernehmlich. Im Zweifelsfall hat der Auftragnehmer vor einvernehmlicher Klärung zunächst Maßnahmen auf Basis der Klassifizierung des Auftraggebers zu setzen, um Nachteile für den Auftraggeber zu vermeiden.

Klasse 1 - „kritisch“

Die zweckmäßige Nutzung eines Teiles des IT-Systems oder des IT-Gesamtsystems ist nicht möglich oder unzumutbar eingeschränkt. Der Fehler hat schwerwiegenden Einfluss auf die Geschäftsabwicklung oder Sicherheit. Das sind vor allem Fehler, die eine weitere Verarbeitung ausschließen.

Funktionsbezogene Beispiele: Systemstillstand ohne Wiederanlauf, Datenverlust/Datenzerstörung, falsche Ergebnisse bei zeitkritischer Massenverarbeitung von Daten.

Maßnahmen: Der Auftragnehmer beginnt während der Wartungsbereitschaftszeit spätestens innerhalb der vereinbarten Reaktionszeit mit der Bearbeitung des Fehlers durch qualifiziertes Personal, sorgt kurzfristig (angestrebt wird grundsätzlich 8 Arbeitsstunden ab Beginn der Fehlerbehebung) zumindest für eine Umgehung und sorgt soweit möglich kurzfristig für eine Fehlerbehebung z. B. durch Austausch von Hardwarekomponenten, Umkonfiguration von Software, Behebung von Softwarefehlern durch Patches. Darüber hinaus meldet der Auftragnehmer den Fehler – ausgenommen Abnutzungsfehler – umgehend und mit hoher Priorität an einen vom Auftragnehmer verschiedenen Hersteller.

Klasse 2 - „schwer“

Die zweckmäßige Nutzung eines Teiles des IT-Systems oder des IT-Gesamtsystems ist ernstlich eingeschränkt. Der Fehler hat wesentlichen Einfluss auf die Geschäftsabwicklung oder Sicherheit, lässt aber eine Weiterarbeit zu.

Funktionsbezogene Beispiele: falsche oder inkonsistente Verarbeitung, spürbare Unterschreitung der vereinbarten Leistungsdaten des IT-Systems, Häufung von kurzfristigen Störungen des IT-Betriebes.

Maßnahmen: Der Auftragnehmer beginnt während der Wartungsbereitschaftszeit innerhalb der vereinbarten Reaktionszeit mit der Bearbeitung des Fehlers durch qualifiziertes Personal, sorgt mittelfristig zumindest für eine Umgehung und sorgt soweit möglich mittelfristig für eine Korrektur der Fehlerursache z. B. durch Austausch von Hardwarekomponenten, Umkonfiguration von Software, Behebung von Softwarefehlern durch Patches. Darüber hinaus meldet der Auftragnehmer den Fehler – ausgenommen Abnutzungsfehler – umgehend an einen vom Auftragnehmer verschiedenen Hersteller.

Klasse 3 - „leicht“

Die zweckmäßige Nutzung eines Teiles des IT-Systems oder des IT-Gesamtsystems ist leicht eingeschränkt. Der Fehler hat unwesentlichen Einfluss auf die Geschäftsabwicklung oder Sicherheit, lässt jedoch eine weitere Verarbeitung uneingeschränkt zu.

Funktionsbezogene Beispiele: falsche Fehlermeldung/ein Programm geht in einen Wartezustand und kann nur durch Betätigen einer Taste wieder aktiviert werden.

Maßnahmen: Der Auftragnehmer beginnt in angemessener Zeit mit der Bearbeitung des Fehlers durch qualifiziertes Personal und sorgt soweit möglich für eine Korrektur der Fehlerursache z. B. durch Austausch von Hardwarekomponenten, Umkonfiguration von Software, Behebung von Softwarefehlern im Rahmen der Releasepolitik. Darüber hinaus meldet der Auftragnehmer den Fehler – ausgenommen Abnutzungsfehler – an einen vom Auftragnehmer verschiedenen Hersteller.

Klasse 4 - „trivial“

Die zweckmäßige Nutzung des IT-Systems oder des IT-Gesamtsystems ist ohne Einschränkung möglich. Der Fehler hat keinen oder nur geringfügigen Einfluss auf die Geschäftsabwicklung oder Sicherheit. Das sind vor Allem Schönheitsfehler oder Fehler, die von Mitarbeitern des Auftraggebers selbst umgangen werden können.

Funktionsbezogene Beispiele: Störende zusätzliche Ausgaben am Bildschirm, Dokumentationsfehler/Schreibfehler.

Maßnahmen: Der Auftragnehmer sorgt ohne besondere Priorität im Rahmen geplanter vorbeugender Wartung oder der Releasepolitik für die Fehlerbehebung.

Anmerkung: Eine aktuelle Version der Allgemeinen Vertragsbedingungen der Republik Österreich für die Lieferung, Implementierung, Einführung und Wartung von IT-Systemen, Internetapplikationen bzw. sonstigen IT-Dienstleistungen, kurz AVB-IT, findet sich im Internet unter den Seiten der Bundesbeschaffung GmbH (BBG, vgl. Anhang B).

C.4 Verpflichtungserklärung betreffend die Benutzung von IT-Systemen (Muster)

Verpflichtungserklärung
betreffend die Benutzung der IT-Systeme des *(Dienststelle)*

Name, Titel: .....Organisationseinheit: …….....

Als Bedienstete(r) des *(Dienststelle)* nehme ich hiermit zur Kenntnis, dass

- das unbefugte Kopieren und die unbefugte Weitergabe von Software strafrechtlich verfolgbar ist;
- die unbefugte Installation, Nutzung und Weitergabe von Software als Verletzung der Dienstpflichten geahndet wird;
- zur Beschaffung von Hardware und Software nur die geschäftseinteilungsmäßig berechtigten Bediensteten der Abteilung „XX“ *(z.B. IT-Abteilung)* und die Bediensteten des Präsidiums berechtigt sind;
- zur Installation, Reparatur und Veränderung von Hardware und Software nur Bedienstete der Abteilung „XX“ *(z.B. IT-Abteilung)* im Rahmen ihrer dienstlichen Obliegenheiten bzw. Personen im Auftrag der Abteilung „XX“ *(z.B. IT-Abteilung)* berechtigt sind;
- die Abteilung „XX“ *(z.B. IT-Abteilung)* berechtigt ist, alle EDV-Systeme auf Kopien von unbefugt eingespielter Software zu prüfen, solche Softwarekopien zu löschen und verpflichtet ist, den Vorfall der Abteilung „YY“ *(z.B. Personalabteilung)* zu melden.

Ich nehme weiters nachstehende urheberrechtliche Bestimmungen zur Kenntnis:

- Originalsoftware darf ausschließliche insofern vervielfältigt und bearbeitet werden, als dies für ihre bestimmungsgemäße Benutzung durch die/den zu Benutzung Berechtigte/n notwendig ist (Arbeits- und Sicherungskopien);
- dem *(Dienststelle)* als Dienstgeber steht gemäß § 40b des Urheberrechtsgesetzes, BGBl. Nr. 111/1936, in der geltenden Fassung, ein unbeschränktes Werknutzungsrecht an allen von mir in Erfüllung meiner dienstlichen Obliegenheiten geschaffenen Computerprogrammen zu.

Um die Sicherheit des Computernetzwerkes und die Einhaltung der Software-Lizenzbestimmungen gewährleisten zu können, bestätige ich die Einhaltung folgender Benutzungsregeln:

- für die Vertraulichkeit der „Benutzerkennung“, die mir von einer/einem Bediensteten der Abteilung „XX“ *(z.B. IT-Abteilung)* mitgeteilt wurde, ist Sorge zu tragen;
- die Anwender/innen dürfen keine zusätzliche Hardware und Software auf dem PC installieren bzw. verwenden;
- die von der Abteilung „XX“ *(z.B. IT-Abteilung)* vorgegebene Konfiguration (Hard- und Software) darf nicht verändert werden, eine Änderung aus Versehen ist zum Schutz des gesamten Systems unverzüglich der Abteilung „XX“ *(z.B. IT-Abteilung)* zu melden;
- die Sicherung der lokal auf einem (nicht vernetzten) Einzelplatz-PC gehaltenen Daten hat in Eigenverantwortung zu erfolgen.

Weiters verpflichte ich mich, die Erklärung zur Einhaltung des Datengeheimnisses gemäß §15 Datenschutzgesetz 2000 ebenfalls nachweislich zur Kenntnis zu nehmen.

(Datum, Unterschrift)

C.5 Vereinbarung betreffend die Überlassung von Daten (Muster)

Anmerkung:
Die in Kursivschrift gehaltenen Passagen sind nur für Dienstleistungen (DL) im Ausland anzuwenden und bei Inland-DL wegzulassen.

Vereinbarung

betreffend die Überlassung von Daten *in das Ausland* zum Zweck der Verarbeitung als Dienstleistung gemäß § 10 *in* Verbindung *mit § 12 (und/oder § 13)* des *österreichischen* Datenschutzgesetzes 2000, BGBl. I Nr. 165/1999 (in der Folge DSG 2000) zwischen:

(im folgenden Auftraggeber/in)	(im folgenden Dienstleister/in)

Durchzuführende Arbeiten (bzw. Verarbeitungen):

1. Der/Die Dienstleister/in pflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich dem/der Auftraggeber/in zurückzugeben oder nur nach dessen schriftlichem Auftrag zu übermitteln. Desgleichen bedarf eine Verwendung der überlassenen Daten für eigene Zwecke des Dienstleisters bzw. der Dienstleisterin eines derartigen schriftlichen Auftrages.

2. Der/Die Dienstleister/in erklärt rechtsverbindlich, dass er/sie alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Wahrung des Datengeheimnisses im Sinne des § 15 DSG 2000 verpflichtet hat. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit dem Datenverkehr beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Dienstleister bzw. bei der Dienstleisterin aufrecht. Die Verpflichtung zur Verschwiegenheit ist auch für Daten von juristischen Personen und handelsrechtlichen Personengesellschaften einzuhalten.

3. Der/Die Dienstleisterin erklärt rechtsverbindlich, dass er ausreichende Sicherheitsmaßnahmen im Sinne des § 14 DSG 2000 ergriffen hat, um zu verhindern, dass Daten ordnungswidrig verwendet oder Dritten unbefugt zugänglich werden.

[Wählen Sie unter den Optionen 4.a. bis 4.c. <u>eine</u> aus und streichen Sie die anderen.]

4.a. Der/Die Dienstleister/in ist nicht berechtigt, einen/eine Subverarbeiter/in heranzuziehen.

ODER

4.b. Der/Die Dienstleister/in kann ein anderes Unternehmen nur dann mit der Durchführung von Verarbeitungen betrauen, wenn der/die Auftraggeber/in zustimmt. Er/Sie muss jedoch mit dem/der Subverarbeiter/in einen Vertrag im Sinne des § 10 DSG 2000 abschließen. In diesem Vertrag hat der/die Dienstleister/in sicherzustellen, dass der/die Subverarbeiter/in dieselben Verpflichtungen eingeht, die dem/der Dienstleister/in auf Grund dieser Vereinbarung obliegen.

ODER

4.c. Der/Die Dienstleister/in kann ein anderes Unternehmen auch ohne Zustimmung des Auftraggebers bzw. der Auftraggeberin zur Durchführung von Verarbeitungen heranziehen. Er hat jedoch den/die Auftraggeber/in von der beabsichtigten Heranziehung eines Subverarbeiters bzw. einer Subverarbeiterin so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann. Außerdem muss ein Vertrag zwischen dem/der Dienstleister/in und dem/der Subverarbeiter/in im Sinne des § 10 DSG 2000 geschlossen werden. In diesem Vertrag hat der/die Dienstleister/in sicherzustellen, dass der/die Subverarbeiter/in dieselben Verpflichtungen eingeht, die dem/der Dienstleister/in auf Grund dieser Vereinbarung obliegen.

5. Der/Die Dienstleister/in trägt für die technischen und organisatorischen Voraussetzungen Vorsorge, dass der/die Auftraggeber/in die Bestimmungen der § 26 (Auskunftsrecht) und § 27 (Recht auf Richtigstellung oder Löschung) DSG 2000 gegenüber dem/der Betroffenen innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem/der Auftraggeber/in alle dafür notwendigen Informationen.

6. Der/Die Dienstleister ist nach Beendigung der Dienstleistung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem/der Auftraggeber/in zu übergeben bzw. in dessen/deren Auftrag für ihn/sie weiter vor unbefugter Einsicht gesichert aufzubewahren oder auftragsgemäß zu vernichten.

7. Der/Die Auftraggeber/in verpflichtet sich, den/die Dienstleister/in unmittelbar von Änderungen des *österreichischen* Datenschutzgesetzes 2000 und ergänzender Bestimmungen zu unterrichten. Der/Die Auftraggeber/in räumt dem/der Dienstleister/in eine angemessene Frist ein, sich auf geänderte Datenschutzbestimmungen einzustellen.

8. Dem/Der Auftraggeber/in wird hinsichtlich der Verarbeitung der von ihm/ihr überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle der *ausländischen* Datenverarbeitungseinrichtungen eingeräumt.

Für den/die Auftraggeber/in	Für den/die Dienstleister/in
.....	.....
unterzeichnet am:	unterzeichnet am:
.....	.....

C.6 Verpflichtungserklärung zur Einhaltung des DSG 2000 für öffentlich Bedienstete (Muster)

Verpflichtungserklärung für Dienstnehmer/innen, welche in einem öffentlich rechtlichen Dienstverhältnis stehen, zur Einhaltung des Datengeheimnisses gemäß § 15 Datenschutzgesetz 2000 und zur Verschwiegenheit bezüglich sonstiger Dienst- und Amtsvorgänge

Ich nehme zur Kenntnis, dass ich - unbeschadet der auch anderen gesetzlichen Bestimmungen über die Geheimhaltungspflicht (Amtsverschwiegenheit, u.a.) – jedenfalls automationsunterstützt oder konventionell verarbeitete Daten, die mir in Ausübung meines Dienstes anvertraut oder zugänglich gemacht worden sind, nur unter Einhaltung der Bestimmungen des Datenschutzgesetzes 2000 (DSG 2000) und der innerorganisatorischen Datenschutzvorschriften - insbesondere der Datensicherheitsvorschriften - verwenden darf.

Ich nehme des weiteren zur Kenntnis, dass Verstöße gegen die oben angeführte Verpflichtung zu entsprechender strafrechtlicher Verfolgung führen können, schadenersatzpflichtig machen und auch dienstrechtliche Folgen nach sich ziehen können (z.B. Entlassung, Kündigung).

Aus einer Verweigerung der Ausführung eines Auftrages, der gegen das Datengeheimnis verstoßen würde, darf mir kein Nachteil erwachsen (§ 15 Abs. 4 DSG 2000).

In Durchführung der o.a. Ausführungen verpflichte ich mich insbesondere

- zur absoluten Verschwiegenheit über alle Daten, die mir ausschließlich auf Grund meiner berufsmäßigen Beschäftigung anvertraut worden sind, sofern sie nicht von den zuständigen Organwalterinnen und Organwaltern ausdrücklich als unbedenklich bezeichnet wurden,
- dafür zu sorgen, dass Unbefugte keinen Zugang zu derartigen Daten erhalten können,
- Daten, die mir in Ausübung meines Dienstes bekannt geworden sind, nur zu dem zum jeweiligen rechtmäßigen Aufgabenvollzug gehörenden Zweck zu verwenden,
- Daten nur auf Anordnung einer befugten Organwalterin bzw. eines befugten Organwalters zu übermitteln,
- diese Verpflichtung auch nach Beendigung meines Dienstverhältnisses einzuhalten.

..... (Unterschrift)		..... (Datum)
..... (vollst. Name, akad. Grad)	..... (Amtstitel)	..... (Dienststelle/Org. Einheit)

C.7 Verpflichtungserklärung zur Einhaltung des DSG 2000 für Dienstnehmer/innen eines (privaten) Dienstleisters (Muster)

Verpflichtungserklärung für Dienstnehmer/innen - welche im Rahmen ihrer Tätigkeit für einen (privaten) Dienstleister einer öffentlich rechtlichen Körperschaft oder im Rahmen eines Arbeitskräfteüberlassungsvertrages tätig sind - zur Einhaltung des Datengeheimnisses gemäß § 15 Datenschutzgesetz 2000 und zur Verschwiegenheit bezüglich sonstiger bekannt gewordener Dienst- und Amtsvorgänge

Diese Verpflichtungserklärung betrifft:

Familienname: _____ (in BLOCKSCHRIFT)

Vornamen: _____ (in BLOCKSCHRIFT)

1) VERPFLICHTUNGSERKLÄRUNG

Im Zuge Ihres Dienstverhältnisses erhalten Sie voraussichtlich Kenntnis über Personen und personenbezogene Umstände und Daten sowie über technische Daten betreffend die technische Infrastruktur und den strukturellen Aufbau von Datenanwendungen.
Alle diese Daten sind absolut vertraulich zu behandeln und unterliegen den Bestimmungen des österreichischen Datenschutzgesetzes.

Mit Ihrer Unterschrift verpflichten Sie sich daher:

- das Datengeheimnis gemäß den Bestimmungen des Datenschutzgesetzes i.d.g.F., insbesondere § 15 DSG 2000 (Datengeheimnis) zu wahren.
- zu absoluter Verschwiegenheit über alle, Ihnen anlässlich Ihrer Tätigkeit bekannt gewordenen, nicht von den zuständigen Personen ausdrücklich als unbedenklich bezeichneten Dienst- und Amtsvorgänge.

Mit Ihrer Unterschrift verpflichten Sie sich weiters:

- unbefugten Personen oder unzuständigen Stellen die Kenntnisnahme von Daten, die Ihnen in Ausübung Ihres Dienstes bekannt geworden sind, nicht zu ermöglichen, sowie solche Daten nicht zu einem anderen als dem zum jeweiligen rechtmäßigen Aufgabenvollzug gehörenden Zweck zu verwenden,
- automationsunterstützt oder manuell verarbeitete Daten, die Ihnen auf Grund Ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger Verschwiegenheitspflichten, nur auf Grund einer ausdrücklichen mündlichen oder schriftlichen Zustimmung des Bundesministeriums für Inneres oder dessen Beauftragten zu verwenden,
- diese Verpflichtung auch nach Beendigung Ihres Mitarbeiterverhältnisses und dem Ausscheiden aus der Firma einzuhalten.

Sie nehmen durch Ihre Unterschrift zur Kenntnis,

- dass weiterreichende andere Bestimmungen über die Geheimhaltungspflicht von der oben angeführten Verpflichtung unberührt bleiben, sofern sie nicht mit dem Datenschutzgesetz im Widerspruch stehen,
- dass als Dienst- und Amtsvorgänge insbesondere jene zur Kenntnis gelangten Vorgänge zu verstehen sind, die dienstinterner Natur sind, oder die Rechte Dritter berühren;
- dass Verstöße gegen die oben angeführte Verpflichtung zu entsprechender strafrechtlicher Verfolgung führen können, schadenersatzpflichtig machen und auch arbeitsrechtliche Folgen haben können (z.B. Entlassung gemäß § 27 Angestelltengesetz).

_____ _____

Ort, Datum Unterschrift des/der Verpflichteten

2) VERPFLICHTUNGSBESTÄTIGUNG

- Herr/Frau ..... hat die oben stehende Verpflichtung in meiner Gegenwart unterschrieben.

- Dem/Der Verpflichteten sind vor der Unterschriftleistung folgende Vorschriften ausgehändigt worden:

  .....

_____ _____

Ort, Datum Unterschrift des/der Verpflichtenden

C.8 Verpflichtungserklärung zur Nutzung von dienstlich beigestellten mobilen Arbeitsplatzrechnern (Notebooks) (Muster)

Der/Die Notebook-Benutzer/in verpflichtet sich,

- das zugeteilte Notebook und den Zugang zu den organisationseigenen Ressourcen mittels Datenfernübertragungseinrichtung ausschließlich für dienstliche Zwecke zu verwenden;
- die unzulässige Verwendung des zugeteilten Notebooks und die zugeteilten Einwählparameter durch dritte Personen auf geeignete Art und Weise zu verhindern;
- mit dem zur Verfügung gestellten technischen Equipment nur von der Dienstgeberin bzw. vom Dienstgeber vorkonfigurierten bzw. bekannt gegebenen Wählverbindungen zu nutzen und keine Verbindungen zu anderen IT-Providern bzw. IT-Systemen, weder über Wählleitungsverbindungen noch über sonstige lokale Verbindungsmöglichkeiten (z.B. USB, Infrarot, RS232, Ethernet, Token Ring usw.), herzustellen;
- niemals gleichzeitig zwei oder mehrere DFÜ-Verbindungen zu unterschiedlichen IT-Systemen zu betreiben;
- bei Verbindungen zu Fremdsystemen erhöhte Vorsicht in sicherheitstechnischer Hinsicht walten zu lassen;
- für den Zugang zu den organisationseigenen Ressourcen mittels Datenfernübertragungseinrichtungen nur ein von der Arbeitgeberin bzw. vom Arbeitgeber zur Verfügung gestelltes, speziell gesichertes, technisches Equipment zu nutzen;
- in das Notebook von extern eingebrachte Daten unverzüglich und bestmöglich auf Computerviren zu prüfen und die Prüfsoftware in kürzestmöglichen Abständen auf Aktualität zu überprüfen und gegebenenfalls die Aktualität des Systems herzustellen;
- sich nach den Grundsätzen der Zweckmäßigkeit und Sparsamkeit zu bemühen, die Kosten für Einwahlverbindungen möglichst gering zu halten und nur jene Daten abzurufen, die für den dienstlichen Gebrauch nötig sind;
- bei der Verwendung von nicht durch die EDV-Abteilung zur Verfügung gestellten Programmen alle lizenzrechtlichen Bestimmungen zu beachten;
- Service und Reparaturen nur durch den Arbeitgeber bzw. von diesem benannte Fachwerkstätten durchführen zu lassen;
- alle datenschutzrechtlichen und das Amtsgeheimnis betreffenden Bestimmungen einzuhalten.

Die IT-Sicherheits-Verantwortlichen behalten sich das Recht vor, aktive Netzwerkverbindungen einer Benutzerin bzw. eines Benutzers sofort zu unterbrechen, wenn eine unzulässige Verwendung entdeckt wird.

_____
Name der/des Bediensteten

_____
Datum und Unterschrift der/des Bediensteten

C.9 Verpflichtungserklärung zur Nutzung von dienstlich beigestellten mobilen Arbeitsplatzrechnern (Notebooks) mit Zugangsmöglichkeit zu zentralen Ressourcen mittels Datenfernübertragungseinrichtungen (RAS-Zugang) (Muster)

Der/Die Notebook-Benutzer/in verpflichtet sich,

- das zugeteilte Notebook und den Zugang zu den organisationseigenen Ressourcen mittels Datenfernübertragungseinrichtung ausschließlich für dienstliche Zwecke zu verwenden;
- die unzulässige Verwendung des zugeteilten Notebooks und die zugeteilten Einwählparameter durch dritte Personen auf geeignete Art und Weise zu verhindern;
- mit dem zur Verfügung gestellten technischen Equipment nur die durch die EDV-Abteilung vorkonfigurierten bzw. bekannt gegebenen Wählverbindungen zu nutzen und keine Verbindungen zu anderen IT-Providern bzw. IT-Systemen, weder über Wählleitungsverbindungen noch über sonstige lokale Verbindungsmöglichkeiten (z.B. USB, Infrarot, RS232, Ethernet, Token Ring u.s.w.), herzustellen;
- niemals gleichzeitig zwei oder mehrere DFÜ-Verbindungen zu unterschiedlichen IT-Systemen zu betreiben;
- bei Verbindungen zu Fremdsystemen erhöhte Vorsicht in sicherheitstechnischer Hinsicht walten zu lassen;
- für den Zugang zu den BMI-Ressourcen mittels Datenfernübertragungseinrichtungen nur das von der Arbeitgeberin bzw. vom Arbeitgeber zur Verfügung gestellte technische Equipment zu nutzen;
- in das Notebook von extern eingebrachte Daten unverzüglich und bestmöglich auf Computerviren zu prüfen und die Prüfsoftware in kürzestmöglichen Abständen auf Aktualität zu überprüfen und gegebenenfalls die Aktualität des Systems herzustellen;
- sich nach den Grundsätzen der Zweckmäßigkeit und Sparsamkeit zu bemühen, die Netzwerkbelastungen möglichst gering zu halten und nur jene Daten abzurufen, die für den dienstlichen Gebrauch nötig sind;
- ohne Zustimmung durch die EDV-Abteilung auf dem zugeteilten Notebook keine anderen als die durch die EDV-Abteilung zur Verfügung gestellten Programmen zu verwenden und keine Modifikationen an den vorhandenen System-Einstellungen vorzunehmen;
- Service und Reparaturen nur durch den Arbeitgeber bzw. von diesem benannte Fachwerkstätten durchführen zu lassen;
- alle datenschutzrechtlichen und das Amtsgeheimnis betreffenden Bestimmungen einzuhalten.

Die IT-Sicherheits-Verantwortlichen behalten sich das Recht vor, aktive Netzwerkverbindungen einer Benutzerin bzw. eines Benutzers sofort zu unterbrechen, wenn eine unzulässige Verwendung entdeckt wird.

_____
Name der/des Bediensteten

_____
Datum und Unterschrift der/des Bediensteten

C.10 Inhaltsverzeichnis Virenschutzkonzept (Muster)

Teil A: Sensibilisierung
1 Abhängigkeit der Institution vom IT-Einsatz

2 Beschreibung des Gefährdungspotentials
2.1 Viren
2.2 Makro-Viren
2.3 Trojanische Pferde
2.4 Hoax
3 Schadensszenarien
4 Potentiell betroffene IT-Systeme

Teil B: Erforderliche Schutzmaßnahmen
5 Virenschutz-Strategie
5.1 Nicht-vernetzte IT-Systeme
5.2 Vernetzte Endgeräte
5.3 Server
6 Aktualisierung der Viren-Suchprogramme
6.1 Nicht-vernetzte IT-Systeme
6.2 Vernetzte Endgeräte
6.3 Server

Teil C: Regelungen
7 Regelungen zum Schutz vor Viren
7.1 Nutzungsverbot nicht freigegebener Software
7.2 Schulung der IT-Benutzer/innen
7.3 Umstellung der Boot-Reihenfolge
7.4 Anlegen einer Notfall-Diskette
7.5 Verhaltensregeln bei Auftreten eines Virus
7.6 Maßnahmen bei nicht-resident virenkontrollierten IT-Systemen
7.6.1 Regelmäßiger Einsatz eines Viren-Suchprogramms
7.6.2 Virenkontrolle bei Datenträgeraustausch und Datenübertragung
7.6.3 Prüfung eingehender Dateien auf Makro-Viren
8 Regelung der Verantwortlichkeiten
8.1 Ansprechpartner/innen für Viren
8.2 Verantwortlichkeit der Systemadministration
8.3 Verantwortlichkeit der einzelnen IT-Benutzer/innen
8.4 Verantwortlichkeit des IT-Sicherheitsmanagements

Teil D: Hilfsmittel
10 Verhaltensregeln bei Auftreten eines Virus
11 Meldewege bei Auftreten eines Virus
12 Benutzerhandbuch des Viren-Suchprogramms

C.11 Inhaltsverzeichnis Kryptokonzept (Muster)

1. Definitionen

2. Gefährdungslage zur Motivation
- Abhängigkeit der Institution vom Datenbestand
- Typische Gefährdungen
- Institutionsrelevante Schadensursachen
- Schadensfälle im eigenen Haus

3. Festlegung einer organisationsinternen Sicherheitspolitik
- Festlegung von Verantwortlichkeiten
- Zielsetzung, Sicherheitsniveau

4. Einflussfaktoren
- Identifikation der zu schützenden Daten
- Vertraulichkeitsbedarf der Daten
- Integritätsbedarf der Daten
- Verfügbarkeitsanforderungen an die Daten
- Anforderungen an die Performance
- Schlüsselverteilung
- Datenvolumen
- Art der Daten (lokal / verteilt (LAN/WAN))
- Art der Anwendungen, bei denen kryptographische Verfahren zum Einsatz kommen sollen
- Häufigkeit des Einsatzes des kryptographischen Verfahrens
- Anforderungen an die kryptographische Stärke der Algorithmen bzw. Verfahren
- Wiederherstellbarkeit der gesicherten Daten
- Personalaufwand
- Erforderliche Funktionalität
- Kosten einschließlich Folgekosten (Wartung, Administration, Updates, ...)
- Kenntnisse und datenverarbeitungsspezifische Qualifikationen der IT-Benutzer/innen

5. Festlegung des Einsatzes
- Art der kryptographischen Verfahren
- Einsatzbedingungen an die kryptographischen Produkte
- Häufigkeit und Zeitpunkt des Einsatzes
- Benennung der Verantwortlichen
- Festlegung der organisatorischen Regelungen
- Durchführung der personellen Maßnahmen (Schulung, Vertretungsregelungen, Verpflichtungen, Rollenzuteilung)
- Dokumentation der Einsatzbedingungen / Konfiguration
- Interoperabilität, Standardkonformität, Investitionsschutz

6. Schlüsselmanagement

C.12 Inhaltsverzeichnis Datensicherungskonzept (Muster)

1. Definitionen
- Anwendungsdaten, Systemdaten, Software, Protokolldaten
- Vollsicherung, inkrementelle Datensicherung

2. Gefährdungslage zur Motivation
- Abhängigkeit der Organisation vom Datenbestand
- Typische Gefährdungen wie ungeschulte Benutzer/innen, gemeinsam genutzte Datenbestände, Viren, Hacker, Stromausfall, Festplattenfehler
- Organisationsrelevante Schadensursachen
- Schadensfälle im eigenen Haus

3. Einflussfaktoren je IT-System
- Spezifikation der zu sichernden Daten
- Verfügbarkeitsanforderungen der IT-Anwendungen an die Daten
- Rekonstruktionsaufwand der Daten ohne Datensicherung
- Datenvolumen
- Änderungsvolumen
- Änderungszeitpunkte der Daten
- Fristen
- Vertraulichkeitsbedarf der Daten
- Integritätsbedarf der Daten
- Kenntnisse und datenverarbeitungsspezifische Fähigkeiten der IT-Benutzer/innen

4. Datensicherungsplan je IT-System
4.1 Festlegungen je Datenart
- Art der Datensicherung
- Häufigkeit und Zeitpunkt der Datensicherung
- Anzahl der Generationen
- Datensicherungsmedium
- Verantwortlichkeit für die Datensicherung
- Aufbewahrungsort der Backup-Datenträger
- Anforderungen an das Datensicherungsarchiv
- Transportmodalitäten
- Rekonstruktionszeiten bei vorhandener Datensicherung

4.2 Festlegung der Vorgehensweise bei der Datenrestaurierung
4.3 Randbedingungen für das Datensicherungsarchiv
- Vertragsgestaltung (bei externen Archiven)
- Refresh-Zyklen der Datensicherung
- Bestandsverzeichnis
- Löschen von Datensicherungen
- Vernichtung von unbrauchbaren Datenträgern

4.4 Vorhalten von arbeitsfähigen Lesegeräten

5. Minimaldatensicherungskonzept
6. Verpflichtung der Mitarbeiter/innen zur Datensicherung
7. Sporadische Restaurierungsübungen

C.13 Inhaltsverzeichnis Disaster Recovery Handbuch (Muster)

Teil A: Sofortmaßnahmen

1 Alarmierung im Notfall
1.1 Alarmierungsplan und Meldewege
1.2 Adresslisten betroffener Mitarbeiter/innen
1.3 Festlegung konkreter Aufgaben für einzelne Personen/Funktionen im Notfall
1.4 Notrufnummern
(z.B. Feuerwehr, Polizei, Rettung, Notarzt, Wasser- und Stromversorger, Ausweichrechenzentrum, externes Datenträgerarchiv, externe Telekommunikationsanbieter)

2 Handlungsanweisung für spezielle Ereignisse, Treffpunkte
2.1 Brand
2.2 Wassereinbruch
2.3 Stromausfall
2.4 Ausfall der Klimaanlage
2.5 Explosion
2.6 Sabotage
2.7 Ausfall der Datenfernübertragungseinrichtung
2.8 Einbruch
2.9 Vandalismus
2.10 Bombendrohung
2.11 Streik / Demonstrationen
2.12 .....

Teil B: Regelungen für den Notfall

3 Allgemeine Regelungen
3.1 Notfall-Verantwortliche
3.2 Benennung der an der Durchführung der Notfallpläne beteiligten Organisationseinheiten, Kompetenzverteilung
3.3 Organisationsrichtlinien, Verhaltensregeln

4 Tabelle der Verfügbarkeitsanforderungen

Teil C: Wiederanlaufpläne für kritische Komponenten

5 Wiederanlaufplanung
5.1 Wiederanlaufplan für Komponente 1 (z.B. Host)
5.1.1 Wiederbeschaffungsmöglichkeiten
5.1.2 Interne / externe Ausweichmöglichkeiten
5.1.3 DFÜ-Versorgung
5.1.4 Eingeschränkter IT-Betrieb
5.1.5 Wiederanlaufreihenfolge
5.2 Wiederanlaufplan für Komponente 2 (z.B. Drucker)
...

Teil D: Dokumentation

6 Beschreibung der IT-Systeme
6.1 Beschreibung des IT-Systems A (im Überblick)
6.1.1 Beschreibung der Hardware-Komponenten
6.1.2 Beschreibung der Software-Komponenten
6.1.2.1 Bestandsverzeichnis der Systemsoftware
6.1.2.2 Bestandsverzeichnis der zu dem IT-System gehörenden Systemdaten
6.1.3 Beschreibung der Netzanbindungen des IT-Systems
6.1.4 Beschreibung der IT-Anwendungen
6.1.4.1 Bestandsverzeichnis der Anwendungssoftware
6.1.4.2 Bestandsverzeichnis der zu einer IT-Anwendung gehörenden Daten
6.1.4.3 Kapazitätsanforderungen einzelner IT-Anwendungen im Normalfall
6.1.4.4 Minimale Kapazitätsanforderungen der IT-Anwendungen für den Notfall
6.1.4.5 Wiederanlaufverfahren der IT-Anwendungen
6.1.5 Datensicherungsplan
6.1.6 Beschreibung der notwendigen Infrastruktureinrichtungen
6.1.7 Sonstige Unterlagen (Handbücher etc.)
6.2 Beschreibung des IT-Systems B
...

7 Wichtige Informationen
7.1 Ersatzbeschaffungsplan
7.2 Hersteller- und Lieferantenverzeichnis
7.3 Verzeichnis der Dienstleistungsunternehmen des Fachgebiets "Sanierung"

Letztes Änderungsdatum: _____

Anhang D: Wichtige Adressen

Die angegebenen Adressen entsprechen dem Stand zum Zeitpunkt des Redaktionsschlusses des vorliegenden Handbuches. Dabei ist zu beachten, dass insbesondere Internet-Adressen einer besonderen Dynamik unterliegen.

Österreich:

Bundeskanzleramt, Büro der Informationssicherheitskommission
Ballhausplatz 2
1014 Wien
Tel: 01 531 15 2594

Bundeskanzleramt, Geschäftsstelle der Datenschutzkommission
Ballhausplatz 1
1014 Wien
Tel: 01 531 15 2528
www.dsk.gv.at

Österreichisches Normungsinstitut (ON)
Heinestr. 38
A-1020 Wien
Tel.: 01 21300 0
www.on-norm.at

Rundfunk und Telekom Regulierungs-GmbH (RTR)
(früher: Telekom Control GmbH, TKC)
Mariahilfer Strasse 77-79
A-1060 Wien
www.rtr.at

Verband der Sicherheitsunternehmen Österreichs (VSÖ)
Fürstengasse 1
A-1090 Wien
Tel.: 01 3194132

Verband der Versicherungsunternehmen Österreichs (VVÖ)
Schwarzenbergplatz 7
A-1030 Wien
Tel.: 01 71156 0
www.vvo.at

Zentrum für sichere Informationstechnologie - Austria (A-SIT)
Weyringergasse 35
A-1040 Wien
Tel.: 01 5031963 0
www.a-sit.at

International:

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 183
D-53175 Bonn
www.bsi.de

International Organisation for Standardisation (ISO)
1, rue de Varembé
Case postale 56
CH-1211 Genève 20
www.iso.ch

VdS Schadenverhütung
Amsterdamer Straße 174
D-50735 Köln
Tel. 0049 221 7766 0

Anhang E: Referenzierte IKT-Board Beschlüsse und Gesetze

E.1 IKT-Board Beschlüsse

Nachfolgend sind die im Rahmen des Sicherheitshandbuches referenzierten IKT-Board Beschlüsse aufgelistet und zusammengefasst.

Die Kurzbeschreibung beschreibt nur den Kern des Themas, um die zu Grunde liegende IKT-Board-Entscheidung leichter identifizieren zu können. Sämtliche Referenzen können unter

http://www.cio.gv.at/ikt-board/beratungen/

nachgelesen werden. Alternativ sind nähere Informationen zu den Beschlüssen unter folgender Postadresse erhältlich:

Bundeskanzleramt
Bereich IKT-Strategie des Bundes
Ballhausplatz 2
A-1014 Wien
E-Mail: office@cio.gv.at

Referenz	Sitzungsdatum	Beschreibung
[IKTB-260701-1]	26.07.2001	Beschluss zu Single Sign-On
[IKTB-040901-1]	04.09.2001	Security Layer
[IKTB-140102-1]	14.01.2002	e-Card / Dienstkarte
[IKTB-040402-1]	04.04.2002	IT-Beschaffungshandbuch
[IKTB-040402-2]	04.04.2002	PKI – Zertifikate
[IKTB-040402-3]	04.04.2002	Portalverbund
[IKTB-250602-1]	25.06.2002	Open-Source/Linux (Ausschreibungsbedingung)
[IKTB-250602-2]	25.06.2002	e-Government Gütesiegel
[IKTB-170902-1]	17.09.2002	e-Mail-Policy
[IKTB-170902-3]	17.09.2002	Viren- und Incident-Warnsystem
[IKTB-170902-4]	17.09.2002	Ausweichsysteme
[IKTB-170902-7]	17.09.2002	Vertrauen in Betriebssysteme (Initialkonfiguration)
[IKTB-170902-8]	17.09.2002	Sicherheitspolicies der Ressorts
[IKTB-051102-1]	05.11.2002	Ciphersuits und Keystores im Portalverbund
[IKTB-181202-1]	18.12.2002	Zertifikate
[IKTB-181202-2]	18.12.2002	Bürgerkarte Light
[IKTB-181202-3]	18.12.2002	Österr. Sicherheits- und Verteidigungsdoktrin – Teilstrategie IKT-Sicherheit
[IKTB-110303-1]	11.03.2003	Kennzeichnung von Sicherheitszertifikaten (Servererkennung)

[IKTB-110303-2]	11.03.2003	Verwaltungskennzeichen
[IKTB-110903-3]	11.09.2003	Einsatz von PKI
[IKTB-110903-8]	11.09.2003	Externer Zugang zur E-Mail und internen Portalen
[IKTB-230903-17]	23.09.2003	Richtlinien für E-Mail Zertifikate in der Verwaltung
[IKTB-281003-19]	28.10.2003	Serverzertifikate – Allgemeine Richtlinien
[IKTB-161203-01]	16.12.2003	Vertrauliche und ausfallsichere Kommunikation
[IKTB-090204-01]	09.02.2004	Portalverbundprotokoll (PVP)
[IKTB-090204-02]	16.12.2004	E-Government Gütesiege
[IKTB-090204-03]	16.12.2004	Amtssiegel
[IKTB-240304-01]	24.03.2004	Portalverbund und portal.gv.at
[IKTB-240304-02]	24.03.2004	Amtssiegel / Amtssignatur
[IKTB-110504-01]	11.05.2004	Domänenpolicy
[IKTB-290604-01]	29-06-2004	ECC und Bankkarten
[IKTB-290604-02]	29-06-2004	Förderung der Signaturprüfung
[IKTB-230904-01]	23-09-2004	Elektronischer Bescheid
[IKTB-030505-01]	23-09-2004	Zertifikate im Rahmen der Bundesverwaltung

E.2 Gesetzestexte

Die zitierten Gesetzestexte können online über das Rechtsinformationssystem des Bundes unter folgender URL abgerufen werden:

http://www.ris.bka.gv.at

Die Bundesgesetzblätter sind bei der Wiener Zeitung Digitale Publikationen GmbH (vormals Österreichische Staatsdruckerei - Wiener Zeitung), die Landesgesetzblätter bei den Ämtern der Landesregierungen erhältlich.

[AschG]	"ArbeitnehmerInnenschutzgesetz" (AschG), BGBl-Nr. 450/1994
[B-BSG]	"Bundes-Bedienstetenschutzgesetz" (B-BSG), BGBl-Nr. 70/1999
[DSG 2000]	"Bundesgesetz über den Schutz personenbezogener Daten" (Datenschutzgesetz 2000 - DSG 2000), BGBl. I Nr. 165/1999
[EU 5775/01]	"Beschluss des Rates über die Annahme der Sicherheitsvorschriften des Rates", 7.3.2001
[EU 1999/93/EG]	Richtlinie 1999/93/EG des europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen
[SigG]	"Bundesgesetz über elektronische Signaturen" (Signaturgesetz - SigG), BGBl. I Nr. 190/1999
[StMV]	Standard- und Muster-Verordnung 2000 (StMV), BGBl II Nr. 201/2000
[TKG]	"Telekommunikationsgesetz", BGBl. I Nr. 100/1997
[InfoSiG]	Bundesgesetz über die Umsetzung völkerrechtlicher Verpflichtungen zur sicheren Verwendung von Informationen (Informationssicherheitsgesetz, InfoSiG), BGBl. I Nr. 23/2002
[SigV]	Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung - SigV), BGBl. II Nr. 30/2000
[V A-SIT]	Verordnung des Bundeskanzlers über die Feststellung der Eignung des Vereins "Zentrum für sichere Informationstechnologie - Austria (A-SIT)" als Bestätigungsstelle, BGBl. II Nr. 31/2000
[VBG]	Bundesgesetz über das Dienst- und Besoldungsrecht der Vertragsbediensteten des Bundes Vertragsbedienstetengesetz 1948 - VBG), BGBl. Nr. 86/1948
[BDG 1979]	Bundesgesetz über das Dienstrecht der Beamten (Beamten-Dienstrechtsgesetz 1979 - BDG 1979), BGBl. Nr. 333/1979
[RDG]	Bundesgesetz über das Dienstverhältnis der Richter und Richteramtsanwärter (Richterdienstgesetz - RDG), BGBl. Nr. 305/1961
[ArbVG]	Bundesgesetz betreffend die Arbeitsverfassung (Arbeitsverfassungsgesetz - ArbVG), BGBl. Nr. 22/1974
[AußHG]	Bundesgesetz über die Durchführung des Warenverkehrs der Ein- und Ausfuhr (Außenhandelsgesetz 1995 - AußHG 1995), BGBl. Nr. 172/1995

[PVG]	Bundesgesetz über die Personalvertretung bei den Dienststellen des Bundes (Bundes-Personalvertretungsgesetz - PVG), BGBl. Nr. 133/1967
[Urheberrechtsgesetz]	Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte (Urheberrechtsgesetz), BGBl. Nr. 111/1936
[HalonbankV]	Verordnung über die Einrichtung einer Halonbank (Halonbankverordnung - HalonbankV), BGBl. II Nr. 77/2000
[Halonverbot]	Verordnung über das Verbot von Halonen, BGBl. Nr. 576/1990
[StGB]	Bundesgesetz über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch - StGB), BGBl. Nr. 60/1974