IT-Sicherheitshandbuch

für die öffentliche

Verwaltung

Teil 1: IT-Sicherheitsmanagement

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

IT-Sicherheitshandbuch

für die öffentliche Verwaltung

Teil 1:

IT-Sicherheitsmanagement

Version 1.0

Oktober 1998

Vorwort

In den letzten Jahren gab es im Bereich der Informationstechnologie (IT) gerade in der öffentlichen Verwaltung einen bemerkenswerten Innovationsschub. Neue kostengünstige

Technologien und sinkende Hardwarekosten haben diesen Trend begünstigt. Gerade dieser Boom in der IT birgt aber die Gefahr, durch Konzentration auf den massiven Ausbau die notwendigen Begleitmaßnahmen wie zum Beispiel im Bereich von Datensicherheit und Datenschutz zu vernachlässigen.

Es haben sich daher auf Initiative und mit finanzieller Unterstützung des BM für Inneres Ressorts mit traditionellem Sicherheitsbedarf im Rahmen einer Arbeitsgruppe der ADV-Koordination im BKA zum Ziel gesetzt, ein IT-Sicherheitshandbuch für die öffentliche Verwaltung zu entwickeln. Dieses Handbuch sollte den Ressorts ermöglichen, eine eigenständige, jedoch mit anderen Organisationseinheiten kompatible IT-Sicherheitspoliti erstellen. Weiters sollte damit eine einheitliche Sprachregelung im Bereich der IT-Siche erreicht werden.

Der vorliegende erste Teil beinhaltet konkrete Anleitungen zur Etablierung eines umfasse und kontinuierlichen IT-Sicherheitsprozesses innerhalb einer Organisation. In einem zwei derzeit in Planung befindlichen Teil werden dann die organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsmaßnahmen für IT-Systeme mit einem mittlere Schutzbedarf beschrieben werden.

Beide Teile basieren z.T. auf dem Grundschutzhandbuch des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI), für dessen Zustimmung zur Nutzung gedankt werden darf.

Die nachstehend in alphabetischer Reihenfolge angeführten Teilnehmer der Arbeitsgruppe hoffen, mit dem vorliegenden ersten Teil des Sicherheitshandbuches auf die Notwendigkeit Errichtung eines IT-Sicherheitsmanagements hinreichend aufmerksam machen zu können, wünschen viel Erfolg bei einer allfälligen Implementierung und stehen für nähere Fragen u Anregungen gerne zur Verfügung:

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

---

Inhalt

---

1 IT-Sicherheitsmanagement in der öffentlichen Verwaltung

Die Sicherheit und Verlässlichkeit von Systemen der Informationstechnik (IT-Systemen) ist von entscheidender Bedeutung für eine Vielzahl von Organisationen und letztlich für die Funktionsfähigkeit unserer Gesellschaft. Die Erkenntnis, dass weite Bereiche des tägliche Lebens ohne den Einsatz von informationstechnischen Systemen heute nicht mehr funktionsfähig sind, rückt die Frage nach der Sicherheit der Informationstechnologie zunehmend in den Brennpunkt des Interesses. Gerade im Bereich der öffentlichen Verwaltung bestehen besonders hohe Anforderungen an die Vertrauenswürdigkeit und Sicherheit von IT-Systemen.

In den vergangenen Jahren wurde auch zunehmend deutlich, dass sich Sicherheit nicht auf einzelne Teilaspekte, wie die Verschlüsselung vertraulicher Daten oder die Installation v Firewall-Rechnern beschränken kann, sondern integraler Bestandteil eines modernen IT-Konzeptes sein muss. Methodisches Sicherheitsmanagement ist zur Gewährleistung umfassender und angemessener IT-Sicherheit unerlässlich.

1.1 Ziele und Aufgaben des IT- Sicherheitsmanagements

IT-Sicherheitsmanagement ist ein kontinuierlicher Prozess, der die Vertraulichkeit, Integ Verfügbarkeit, Zurechenbarkeit, Authentizität und Zuverlässigkeit von Systemen der Informationstechnik (IT-Systemen) innerhalb einer Organisation gewährleisten soll.

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.

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

1.2 Zielsetzungen des Handbuches

Das vorliegende IT-Sicherheitshandbuch wurde für die Anwendung in der öffentli
tung erstellt und ist auf die spezifischen Anforderungen in diesem Bereich ab
Aufgrund des generellen Ansatzes kann es aber auch durchaus für Anwender außer
Bereiches von Nutzen sein.

Die Anwendung dieses Handbuches soll es den einzelnen Ressorts ermöglichen, di
Bereich relevanten IT-Sicherheitsziele und -strategien zu ermitteln, eine eige
mit den anderen Ressorts kompatible IT-Sicherheitspolitik zu erstellen, geeign
angemessene Sicherheitsmaßnahmen auszuwählen und zu realisieren sowie IT-Siche
laufenden Betrieb zu gewährleisten. Darüber hinaus soll das Handbuch dazu beit
innerhalb der österreichischen Behörden eine einheitliche Vorgehensweise und S
im Bereich der IT-Sicherheit zu entwickeln, wobei aber größtmögliche Flexibili
Umsetzung der unterschiedlichen Sicherheitsanforderungen der einzelnen Ressort
Organisationseinheiten (OEs) gewahrt bleiben soll.

Ziel ist es, IT-Sicherheit zu einem integralen Bestandteil der Entwicklung und
von IT-Systemen in der öffentlichen Verwaltung zu machen.

Einige generelle Anmerkungen:

* Das vorliegende Handbuch konzentriert sich auf den Bereich "Sicherheit von S
  Informationstechnik" (kurz "IT-Sicherheit"). Dies umfasst Hardware, Software
  auch organisatorische, bauliche und personelle Fragen, soweit sie in direkte
  Zusammenhang mit der Sicherheit von IT-Systemen stehen.
  Abzugrenzen davon ist das Gebiet der "Informationssicherheit", das sich mit
  von Information generell, also etwa auch in schriftlicher Form, auf Mikrofil
  gesprochener Form, befasst. Dies ist nicht Gegenstand dieses Handbuches.

* Das IT-Sicherheitshandbuch versteht sich als Sammlung von Leitlinien und Emp
  die entsprechend den spezifischen Anforderungen und Bedürfnissen der anwende
  Organisationseinheit angepasst werden sollten. Es stellt eine Ergänzung zu d
  Regelungen und Vorschriften (Datenschutzgesetz, Verschlusssachenvorschriften
  geheimnis,...) dar und soll diese nicht außer Kraft setzen oder zu ihnen im
  stehen.

* Das IT-Sicherheitshandbuch besteht aus zwei Teilen.
  Teil 1 "IT-Sicherheitsmanagement" liegt nun vor. Er beinhaltet konkrete Anle
  Etablierung eines umfassenden und kontinuierlichen IT-Sicherheitsprozesses i
  Organisation.

Teil 2 "Baseline Security" ist derzeit in Planung. Er beinhaltet die Beschreibung orga
torischer, personeller, infrastruktureller und technischer Standardsicherheitsmaßnahmer
Ziel ist die Gewährleistung eines angemessenen und ausreichenden Sicherheitsniveaus fü
IT-Systeme mit mittlerem Schutzbedarf.

* Seit einigen Jahren werden auf nationaler und internationaler Ebene verstärkt Anstrengu
gen unternommen, einheitliche methodische Vorgehensweisen zur Etablierung von IT-
Sicherheit zu erarbeiten. Die österreichische öffentliche Verwaltung unterstützt diese
Bestrebungen und versucht, im vorliegenden Handbuch diesen internationalen
Entwicklungen so weit wie möglich Rechnung zu tragen. Das Handbuch geht aus von den
Konzepten, die im Technical Report "Guidelines for the Management of IT Security
(GMITS)" der ISO/IEC vorgestellt werden, den im "IT-Grundschutzhandbuch" und "IT-
Sicherheitshandbuch" des Bundesamtes für Informationstechnik (BSI) in Bonn gewählten
Ansätzen, sowie einigen weiteren, im Literaturverzeichnis angeführten Arbeiten, wurde
jedoch an die spezifischen Anforderungen für den definierten Anwendungsbereich adaptie
Der besseren Lesbarkeit halber wird im Text des Handbuches i.a. auf direkte Verweise
sowie die Beschreibung von Unterschieden verzichtet, der interessierte Leser sei hier
Originalliteratur verwiesen.

* Auch die Konzepte und Methoden des IT-Sicherheitsmanagements sind einer ständigen
Änderung und Weiterentwicklung unterworfen. Es ist daher notwendig, das vorliegende
Handbuch kontinuierlich weiterzuentwickeln und neuen Erfordernissen anzupassen. Von
besonderer Bedeutung ist dabei ein Feedback über die Erfahrungen mit der Anwendung des
Handbuches in der Praxis. Alle Anwender des Handbuches werden daher eingeladen,
diesbezügliche Anregungen und Erfahrungen den Verfassern mitzuteilen.

1.3 IT-Sicherheitsmanagement als kontinuierlicher Prozess

Risiken sind in unserer Welt allgegenwärtig. Man kann ihnen nicht völlig aus dem Weg gehe
man muss vielmehr lernen, sie zu erkennen und bestmöglich zu beherrschen. Diese
methodische Bewältigung von Risiken ist Gegenstand des Risikomanagements.

IT-Sicherheitsmanagement stellt jenen Teil des allgemeinen Risikomanagements dar, der di
Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit, Authentizität und Zuverlässi
von Systemen der Informationstechnik gewährleisten soll. Dabei handelt es sich um einen
kontinuierlichen Prozess, dessen Strategien und Konzepte ständig auf ihre Leistungsfähigk
und Wirksamkeit zu überprüfen und bei Bedarf fortzuschreiben sind.

Die nachfolgende Graphik zeigt - in Anlehnung an das Konzept in [ISO/IEC 13335], aber fü
die aktuellen Anforderungen im Bereich der öffentlichen Verwaltung adaptiert - die
wichtigsten Aktivitäten im Rahmen des IT-Sicherheitsmanagements und die eventuell
erforderlichen Rückkopplungen zwischen den einzelnen Stufen.

Anmerkung:
Der dargestellte Prozess kann sowohl auf eine gesamte Organisation als auch a

Der dargestellte Prozess kann sowohl auf eine gesamte Organisation als auch a
Anwendung finden. Generell sollte der Prozess zumindest auf Ressortebene durch
werden, über die Anwendung auf Ebene einzelner Behörden, Abteilungen oder ande
dann im spezifischen Zusammenhang - abhängig vom IT-Konzept und den bestehende
Sicherheitsanforderungen - zu entscheiden.

Im Folgenden wird, wenn nicht ausdrücklich anders angeführt, allgemein der Beg
"Organisation" (oder synonym dazu "Institution") verwendet, wobei aber zu bea
damit beliebige Organisationseinheiten gemeint sein können.

Abbildung 1.1: Aktivitäten im Rahmen des IT-Sicherheitsmanagements

---

IT-Sicherheitsmanagement umfasst damit folgende Schritte:

* ***Entwicklung einer organisationsweiten IT-Sicherheitspolitik***

Als organisationsweite IT-Sicherheitspolitik (*Corporate IT Security Policy*) bezeichnet man die Leitlinien und Vorgaben innerhalb einer Organisation, die unter Berücksich gegebener Randbedingungen grundlegende Ziele, Strategien, Verantwortlichkeite Methoden für die Gewährleistung der IT-Sicherheit festlegen.
Die organisationsweite IT-Sicherheitspolitik (im Folgenden der Einfachheit ha Sicherheitspolitik" bezeichnet) soll allgemeine Festlegungen treffen, die für der Informationstechnologie innerhalb einer Organisation Gültigkeit haben (s. es sich um ein langfristig orientiertes Grundlagendokument handelt, können te

sowie Einzelheiten zu Sicherheitsmaßnahmen und deren Umsetzung nicht Bestandte
organisationsweiten IT-Sicherheitspolitik sein. Sie sind im Rahmen der einzeln
sicherheitspolitiken" zu behandeln.
Die IT-Sicherheitspolitik ist eingebettet in eine Hierarchie von Regelungen un
Abhängig vom IT-Konzept und den Sicherheitsanforderungen kann es auch notwend
eine Hierarchie von IT-Sicherheitspolitiken für verschiedene Organisationseinh
Abteilungen, nachgeordnete Dienststellen,...) zu erstellen.

* ***Risikoanalyse***

Eine wesentliche Aufgabe des IT-Sicherheitsmanagements ist das Erkennen und E
von Sicherheitsrisiken und deren Reduktion auf ein tragbares Maß. Im Rahmen de
vorliegenden Handbuches werden drei Risikoanalysestrategien behandelt (s. Kap.
Detaillierte Risikoanalyse, Grundschutzansatz und Kombinierter Ansatz. Die Wal
Risikoanalysestrategie sollte im Rahmen der IT-Sicherheitspolitik erfolgen, un
organisationsweit einheitliches Vorgehen zu gewährleisten.

* ***Erstellung eines IT-Sicherheitskonzeptes***

Abhängig von den Ergebnissen der Risikoanalyse werden in einem nächsten Schrit
Maßnahmen ausgewählt, die die Risiken auf ein definiertes und beherrschbares M
sollen. Im Anschluss daran ist das verbleibende Restrisiko zu ermitteln und zu
für die Organisation tragbar ist oder weitere Maßnahmen zur Risikoreduktion er
Für große und komplexe IT-Systeme sollten eigene IT-Systemsicherheitspolitiken
werden, die - kompatibel mit der organisationsweiten IT-Sicherheitspolitik - s
grundlegenden Leitlinien zur Sicherheit eines konkreten IT-Systems vorgeben al
konkrete Sicherheitsmaßnahmen und ihre Umsetzung beschreiben.
In einem IT-Sicherheitsplan werden alle kurz-, mittel- und langfristigen Aktio
die zur Umsetzung der ausgewählten Maßnahmen erforderlich sind.

Die Erstellung von IT-Sicherheitskonzepten wird in Kapitel 4 dieses Handbuches

* ***Umsetzung des IT-Sicherheitsplans***

Bei der Implementierung der ausgewählten Sicherheitsmaßnahmen ist zu beachten,
meisten technischen Sicherheitsmaßnahmen ein geeignetes organisatorisches Umfe
um vollständig wirksam zu sein. Unabdingbare Voraussetzung für eine erfolgreic
des IT-Sicherheitsplanes in der Praxis sind auch entsprechende Sensibilisierun
Schulungsmaßnahmen. Weiters ist sicherzustellen, dass die IT-Systeme den Anfor
IT-Systemsicherheitspolitiken und des IT-Sicherheitsplanes in der konkreten Ei
genügen ("Akkreditierung").

Kapitel 5 des vorliegenden Handbuches behandelt diese Umsetzungsfragen.

* ***IT-Sicherheit im laufenden Betrieb***

Umfassendes IT-Sicherheitsmanagement beinhaltet nicht zuletzt auch die Aufgabe
heit im laufenden Betrieb aufrechtzuerhalten und gegebenenfalls veränderten Be
anzupassen. Zu den erforderlichen Follow-Up-Aktivitäten zählen (s. Kapitel 6)
ü Aufrechterhaltung des erreichten Sicherheitsniveaus

ü Aufrechterhaltung des erreichten Sicherheitsniveaus
dies umfasst:
- Wartung und administrativen Support von Sicherheitseinrichtungen,
- die Überprüfung von Maßnahmen auf Übereinstimmung mit der IT-Sicherheits
(*Security Compliance Checking*)
- die fortlaufende Überwachung der IT-Systeme (*Monitoring*)
ü Reaktion auf sicherheitsrelevante Ereignisse (*Incident Handling*)
ü Change Management

---

2 Entwicklung einer organisationsweiten IT-Sicherheitspolitik

Die IT-Sicherheitspolitik bildet die Basis für die Entwicklung und die Umsetzung eines risikogerechten und wirtschaftlich angemessenen IT-Sicherheitskonzeptes. Sie stellt ein Grundlagendokument dar, das die sicherheitsbezogenen Ziele, Strategien, Verantwortlichke und Methoden langfristig und verbindlich festlegt.

Die organisationsweite IT-Sicherheitspolitik soll allgemeine Festlegungen treffen, die fü Einsatzbereiche der Informationstechnologie innerhalb einer Organisation zur Anwendung kommen. Diese Richtlinien werden in den nachgeordneten "IT-Systemsicherheitspolitiken", etwa der PC-Sicherheitspolitik oder der Netzsicherheitspolitik, konkret umgesetzt.

2.1 Erstellung von IT-Sicherheitspolitiken

Geltungsbereich

Jedes Ressort sollte eine eigene, ressortspezifische IT-Sicherheitspolitik erstellen. Be können aus dieser weitere Sicherheitspolitiken, etwa auf Behörden- oder Abteilungsebene, abgeleitet werden.

Das folgende Kapitel gibt eine Anleitung zur Erstellung einer derartigen Politik und leg wesentlichen Inhalte fest. Ziel dieses Abschnittes des IT-Sicherheitshandbuches ist es, d Erarbeitung eigenständiger, jedoch mit denen anderer Institutionen der öffentlichen Ver- waltung kompatibler IT-Sicherheitspolitiken zu unterstützen. Dies soll ein äquivalentes N der IT-Sicherheit in den einzelnen Organisationen gewährleisten sowie Synergieeffekte nut machen.

Aufgaben und Ziele einer IT-Sicherheitspolitik

Eine organisationsweite IT-Sicherheitspolitik hat die Aufgabe, alle Aspekte einer sichere
Nutzung der Informationstechnik innerhalb einer Organisation abzudecken. Dabei gilt:

ü Die IT-Sicherheitspolitik wird als schriftliches Dokument erstellt und bildet die Grun
des IT-Sicherheitsmanagements.
ü Die IT-Sicherheitspolitik legt Leitlinien fest, schreibt aber keine Implementierung vo
ü Die IT-Sicherheitspolitik wird offiziell verabschiedet und in Kraft gesetzt.
ü Jeder Mitarbeiter muss Kenntnis über die wichtigsten Inhalte der IT-Sicherheitspolitik
haben; die direkt mit IT-Sicherheit beschäftigten Mitarbeiter (dazu gehören die Mitgli
des IT-Sicherheitsmanagement-Teams, der Datenschutz-/IT-Sicherheitsbeauftragte, die

---

Bereichs-IT-Sicherheitsbeauftragten sowie die Applikations-/Projektverantwor
auch Kap. 2.2.2) müssen im Besitz einer aktuellen Version der IT-Sicherheit

2.2 Die Inhalte der IT-Sicherheitspolitik

Der folgende Abschnitt beschreibt, welche Themenbereiche die IT-Sicherheitspo
sprechen sollte, und gibt Hinweise und Leitlinien zur Erstellung dieses Dokum

2.2.1 Grundsätzliche Ziele und Strategien

Schritt 1: Festlegung der wesentlichen IT-Sicherheitsziele

Bei der Erstellung der IT-Sicherheitspolitik sind zunächst die spezifischen I
der Organisation zu erarbeiten, die mit dieser Politik erreicht werden sollen

Beispiele für solche Ziele sind:
ü Gewährleistung der aus gesetzlichen Vorgaben resultierenden Anforderungen
ü Gewährleistung des Vertrauens der Öffentlichkeit in die betroffene Organisa
öffentliche Verwaltung im Allgemeinen
ü Hohe Verlässlichkeit des Handelns, insbesondere in Bezug auf Vertraulichkei
und Rechtzeitigkeit. Dies erfordert:
Vertraulichkeit der verarbeiteten Informationen und Einhaltung des Datens
Korrektheit, Vollständigkeit und Authentizität der Informationen (Integrit
Rechtzeitigkeit (Verfügbarkeit der IT)
ü Sicherung der investierten Werte
ü Sicherstellung der Kontinuität der Arbeitsabläufe
ü Reduzierung der im Schadensfall entstehenden Kosten (Schadensvermeidung und
Schadensbegrenzung)
ü Gewährleistung des besonderen Prestiges

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

Zur Präzisierung dieser Ziele können folgende Fragen hilfreich sein:
ü Welche essentiellen Aufgaben der betreffenden Organisation können ohne IT-Ur
nicht mehr durchgeführt werden?
ü Welche wesentlichen Entscheidungen hängen von der Genauigkeit, Integrität o

ü Welche wesentlichen Entscheidungen hängen von der Genauigkeit, Integrität od
barkeit von durch die IT-Systeme verarbeiteter Information ab?
ü Welche vertrauliche Information ist zu schützen?

ü Welche Auswirkungen hätte eine gravierende Verletzung der Sicherheit (Verlus
Vertraulichkeit, Integrität und/oder Verfügbarkeit)?

Schritt 2: Festlegung des angestrebten Sicherheitsniveaus

In diesem Schritt ist festzulegen, welches Sicherheitsniveau in Bezug auf
ü Vertraulichkeit,
ü Integrität und
ü Verfügbarkeit
angestrebt werden soll.

Schritt 3: Ausarbeitung von Strategien für das IT-Sicherheitsmanagement

Die IT-Sicherheitsstrategie legt fest, wie die definierten Sicherheitsziele e
können.

Eine organisationsweite IT-Sicherheitspolitik kann und soll lediglich eine Hi
Beschreibung der gewählten Strategie beinhalten - Detailbeschreibungen sind A
nachgeordneten IT-Systemsicherheitspolitiken.
Beispiele für Bereiche, die in der IT-Sicherheitsstrategie angesprochen werde

ü die Forderung nach einer organisationsweiten Methodik zur IT-Sicherheit,
ü eine klare Zuordnung aller Verantwortlichkeiten im IT-Sicherheitsprozess,
ü die Einführung eines QM-Systems,
ü die Entwicklung einer IT-Systemsicherheitspolitik für jedes IT-System,
ü die Etablierung eines organisationsweiten Incident Handling Plans,
ü die Voraussetzungen für eine sichere externe Kommunikation,
ü Orientierung an internationalen Richtlinien und Standards,
ü IT-Sicherheit als integraler Bestandteil des gesamten Lebenszyklus eines IT-
ü die Förderung des Sicherheitsbewusstseins aller Mitarbeiter.

2.2.2 Organisation und Verantwortlichkeiten für IT-Sicherheit

Um eine Berücksichtigung aller wichtigen Aspekte und eine effiziente Erledigu
anfallender Aufgaben zu gewährleisten, ist es erforderlich, die Rollen und Ve
aller in den IT-Sicherheitsprozess involvierten Personen klar zu definieren.
Die Organisation des IT-Sicherheitsmanagements ist für jede Institution - ents
Größe, Struktur und Aufgaben - spezifisch festzulegen und in der IT-Sicherheit
schreiben. Als Leitlinie soll dabei das nachfolgende Bild dienen, das beispie
Organisation des IT-Sicherheitsmanagements auf Ebene eines Ressorts aussehen k

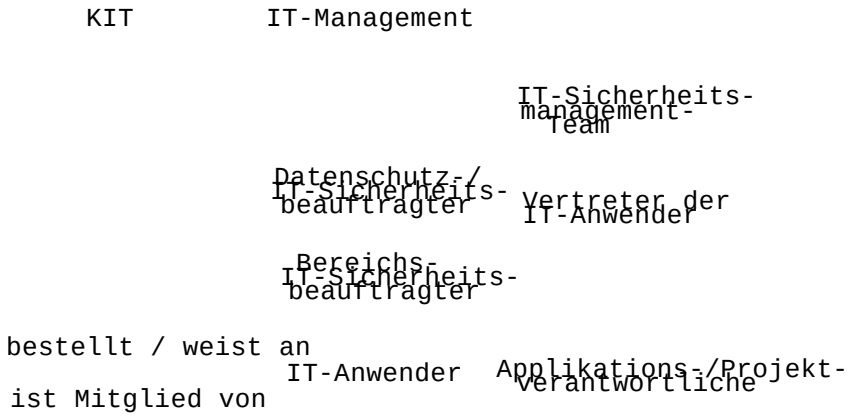


Abbildung 2.1: Beispiel zur Organisation des IT-Sicherheitsmanagements in einem Re

Das nächste Bild zeigt, wie das IT-Sicherheitsmanagement in einer kleinen bis mittelgroße
Institution organisiert sein könnte:

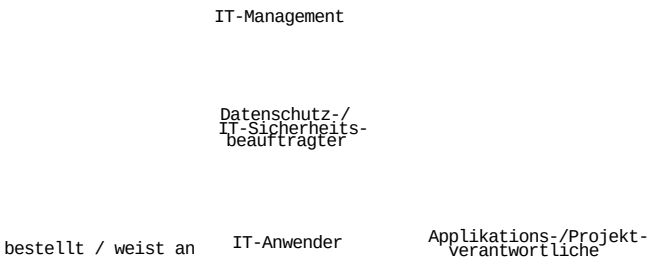


Abbildung 2.2: Beispiel zur Organisations des IT-Sicherheitsmanagements in einer Institution kleiner bis mittlerer Größe

Zentrale Aufgaben im IT-Sicherheitsmanagementprozess kommen dabei
ü dem IT-Sicherheitsmanagement-Team,

ü dem Datenschutz-/IT-Sicherheitsbeauftragten,
ü dem Bereichs-IT-Sicherheitsbeauftragten und
ü den Applikations-/Projektverantwortlichen
zu.

Es ist zu betonen, dass es sich bei diesen Funktionen bzw. Gremien, die im Fo
beschrieben werden, um Rollen handelt, die - abhängig von der Größe und den S
anforderungen einer Organisation - durchaus auch von mehreren Personen wahrge
werden können. In diesem Fall ist auf eine genaue Trennung der Kompetenzen un
wortlichkeiten Bedacht zu nehmen. Genauso ist es möglich, dass eine Person ei
zusätzlich zu anderen Aufgaben übernimmt (beispielsweise könnte ein Systemadm
Bereichs-IT-Sicherheitsbeauftragter für dieses System agieren), wobei darauf
dass ausreichend Zeit für die sicherheitsrelevanten Tätigkeiten zur Verfügung
keinen Kollisionen von Verantwortlichkeiten oder Interessen kommt.

Nachfolgend werden die wichtigsten typischen Aufgaben und Verantwortlichkeite
Funktionen bzw. Gremien kurz beschrieben. Eine detaillierte, auf die speziell
Anforderungen der betreffenden Organisation abgestimmte Beschreibung ist im R
organisationsweiten IT-Sicherheitspolitik zu geben.

Das IT-Sicherheitsmanagement-Team

Aufgaben:
Das IT-Sicherheitsmanagement-Team ist verantwortlich für die Regelung der orga
weiten IT-Sicherheitsbelange sowie für die Erarbeitung von Plänen, Vorgaben u
zur IT-Sicherheit. Zu seinen Aufgaben zählen unter anderem:
ü Festlegung der IT-Sicherheitsziele der Organisation
ü Entwicklung einer organisationsweiten IT-Sicherheitspolitik
ü Unterstützung und Beratung bei der Erstellung des IT-Sicherheitskonzeptes s
  Überprüfung des Konzeptes auf Erreichung der IT-Sicherheitsziele
ü Förderung des IT-Sicherheitsbewusstseins in der gesamten Organisation
ü Festlegung der personellen und finanziellen Ressourcen für IT-Sicherheit

Zusammensetzung des Teams:
Die genaue Festlegung der Zusammensetzung sowie der Aufgaben und Verantwortli
des IT-Sicherheitsmanagement-Teams hat im Rahmen der IT-Sicherheitspolitik zu
Generell ist zu empfehlen, dass der Datenschutz-/IT-Sicherheitsbeauftragte so
der IT-Anwender Mitglieder des IT-Sicherheitsmanagements-Teams sind.

Der Datenschutz-/IT-Sicherheitsbeauftragte

Zentrale Aufgaben des Datenschutz-/IT-Sicherheitsbeauftragten sind die Wahrne
datenschutzrechtlichen Belange lt. Datenschutzgesetz in der jeweils gültigen
fachliche Verantwortung für alle IT-Sicherheitsfragen innerhalb einer Organis

Zu seinen Pflichten gehören:
ü die verantwortliche Mitwirkung an der Erstellung des IT-Sicherheitskonzepte
ü die Gesamtverantwortung für die Realisierung der ausgewählten Sicherheitsma
ü die Planung und Koordination von Schulungs- und Sensibilisierungsveranstalt

ü die Planung und Koordination von Schulungs- und Sensibilisierungsveranstalt
ü die Gewährleistung der IT-Sicherheit im laufenden Betrieb,
ü die Verwaltung der für IT-Sicherheit zur Verfügung stehenden Ressourcen sow
ü die Wahrnehmung der datenschutzrechtlichen Belange lt. Datenschutzgesetz in gültigen Fassung.

Der Datenschutz-/IT-Sicherheitsbeauftragte kann einzelne Aufgaben delegieren, verantwortung für die IT-Sicherheit verbleibt aber bei ihm.
Abhängig von Größe und Aufgaben einer Institution kann eine Trennung der date lichen und der übrigen IT-sicherheitsspezifischen Aufgaben sinnvoll sein. Auf Komplexität und Vielfalt der Aufgaben besteht auch, wie bereits oben erwähnt, Möglichkeit diese Funktion durch mehrere Personen abzudecken.

Der Funktion des Datenschutz-/IT-Sicherheitsbeauftragten kommt eine zentrale Daher sollte diese Rolle in jedem Fall - also auch bei kleinen Organisationse und klar einer Person (eventuell zusätzlich zu anderen Aufgaben) zugeordnet s

Die Bereichs-IT-Sicherheitsbeauftragten

Die Komplexität moderner IT-Systeme erfordert zur Gewährleistung eines angemes Sicherheitsniveaus tief gehende Systemkenntnisse, die von einer einzelnen Per mehr abgedeckt werden können, insbesondere wenn mehrere unterschiedliche Syst formen zum Einsatz kommen. Daher wird es in den meisten Fällen empfehlenswert Bereichs-IT-Sicherheitsbeauftragte zu definieren. Diese haben die fachliche V alle IT-Sicherheitsbelange in einem bestimmten Bereich. Ein Bereich kann beis IT-System oder eine Betriebssystemplattform sein, auch eine Zuordnung nach Ab denkbar.

Zu den Aufgaben eines Bereichs-IT-Sicherheitsverantwortlichen zählen
ü die Mitwirkung bei den seinen Bereich betreffenden Teilen des IT-Sicherheits
ü die Erarbeitung eines detaillierten Planes zur Realisierung der ausgewählte Sicherheitsmaßnahmen,
ü die Umsetzung dieses Planes,

ü die regelmäßige Prüfung der Wirksamkeit und Einhaltung der eingesetzten IT-S maßnahmen im laufenden Betrieb,
ü Information des Datenschutz-/IT-Sicherheitsbeauftragten über bereichsspezif Schulungsbedarf sowie
ü Meldungen an den Datenschutz-/IT-Sicherheitsbeauftragten bei sicherheitsrel Ereignissen.

Applikations-/Projektverantwortliche

Für jede IT-Anwendung und jedes IT-Projekt ist die fachliche Gesamtverantwort auch die Verantwortung für deren/dessen Sicherheit klar festzulegen.

Zu den Aufgaben des Applikations-/Projektverantwortlichen zählen insbesondere
ü die Festlegung der Sicherheits- und Qualitätsanforderungen,
ü die Klassifikation der verarbeiteten Daten,
ü die Vergabe von Zugriffsrechten sowie
ü organisatorische und administrative Maßnahmen zur Gewährleistung der IT-Sic der Projektentwicklung und im laufenden Betrieb.

Darüber hinaus muss jeder Mitarbeiter, auch wenn er nicht direkt in den Berei involviert ist, seine spezifischen Pflichten und Verantwortlichkeiten im Rahm Sicherheit kennen und erfüllen. Ebenso sind die Rechte und Pflichten von exte arbeitern, Lieferanten und Vertragspartnern festzulegen.

Im Rahmen der organisationsweiten IT-Sicherheitspolitik sind daher auch die A Verantwortlichkeiten folgender Personenkreise im Detail zu definieren.

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

2.2.3 Risikoanalysestrategien, akzeptables Restrisiko und Risikoakzeptanz

Methodisches Risikomanagement ist zur Erarbeitung eines vollständigen und orga weiten IT-Sicherheitskonzeptes unerlässlich. Um Risiken zu beherrschen, ist es erforderlich, sie zu kennen und zu bewerten. Dazu wird in einer Risikoanalyse Gesamtrisiko ermittelt. Ziel ist es, dieses Risiko so weit zu reduzieren, das Restrisiko quantifizierbar und akzeptierbar wird.

In der IT-Sicherheitspolitik sollen die Risikoanalysestrategie der Organisati akzeptable Restrisiko festgelegt werden. Weiters ist die Vorgehensweise bei d von außergewöhnlichen Restrisiken zu definieren.

Im folgenden Abschnitt werden die wichtigsten Punkte, die im Rahmen der IT-Sic politik zum Thema Risikoanalyse festgelegt werden sollten, aufgeführt. Details analyse sind in Kapitel 3 enthalten.

Schritt 1: Festlegung der anzuwendenden Risikoanalysestrategie

Die heute gängige Praxis kennt verschiedene Varianten zur Risikoanalysestrate Organisation, von denen die wichtigsten drei im Folgenden kurz beschrieben we

* Grundschutzansatz:
  Unabhängig vom tatsächlichen Schutzbedarf werden für alle IT-Systeme Grundsc maßnahmen eingesetzt. Diese Vorgehensweise spart Ressourcen und führt schnel relativ hohen Niveau an Sicherheit. Der Nachteil liegt darin, dass der Grund das betrachtete IT-System möglicherweise nicht angemessen sein könnte.

* Detaillierte Risikoanalyse:
  Für alle IT-Systeme wird eine detaillierte Risikoanalyse durchgeführt. Diese gewährleistet die Auswahl von effektiven und angemessenen Sicherheitsmaßnahm benötigt jedoch viel Zeit und Aufwand. Dies führt zu relativ hohen Kosten, d besteht auch die Gefahr, dass die Schutzmaßnahmen für kritische Systeme zu s werden.

* Kombinierter Ansatz:

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
kategorie "niedrig bis mittel" wird von einer pauschalisierten Gefährdungsla
so dass auf eine detaillierte Risikoanalyse verzichtet und eine Grundschutza
durchgeführt werden kann. Dies erlaubt eine schnelle und effektive Auswahl v
legenden Sicherheitsmaßnahmen bei gleichzeitiger Gewährleistung eines angeme
Schutzniveaus. IT-Systeme der Schutzbedarfskategorie "hoch oder sehr hoch" s
detaillierten Risikoanalyse zu unterziehen, auf deren Basis individuelle
Sicherheitsmaßnahmen ausgewählt werden.
Diese Option kombiniert die Vorteile des Grundschutz- und des Risikoanalysea
alle IT-Systeme mit hohem Schutzbedarf wirksam und angemessen geschützt werd
Maßnahmen für die anderen Systeme mit Hilfe des Grundschutzes schnell und ef
ausgewählt werden können.

Schritt 2: Festlegung des akzeptablen Restrisikos

Auch bei Durchführung aller ausgewählten Sicherheitsmaßnahmen verbleibt im Al
ein Restrisiko, dessen Abdeckung wirtschaftlich nicht mehr vertretbar wäre. In
Sicherheitspolitik sind diese akzeptablen Restrisiken so exakt wie möglich zu

Schritt 3: Festlegung der Vorgehensweise zur Akzeptanz von außergewöhnlichen R

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

In der Sicherheitspolitik sind
ü das Vorgehen bei Risiken, die in Abweichung von der generellen Sicherheitspo
  genommen werden sollen, sowie
ü die Verantwortlichkeiten dafür
festzulegen.

2.2.4 Klassifikation von Daten

Die Klassifizierung der von den IT-Systemen verarbeiteten Daten in Bezug auf i
Vertraulichkeit und Integrität ist wesentliche Voraussetzung für die spätere A
Sicherheitsmaßnahmen. Daher sind in der IT-Sicherheitspolitik entsprechende Kl
definieren und weiters die Verantwortlichkeiten für die Durchführung der Klass
festzulegen.

Schritt 1: Definition der Sicherheitsklassen

Es ist jeder Organisation überlassen, in ihrer IT-Sicherheitspolitik eine für
adäquate Definition von Sicherheitsklassen vorzunehmen.

Empfehlung für ein Klassifizierungsschema:
Im Folgenden wird ein Beispiel für ein Klassifizierungsschema gegeben, das für
Szenario im Bereich der öffentlichen Verwaltung geeignet ist. Die Anwendung di

in all denjenigen Bereichen, in denen nicht zwingende Gründe für ein anderes K
schema bestehen, wird aus Gründen der Kompatibilität empfohlen.

Die Sicherheitsklassen können als Maß dafür gesehen werden, welche Auswirkunge
Missbrauch dieser Information - dazu zählen sowohl der Verlust der Vertraulich
die unbefugte Veränderung oder Zerstörung der Information - auf die Institutio

---

Es sind 4 hierarchische Klassen definiert:

* offen:
  Information, die ausdrücklich zur Veröffentlichung freigegeben wurde.
  Dazu zählen etwa Gesetze, Verordnungen und Pressemitteilungen.

* vertraulich:
  Information, die für den internen dienstlichen Gebrauch bestimmt und grundsä
  Veröffentlichung nicht vorgesehen ist (z.B. behördeninterner Schriftverkehr,
  Telefonverzeichnisse, Organisationspläne).

* geheim:
  Information, deren Missbrauch der Organisation, der öffentlichen Verwaltung
  Öffentlichkeit unter Umständen erheblichen Schaden zufügen könnte. Dazu zähl
  anderem alle Daten, die unter eine Verschlusssachenverordnung fallen.

Darüber hinaus wird eine eigene Klasse definiert für lt. Datenschutzgesetz bes
würdige Daten:

* sensibel
  Daten über rassische und ethnische Herkunft, politische Meinungen, Gewerksch
  hörigkeit, religiöse oder philosophische Überzeugungen, Gesundheit oder Sexu
  natürlichen Personen.

Anmerkung:
Im Rahmen der IT-Sicherheitspolitik sollte darauf hingewiesen werden, dass die
der Daten sehr sorgfältig vorzunehmen ist. Nicht nur die Einstufung in eine zu
Sicherheitsklasse ist mit potentiellen Gefahren verbunden, auch die leichtfer
eine zu hohe Sicherheitsklasse ist zu vermeiden, da etwa die Behandlung von g
durchwegs mit erheblichem Aufwand verbunden ist.

Schritt 2: Festlegung der Verantwortlichkeiten und der Vorgehensweise

Es ist generell festzulegen, wer die Klassifikation der Daten vorzunehmen hat
einzelnen Organisationen unterschiedlich sein und auch von IT-System zu IT-Sys
differieren.

Als allgemeine Richtlinie kann gelten, dass die Klassifikation einer Informat
vorzunehmen ist, von dem diese Information stammt, oder von dem Mitarbeiter de
Organisation, der diese Information von außen erhält. Für IT-Anwendungen wird
Regel der Applikations-/Projektverantwortliche (s. Kap. 2.2.2) sein.
Weiters ist festzulegen, in welcher Form die Klassifkation erfolgt und wie die
gekennzeichnet wird.

Schritt 3: Erarbeitung von Regelungen zur Verwendung elektronischer Informati

In diesem Schritt ist festzulegen, wie die Information in Abhängigkeit von der
klassen zu behandeln ist.

Beispiele dafür sind etwa Vorschriften zur Speicherung von schützenswerter Inf
Zugriffskontrolle, verschlüsselte Speicherung, keine Speicherung auf Laptops
Daten,...), Regelungen für Ausdrucke und Kopien, Vorschriften zur Übertragungs
(Authentisierung, Verschlüsselung, digitale Unterschrift, E-Mails,...), Wieder
Datenträgern, etc.

2.2.5 Organisationsweite Richtlinien zu Sicherheitsmaßnahmen

Grundsätzlich soll die IT-Sicherheitspolitik keine Aussagen zur Implementieru
Sicherheitsmaßnahmen treffen, da diese in einem langlebigen Dokument, wie es
organisationsweite IT-Sicherheitspolitik darstellt, nicht sinnvoll wären.

Sie soll jedoch organisationsweit gültige Richtlinien zu Sicherheitsmaßnahmen
für alle Einsatzbereiche der Informationstechnologie innerhalb einer Institut
kommen. Die Interpretation dieser Richtlinien für spezielle Bereiche muss in
Systemsicherheitspolitiken, etwa der Internet-Sicherheitspolitik oder der PC-S
erfolgen.

Die Inhalte dieses Kapitels sind von den einzelnen Ressorts bzw. Organisation
festzulegen. Im Folgenden wird eine Reihe von Themen angeführt, die im Rahmen
Sicherheitspolitik typischerweise behandelt werden sollten. Die Tiefe der ein
abhängig von der Bedeutung der Themen für die Organisation.

1. Computersicherheit

Dieser Abschnitt soll die wichtigsten Sicherheitsmaßnahmen zum Schutz von Rec
Einzelkomponenten umfassen. Zu betrachten sind dabei, je nach Hardwareausstat
Mainframes, Server, Workstations, PCs und Notebooks.

Die IT-Sicherheitspolitik sollte Aussagen zu zumindest folgenden Punkten tref

Ü *Zugriffskontrolle*
- Benutzeridentifikation
- Authentisierung von Personen und Geräten
- Beschränkung der Anzahl vergeblicher Zugriffsversuche

  * Rechteverwaltung und Rechteprüfung
  * Bildschirmsperre

ü *Protokollierung*
  * Auswahl der zu protokollierenden Information
  * Speicherung und Auswertung von Protokollen
  * Verantwortlichkeiten

ü *Virenschutz*
  * Virenschutzkonzept
  * Verpflichtung zur Überprüfung von Datenträgern und Files
  * Aktionen bei Auftreten eines Virus

ü *Aufstellung und Installation von Geräten*

ü *Wartung und Reparatur*

ü *Außerbetriebnahme von Geräten*

2. Netzwerksicherheit

Ziel der Netzwerksicherheit ist der Schutz von Information in Netzwerken sowie der Netzwerk-Infrastruktur. Zu betrachten sind sowohl interne Netzwerke als auch Kommunikation über öffentliche Netze.

Dazu sind im Rahmen der IT-Sicherheitspolitik Aussagen u.a. zu folgenden Punkten zu tref

ü *Schutz der Netzwerkkomponenten (z.B. Firewalls, Router)*

ü *Sicherheit der Daten während der Übertragung*

ü *Firewalls*

ü *Internet/Intranet*

ü *Remote Support*

3. Software

In diesem Kapitel sind u.a. zu regeln:
ü der Einsatz von Originalsoftware,
ü Verteilung von Software,

ü private Verwendung dienstlicher Hard- und Software,
ü Verwendung privater Hard- und Software für dienstliche Zwecke,
ü Evaluierung und Zertifizierung von sicherheitskritischen Anwendungen gemäß internationalen Kriterienkatalogen (etwa ITSEC, Common Criteria,...).

4. Sicherheit in der Systementwicklung

Es ist dafür Sorge zu tragen, dass der IT-Sicherheitsprozess so weit wie mögl
gesamten Lebenszyklus eines IT-Systems integriert wird. Dazu sind auch die Ve
keiten für die Sicherheit in den einzelnen Phasen der Systementwicklung sowie
Pflichten der Beteiligten festzulegen.

Dies betrifft
ü Eigenentwicklungen durch IT-Abteilung,
ü Eigenentwicklungen durch interne Anwender sowie
ü Systementwicklung durch Externe.

Dabei sind die sicherheitsrelevanten Aspekte zumindest folgender Bereiche zu
ü Vorgehensmodelle
ü Methodik
ü Trennung von Entwicklung und Produktion
ü Qualitätssicherung / Qualitätsmanagement
ü Dokumentation (z.B. Übergabe oder Hinterlegen des Sourcecodes bei
Fremdentwicklungen)

5. Personelle Sicherheit

Auch personelle Angelegenheiten sollten, soweit sie direkt auf die IT-Sicherhe
nehmen, in der IT-Sicherheitspolitik geregelt werden. Dazu zählen etwa:
ü Voraussetzungen und Maßnahmen bei Einstellung und Ausscheiden von Mitarbeit
(Geheimhaltungsverpflichtungen, Vergabe/Sperre/Löschen von User-IDs, Passwor
Verwaltung,...)
ü Schulungsprogramme
ü Programme zur Sensibilisierung für sicherheitsrelevante Fragen
ü Regelungen für den Einsatz von Fremdpersonal

Darüber hinaus sollten in diesem Rahmen Policies zu den sicherheitsrelevanten
ü Teleworking,
ü Outsourcing und
ü Remote Support

---

formuliert werden, falls Anwendungen dieser Art existieren oder geplant sind.

Optional können darüber hinaus im Rahmen der IT-Sicherheitspolitik auch Regel
zu folgenden Bereichen - soweit sie direkten Bezug zur IT-Sicherheit haben - g
werden:

Bauliche Sicherheit
Umgang mit Dokumenten in Schriftform und auf elektronischen Speichermedien
Telefon und FAX

2.2.6 Disaster Recovery Planung

Ziel der Disaster Recovery Planung ist es, die Verfügbarkeit der wichtigsten A
Systeme innerhalb eines definierten Zeitraumes zu gewährleisten sowie Verkehr

Systeme innerhalb eines definierten Zeitraumes zu gewährleisten sowie Vorkehr
Schadensbegrenzung im Katastrophenfall zu treffen.

Der in der IT-Sicherheitspolitik zu beschreibende Planungsprozess sollte die
angeführten Bereiche umfassen. Die eigentliche Durchführung der Schritte (als
Erfassung der Anwendungen oder die Erstellung eines Backup-Konzeptes) ist nic
der IT-Sicherheitspolitik, sondern muss in den entsprechenden weiteren Aktivi

1. Definition von Verfügbarkeitsklassen

Um den Verfügbarkeitsanspruch von IT-Anwendungen einer Organisation darstelle
können, sind im Rahmen der IT-Sicherheitspolitik entsprechende Verfügbarkeits
definieren.

Nachfolgend ein Beispiel für ein solches Klassifizierungsschema:

* Verfügbarkeitsklasse 1:
  Die Applikation muss innerhalb von einigen Minuten wieder verfügbar sein.

* Verfügbarkeitsklasse 2:
  Die Applikation muss innerhalb von einigen Stunden wieder verfügbar sein.

* Verfügbarkeitsklasse 3:
  Die Applikation muss innerhalb von einigen Tagen wieder verfügbar sein.

---

2. Erfassung aller Anwendungen und Klassifikation nach Verfügbarkeitsanforde

Um die Verfügbarkeit der wichtigsten DV-Anwendungen einer Organisation zu gewä
ist eine Klassifizierung aller Anwendungen gemäß den oben zu definierenden Kla
vorzunehmen.

3. Festlegung der Schadensereignisse, gegen die Vorkehrungen zu treffen sind; Risikoakzeptanz bei nicht abzudeckenden Ereignissen

Ein Disaster Recovery Plan muss nicht notwendigerweise alle Schadensereigniss
die IT-Sicherheitspolitik soll die wesentlichen Leitlinien darüber vorgeben, w
ereignisse abzudecken sind und wie mit den nicht abzudeckenden Ereignissen um

4. Notfallorganisation und Notlaufplan

Hier sind die wichtigsten Anforderungen und Leitlinien zum Thema Notfallorgan
anzuführen. Dazu gehören:
ü die Festlegung der Verantwortlichkeiten und insbesondere die Benennung eine
  Notfallverantwortlichen;
ü die schriftliche Festlegung von Sofortmaßnahmen im Katastrophenfall

5. Erstellung eines Backup-Konzeptes

Dieses Kapitel umfasst die Anforderungen an
ü ein Datensicherungskonzept,
ü einen Datensicherungsplan,
ü die Backup-Planung für Hardware- und Netzwerkkomponenten (Ausweich-RZ, Backu
Verträge,...)
ü Redundanzplanung (Spiegelsysteme,...) sowie
ü die Wiederbeschaffbarkeit von Hard- und Software.

6. Erstellung von Wiederanlaufplänen

Die Vorgangsweise für einen geregelten Wiederanlauf nach Ausfall einer IT-Komp
eines IT-Systems ist in Form von schriftlichen Arbeitsanweisungen ("Wiederanl
niederzulegen.

Dazu zählen:
ü Aufbau und Installation der notwendigen Hardware-Komponenten,
ü Einspielen der Systemsoftware,
ü Einspielen der Anwendungssoftware,
ü Bereitstellen der notwendigen Daten einschließlich Konfigurationsdateien,
ü Wiederanlauf.

Eine revisionsfähige Protokollierung des Wiederanlaufs ist zu gewährleisten.

Weiters sind die Verantwortlichkeiten für die Erstellung, regelmäßige Tests so
Umsetzung des Wiederanlaufplanes im Ernstfall festzulegen.

7. Regelmäßige Tests und Training

In diesem Abschnitt sind die Anforderungen an Testpläne für das Disaster Recov
mäßige Tests (etwa Alarmierungspläne, Wiedereinspielen gesicherter Daten, Ver
Applikationen auf Ausweichsysteme) zu definieren.

8. Weiterentwicklung und Anpassung des Disaster Recovery Plans

Um die Funktionsfähigkeit und Effizienz des Disaster Recovery Plans zu gewähr
dieser regelmäßig auf seine Aktualität zu prüfen und gegebenenfalls an Veränd
anzupassen.

2.2.7 Nachfolgeaktivitäten zur Überprüfung und Aufrechterhaltung der Sicherh

Ein IT-Sicherheitskonzept ist kein statisches, unveränderbares Dokument, umfas
Sicherheitsmanagement beinhaltet vielmehr auch die kontinuierliche Aufgabe, I
laufenden Betrieb aufrechtzuerhalten.

Die IT-Sicherheitspolitik muss daher Leitlinien zur Bewertung der IT-Sicherhei
Angemessenheit, Wirksamkeit und Ordnungsmäßigkeit der eingesetzten IT-Sicherhe
maßnahmen sowie deren Übereinstimmung mit der IT-Sicherheitspolitik und dem I
Sicherheitskonzept vorgeben.

Sicherheitskonzept vorgeben.

Dies umfasst folgende Themenbereiche:

1. Aufrechterhaltung des erreichten Sicherheitsniveaus

Erstes Ziel aller Follow-Up-Aktivitäten muss es sein, das einmal erreichte Si
auch im laufenden Betrieb zu erhalten.

Dazu ist es erforderlich, dass
ü Wartung und administrativer Support der Sicherheitseinrichtungen gewährleist
ü die realisierten Maßnahmen regelmäßig auf ihre Übereinstimmung mit der IT-
Sicherheitspolitik geprüft (*Security Compliance Checking*) und
ü die IT-Systeme fortlaufend überwacht werden (*Monitoring*)

2. Change Management

Hier ist festzulegen, wie eine angemessene Reaktion auf alle sicherheitsreleva
oder Software-Änderungen in einem IT-System sichergestellt werden soll.

3. Reaktion auf sicherheitsrelevante Ereignisse (Incident Handling)

Hier sind die Aufgaben und Verantwortlichkeiten aller Mitarbeiter bei Auftret
sicherheitsrelevanten Ereignissen festzulegen. Ziel ist die Erstellung von "I
Plänen" sowohl für die einzelnen Bereiche als auch für die gesamte Organisatio

Die IT-Sicherheitspolitik soll wiederum nur die Leitlinien für die Aufrechterh
heit im laufenden Betrieb festlegen. Details zum tatsächlichen Vorgehen sind
Plänen und Vorgaben festzuschreiben (s. dazu Kap. 6 dieses Handbuches).

2.3 Life Cycle der IT-Sicherheitspolitik

2.3.1 Erstellung

Die IT-Sicherheitspolitik soll von allen Mitarbeitern getragen werden. Es ist
dass bei ihrer Erstellung alle wesentlichen Kräfte der Organisation beteiligt
Dokument mit Vertretern aller Beteiligten bzw. Betroffenen abgestimmt wird.

Zunächst ist ein Verantwortlicher für die Erstellung der IT-Sicherheitspolitik
Im Allgemeinen wird dies, soweit bereits definiert, der Datenschutz-/IT-Sicher
sein.

Weiters sollen Vertreter folgender Bereiche an der Erstellung der organisatio
Sicherheitspolitik mitarbeiten bzw. in den Abstimmungsprozess miteinbezogen w
ü IT-Abteilung
ü Anwender
ü Sicherheitsabteilung
ü Personalabteilung

ü Gebäudeverwaltung und Infrastruktur
ü Revision
ü Budgetabteilung

Die wesentlichen Inhalte der IT-Sicherheitspolitik müssen allen Betroffenen u
also allen Mitarbeitern der Organisation, aber auch etwa externen Mitarbeiter
Lieferanten, bekannt sein.
Dazu sollten in der Folge die für die einzelnen Personengruppen wichtigsten R
Vorgaben der IT-Sicherheitspolitik zusammengefasst und jedem Betroffenen in s
Form zur Kenntnis gebracht werden. Wo nötig, sind das Einverständnis mit dies
und die Kenntnis der daraus erwachsenden Verpflichtungen auch durch eine Unte
bestätigen zu lassen (etwa Verpflichtung auf das Datengeheimnis, Ergänzungen z
Dienstverträgen, Geheimhaltungsverpflichtungen von externen Personen,...)

2.3.2 Offizielle Inkraftsetzung

Die IT-Sicherheitspolitik wird von der Leitung der Organisation offiziell ver
Kraft gesetzt.

Wesentliche Voraussetzung für eine erfolgreiche Implementierung und Umsetzung
Sicherheitspolitik ist, dass sie die volle und für jeden Beteiligten sichtbar
das Management erhält.

2.3.3 Regelmäßige Überarbeitung

Zwar stellt die IT-Sicherheitspolitik ein langfristiges Dokument dar, dennoch
regelmäßig auf ihre Aktualität und Übereinstimmung mit den tatsächlichen Anfo
überprüfen und bei Bedarf entsprechend anzupassen. Die Verantwortung dafür is
festzulegen. Im Allgemeinen wird sie beim Datenschutz-/IT-Sicherheitsbeauftra

3 Risikoanalyse

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

3.1 Risikoanalysestrategien

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

Die aktuelle Literatur kennt verschiedene Optionen für solch eine Strategie, von denen di wichtigsten drei im Rahmen dieses Handbuches behandelt werden.

* Detaillierte Risikoanalyse:
  Für alle IT-Systeme wird eine detaillierte Risikoanalyse durchgeführt. Diese Methode fü 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 pauschali sierten Gefährdungslage ausgegangen. Als Sicherheitsmaßnahmen kommen sog. Grund- schutzmaßnahmen (*Baseline Security Controls*) zum Einsatz. Durch den Verzicht auf eine detaillierte Risikoanalyse spart diese Vorgehensweise Ressourcen und führt schnell zu e relativ hohen Niveau an Sicherheit. Der Nachteil liegt darin, dass der Grundschutzleve 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 Schutzbedar kategorie "niedrig bis mittel" wird auf eine detaillierte Risikoanalyse verzichtet. Di eine schnelle und effektive Auswahl von grundlegenden Sicherheitsmaßnahmen bei gleich- zeitiger Gewährleistung eines angemessenen Schutzniveaus. IT-Systeme der Schutzbedarfs- kategorie "hoch bis sehr hoch" sind einer detaillierten Risikoanalyse zu unterziehen, deren Basis individuelle Sicherheitsmaßnahmen ausgewählt werden.

Diese Option kombiniert die Vorteile des Grundschutz- und des Risikoanalysea alle IT-Systeme mit hohem Schutzbedarf wirksam und angemessen geschützt werd Maßnahmen für die anderen Systeme mit Hilfe des Grundschutzes schnell und ef ausgewählt werden können. Sie wird in den meisten Einsatzumgebungen die empf vorte Strategie zur Risikoanalyse darstellen.

werte Strategie zur Risikoanalyse darstellen.

Im Folgenden werden die drei angeführten Risikoanalysestrategien näher erläute

3.2 Detaillierte Risikoanalyse

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

Die erstmalige Durchführung einer detaillierten Risikoanalyse und die anschli
eines Sicherheitskonzeptes erfordert einen Aufwand, der zumindest im Bereich
ev. auch von Monaten liegt. Zur Reduktion des Aufwandes kann man für IT-Syste
denen lediglich Anwendungen mit niedrigem bis mittlerem Schutzbedarf laufen,
detaillierte Risikoanalyse verzichten und Grundschutzmaßnahmen zum Einsatz br
dazu Kap. 3.3 und 3.4).

IT-Systeme, auf denen Anwendungen mit hohem oder sehr hohem Schutzbedarf inst
erfordern hingegen eine genaue Analyse der bestehenden Werte, Bedrohungen und
stellen und damit die Durchführung einer detaillierten Risikoanalyse.

Eine detaillierte Risikoanalyse umfasst folgende Schritte:

Schritt 1: Abgrenzung des Analysebereiches

Hier ist das zu analysierende IT-System zu spezifizieren und anzugeben, ob un
Maße auch andere Objekte (z.B. Gebäude und Infrastruktur) in die Analyse einb
sollen.

Schritt 2: Identifikation der bedrohten Objekte ("Assets")

Ziel dieses Schrittes ist die Erfassung aller bedrohten Objekte, die innerhal
gangenen Schritt festgesetzten Analysebereiches liegen.

Schritt 3: Wertanalyse

In diesem Schritt wird der Wert der bedrohten Objekte ermittelt. Die Wertanal
Einzelnen:
ü die Festlegung der Bewertungsbasis für Sachwerte
ü die Festlegung der Bewertungsbasis für immaterielle Werte
ü Ermittlung der Abhängigkeiten zwischen den Objekten
ü Bewertung der bedrohten Objekte

Schritt 4: Bedrohungsanalyse

Die Objekte sind vielfachen Bedrohungen ausgesetzt, die sowohl aus Nachlässig
Versehen als auch aus Absicht resultieren können. Die Bedrohungsanalyse umfas

ü die Identifikation möglicher Bedrohungen (Katastrophen, Fehlbedienung, bewus
Angriffe) und möglicher Angreifer (Mitarbeiter, Leasingpersonal, Außensteher
ü die Ermittlung der Eintrittswahrscheinlichkeiten

Schritt 5: Schwachstellenanalyse

Eine Bedrohung kann nur durch die Ausnutzung einer vorhandenen Schwachstelle
werden. Es ist daher erforderlich, mögliche Schwachstellen des Systems in de
ü Organisation
ü Hard- und Software
ü Personal
ü Infrastruktur
zu identifizieren und ihre Bedeutung zu klassifizieren.

Schritt 6: Identifikation bestehender Sicherheitsmaßnahmen

Zur Vermeidung unnötiger Aufwände und Kosten sind die bereits existierenden S
maßnahmen zu erfassen und auf ihre Auswirkungen hinsichtlich der Gesamtsystem
sowie auf korrekte Funktion zu prüfen. Geplante neue Sicherheitsmaßnahmen müs
existierenden kompatibel sein und eine wirtschaftlich und technisch sinnvolle
darstellen.

Schritt 7: Risikobewertung

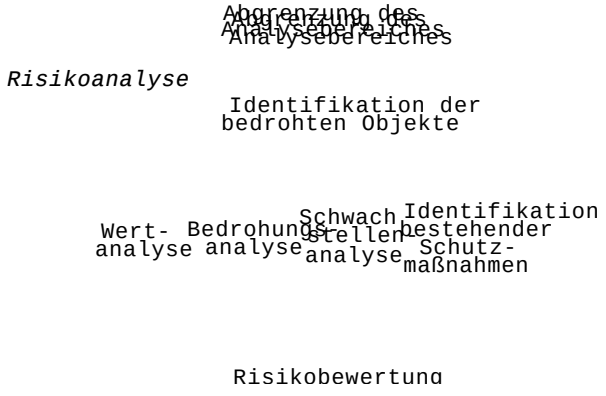
In diesem Schritt werden die Einzelrisiken und das Gesamtrisiko ermittelt und

---

Schritt 8: Auswertung

Eine Auswertung und Aufbereitung des Ergebnisses schließt die Risikoanalyse a

Der Zusammenhang zwischen diesen Schritten sowie die Einbettung der Risikoana
IT-Sicherheitsprozess ist in der folgenden Graphik dargestellt (vgl [ISO/IEC



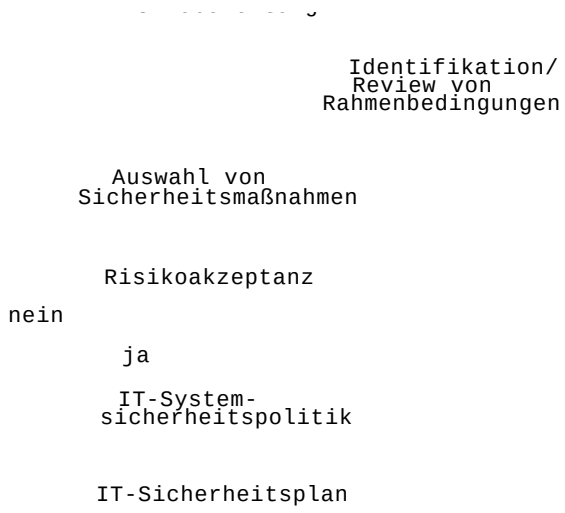


Abbildung 3.1: Risikomanagement mit detaillierter Risikoanalyse

---

Bei der Durchführung einer Risikoanalyse sind folgende Prinzipien zu beachten

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

In den nachfolgenden Kapiteln werden die einzelnen Schritte einer Risikoanaly
behandelt. Das vorliegende Handbuch gibt Hinweise und Unterstützung zur Durch
dieser Schritte. Die Wahl einer konkreten Risikoanalysemethode sowie ein etwa
von Tools zur Unterstützung dieser Analyse bleiben der durchführenden Institu
Wichtig ist, dass alle der im Folgenden angeführten Schritte durchgeführt werd
geforderten Ergebnisse liefern.

3.2.1 Abgrenzung des Analysebereiches

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

3.2.2 Identifikation der bedrohten Objekte (Werte, assets)

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

Unter den bedrohten Objekten einer Organisation ist alles zu verstehen, was fü schutzbedürftig ist, also alle Objekte, von denen der Betrieb des IT-Systems u Anwendungen und damit die Funktionsfähigkeit der Organisation abhängen. Dazu z

ü physische Objekte:
Gebäude, Infrastruktur, Hardware, Datenträger, Paperware,...

ü logische Objekte:
Software, Daten, Information,...
ü Personen
ü Fähigkeiten:
Herstellen eines Produktes, Erbringen einer Dienstleistung,...
ü immaterielle Güter:
Image, Vertrauen in die Institution, gute Beziehungen zu anderen Organisatio

Zwischen den bedrohten Objekten bestehen grundsätzlich komplexe Abhängigkeiter Vertraulichkeit, Integrität oder Verfügbarkeit eines Objektes setzt vielfach e Integrität oder Verfügbarkeit eines anderen Objektes voraus. Beispiele dafür s
ü die Erfordernis einer funktionsfähigen Infrastruktur (Stromversorgung, Klima den Betrieb eines IT-Systems,
ü die Abhängigkeit der Software von unversehrter und verfügbarer Hardware oder
ü die Voraussetzung korrekter Applikations- und Betriebssystemsoftware für die der Anwendungsdaten.

Die Identifizierung der bedrohten Objekte sowie ihre nachfolgende Bewertung s wesentliche Voraussetzungen für ein erfolgreiches IT-Sicherheitsmanagement dar den Erfordernissen im Einzelfall anzupassen, in welcher Tiefe und in welchem M grad die einzelnen Objekte analysiert werden sollen; in vielen Fällen wird ein fassung in Gruppen sinnvoll sein und beitragen, den Analyseaufwand zu begrenze

3.2.3 Wertanalyse

In diesem Schritt wird der Wert der im vorangegangenen Schritt identifizierten ermittelt. Die Wertanalyse umfasst im Einzelnen:

Aktion 1: Festlegung der Bewertungsbasis für Sachwerte
Aktion 2: Festlegung der Bewertungsbasis für immaterielle Werte
Aktion 3: Ermittlung der Abhängigkeiten zwischen den Objekten
Aktion 4: Bewertung der bedrohten Objekte

3.2.3.1 Festlegung der Bewertungsbasi s für Sachwerte

Zunächst ist zu entscheiden, ob die Bewertung quantitativ oder qualitativ erf

Eine quantitative Bewertung kann etwa beruhen auf
ü dem Zeitwert eines Objektes,

ü dem Wiederbeschaffungswert eines Objektes,
ü dem Wert, den das Objekt für einen potentiellen Angreifer hätte, oder
ü dem Schaden, der sich aus dem Verlust oder der Modifikation eines zu schütze
Objektes für die betroffene Organisation ergibt.

Eine qualitative Bewertung erfolgt durch Einteilung in Klassen. Beispiele hie
ü 3-stufige Bewertung: gering - mittel - hoch
ü 5-stufige Bewertung: unbedeutend - gering - mittel - hoch - sehr hoch

3.2.3.2 Festlegung der Bewertungsbasis für immaterielle Werte

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

Eine quantitative Bewertung kann in diesem Fall beruhen auf
ü dem Wert, den das Objekt für einen potentiellen Angreifer hätte (z.B. vertra
Information), oder
ü dem Schaden, der sich aus einem Angriff auf das zu schützende Objekt für die
Organisation ergibt.

Eine qualitative Bewertung erfolgt wiederum durch Zuordnung diskreter Werte u
einer Einteilung in Klassen. Beispiele hierfür sind etwa:
ü 3-stufige Bewertung: gering - mittel - hoch
ü 5-stufige Bewertung: unbedeutend - gering - mittel - hoch - sehr hoch

3.2.3.3 Ermittlung der Abhängigkeiten zwischen den Objekten

Es ist wichtig, auch die gegenseitige Abhängigkeit von Objekten festzustellen,
auf die Bewertung der einzelnen zu schützenden Objekte haben kann.
So ist etwa die Funktionsfähigkeit der Hardware abhängig von der Funktionsfäh
Stromversorgung und ev. der Klimaanlage. Die Integrität von Information bedin
Integrität und Verfügbarkeit der Hard- und Software, die zu ihrer Verarbeitun
Speicherung eingesetzt wird.

3.2.3.4 Bewertung der bedrohten Objekte

Mit Ausnahme der Festsetzung von Zeit- oder Wiederbeschaffungswert wird die Be
von bedrohten Objekten i.a. sehr subjektiv sein. Es ist daher notwendig, im Ra
Analyse:
ü möglichst genaue Bewertungsbasen und Regeln vorzugeben und diese eventuell
  Beispiele zu illustrieren,
ü möglichst viele unterschiedliche Personen nach ihrer Einschätzung zu befrage

Durchführung:
ü Die Person, die die Risikoanalyse durchführt, erstellt eine Liste der zu be
  und gibt die Bewertungsbasen vor.
ü Die Bewertung sollte durch die Applikations-/Projektverantwortlichen sowie
  betroffenen Benutzer vorgenommen werden.
ü Unterstützung in der Bewertung kann von verschiedenen Abteilungen, etwa Fin
  Einkauf, EDV,...kommen.
ü Es ist Aufgabe desjenigen, der die Risikoanalyse durchführt, die einzelnen
  Plausibilität und Konsistenz zu prüfen und ein konsolidiertes Ergebnis zu er

Ergebnis der Wertanalyse:
Aufstellung der bedrohten Objekte und ihres Wertes für die Organisation.

3.2.4 Bedrohungsanalyse

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

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

Bedrohungen sind charakterisiert durch:

ü ihren Ursprung:
  Bedrohungen durch die Umwelt oder durch den Menschen, wobei letztere wieder
  absichtliche oder zufällige Bedrohungen zu unterteilen sind; im Falle absich
  Bedrohungen ist weiters zwischen Innentätern und Außentätern zu unterscheide
ü die Motivation:
  etwa finanzieller Gewinn, Wettbewerbsvorteil, Rache, Geltungssucht, Publici
ü die Häufigkeit des Auftretens

ü die Größe des Schadens, der durch diese Bedrohung verursacht werden kann

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

Die Bedrohungsanalyse umfasst im Einzelnen:
Aktion 1: die Identifikation möglicher Bedrohungen
Aktion 2: die Ermittlung der Eintrittswahrscheinlichkeiten

3.2.4.1 Identifikation m öglicher Bedrohungen

Bedrohungen können unterteilt werden in:

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

Es ist wichtig, alle wesentlichen Bedrohungen zu erfassen, da andernfalls Sich
bestehen bleiben können.
Bei der Identifikation von möglichen Bedrohungen können Bedrohungskataloge hil
die den Charakter von Checklisten haben. Solche Kataloge finden sich etwa in
207 ff und in [ISO/IEC 13335-3], Annex C. Es ist jedoch zu betonen, dass keine
Liste vollständig sein kann, und darüber hinaus auch Bedrohungen einem ständig
und einer ständigen Weiterentwicklung unterworfen sind. Es ist daher immer not
Bedrohungskataloge hinaus auch die Möglichkeit weiterer Bedrohungen in Betrach

In diesem Schritt ist auch zu überlegen, von wem eine Bedrohung jeweils ausgeh
Mitarbeiter, Leasingpersonal, Externe). Der Schutz gegen Innentäter ist mit te

---

Maßnahmen oft nur unzureichend oder mit sehr hohem Aufwand zu bewerkstelligen
in verstärktem Maß auf personelle und organisatorische Maßnahmen zurückzugreif

3.2.4.2 Ermittlung der Eintrittswahrscheinlichkeiten

In diesem Schritt ist zu bestimmen, mit welcher Wahrscheinlichkeit eine Bedrol
betrachteten Umfeld eintreten wird. Diese ist abhängig von:

ü der Häufigkeit der Bedrohung (Wahrscheinlichkeit des Auftretens anhand von

Statistiken,...),
ü der Motivation und den vorausgesetzten Fähigkeiten und Ressourcen eines pote
Angreifers,
ü Einschätzung der Attraktivität und Verwundbarkeit des IT-Systems bzw. seiner
Komponenten,
ü Umweltfaktoren und organisationsspezifischen Einflüssen.

Auch die Eintrittswahrscheinlichkeit kann quantitativ oder qualitativ bewertet

Da eine quantitative Bewertung in vielen Fällen eine Genauigkeit vortäuschen k
durch die ungenaue Methode der Schätzung nicht zu rechtfertigen ist, ist in de
ein Trend in Richtung qualitative 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 Anwend
zu konkretisieren. Im Allgemeinen werden sie in "Anzahl pro Zeiteinheit" ange
sollten so festgelegt werden, dass die Bedeutung der Ziffern von 0 bis 4 glei

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

Es kann durchaus sinnvoll oder sogar erforderlich sein, für verschiedene Anwen
unterschiedliche Auslegungen der Werteskala zu definieren.

Ergebnis der Bedrohungsanalyse:
Liste von Bedrohungen, der von ihnen bedrohten Objekte, und ihrer Eintrittswa
keiten.

3.2.5 Schwachstellenanalyse

vulnerability

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

Schwachstellen können etwa bei Gebäuden, Hardware, Software, in der Organisati
Verwaltung sowie beim Personal auftreten.

Typische Beispiele für Schwachstellen sind etwa:
ü Mangelnder baulicher Schutz von Räumen mit IT-Einrichtungen (Bereich Gebäude
ü Nachlässige Handhabung von Zutrittskontrollen (Bereich Gebäude)
ü Spannungs- oder Temperaturschwankungen (Bereich Hardware)
ü kompromittierende Abstrahlung (Bereich Hardware)

ü Spezifikations- und Implementierungsfehler (Bereich Software)
ü schwache Passwortmechanismen (Bereich Software)
ü unzureichende Ausbildung, mangelndes Sicherheitsbewusstsein (Bereich Persona

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

Eine *Schwachstellenanalyse* ist die Überprüfung von Sicherheitsschwächen, die durch fes
gestellte Bedrohungen ausgenutzt werden können. Diese Analyse muss sowohl das
auch bereits vorhandene Schutzmaßnahmen miteinbeziehen. Es ist wichtig, jede S
daraufhin zu bewerten, wie leicht es ist, sie auszunutzen.

Beispielhafte Auflistungen von Schwachstellen, die auf typische Problembereich
finden sich etwa in [ISO/IEC 13335-3], Annex D sowie in [BSI 7105], S 199 ff.

Ergebnis der Schwachstellenanalyse:
Liste von potentiellen Schwachstellen mit Angaben darüber, wie leicht diese fü
ausgenützt werden können.

3.2.6 Identifikation bestehender Sicherheitsmaßnahmen

Sicherheitsmaßnahmen sind Verfahrensweisen, Prozeduren und Mechanismen, die e
mehrere der nachfolgenden Funktionen erfüllen:
ü Vermeidung von Risiken,
ü Verkleinerung von Bedrohungen oder Schwachstellen,
ü Entdeckung unerwünschter Ereignisse,
ü Eingrenzung der Auswirkungen eines unerwünschten Ereignisses,
ü Überwälzung von Risiken oder
ü Wiederherstellung eines früheren Zustandes.

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

Da die Sicherheitsmaßnahmen, die aufgrund einer Risikoanalyse ausgewählt werde
zusätzlich zu bereits bestehenden Maßnahmen eingeführt werden sollen, ist es n
bereits existierenden oder geplanten Sicherheitsmaßnahmen zu identifizieren un
Auswirkungen zu überprüfen, um unnötigen Aufwand zu vermeiden.

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

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

Ergebnis:
Aufstellung aller bereits existierenden oder geplanten Sicherheitsmaßnahmen m

ihren Implementierungsstatus und ihren Einsatz.

3.2.7 Risikobewertung

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

Ziel dieses Schrittes ist es, die Risiken, denen ein IT-System und seine Objek
zu erkennen und zu bewerten, um auf dieser Basis geeignete und angemessene Si
maßnahmen auswählen zu können.

Risiken sind eine Funktion folgender Parameter:

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

Wie diese Größen miteinander verknüpft werden, um die Höhe der Einzelrisiken u
Gesamtrisikos zu bestimmen, ist abhängig von der gewählten Risikoanalysemetho
können quantitative oder qualitative Bewertungen vorgenommen oder aber beide
keiten kombiniert werden. [ISO/IEC 13335-3] gibt in Annex E vier Beispiele für
Risikobewertung.
Im IT-Sicherheitshandbuch des BSI wird eine quantitative Bewertung des Risiko
Wertepaaren (Schadensausmaß, Eintrittswahrscheinlichkeit) und anschließend ein
der Risiken in "tragbare" und "untragbare" vorgenommen ([BSI 7105], S. 63ff u

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

Ergebnis:
Quantitative oder qualitative Bewertung von Einzelrisiken und Gesamtrisiko für
ten Analysebereich.

3.2.8 Auswertung und Aufbereitung der Ergebnisse

Der adäquaten Aufbereitung, Auswertung und Interpretation der Ergebnisse eine
analyse kommen wachsende Bedeutung zu. Da die Risikoanalyse auch als Grundlag
reichende weiterführende Entscheidungen dient, ist auf eine klare Darstellung
sowie eine umfassende Ergebnisdarstellung zu achten. Hilfreich dabei sind gra
tabellarische Darstellungen.

3.3 Grundschutzansatz

Die im Rahmen dieses Handbuches empfohlene Vorgehensweise zur Grundschutzanal
im Wesentlichen den Vorgaben des IT-Grundschutzhandbuches des BSI ([BSI GSHB]
diesem Kapitel wird eine kurze Zusammenfassung des Verfahrens, angepasst an d
nisse der öffentlichen Verwaltung in Österreich, gegeben. Details zum Verfahr
Katalog von Grundschutzmaßnahmen finden sich in [BSI GSHB]. Darüber hinaus kö
weitere Grundschutzkataloge herangezogen werden, wie etwa [ISO 13569], [BS 77
eigenerstellte Kataloge aufgrund spezifischer Anforderungen (s.u.).

3.3.1 Die Idee des IT-Grundschutzes

Ziel des Grundschutzansatzes ist es, den Aufwand für die Erstellung eines IT-S
konzeptes angemessen zu begrenzen.
Dies wird dadurch erreicht, dass von einer pauschalisierten Gefährdungslage au
damit auf eine detaillierte Risikoanalyse verzichtet wird. Die Auswahl der zu
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 N
  Sicherheit gegen die häufigsten Bedrohungen.
- Grundschutzmaßnahmen sind meist - da stark verbreitet und in einer Vielzahl
  Organisationen im Einsatz - relativ kostengünstig und schnell zu implementie

Dem stehen folgende Nachteile gegenüber:
- Der Grundschutzlevel kann für das betrachtete System zu hoch oder zu niedri
  zu hoch, werden unnötige finanzielle und personelle Ressourcen verbraucht,
  niedrig, bleiben unter Umständen untragbare Risiken bestehen.
- Aufgrund der fehlenden Risikoanalyse kann unter Umständen eine angemessene
  auf sicherheitsrelevante Hard- oder Softwareänderungen schwierig sein.

Die Wahl eines Grundschutzansatzes wird daher in zwei Fällen empfohlen:

- Falls in einem Bereich (IT-System, Abteilung,...) noch keine oder offensich
  schwache Sicherheitsmaßnahmen vorhanden sind, kann die Realisierung von Gru
  maßnahmen dazu beitragen, rasch ein relativ gutes Niveau an IT-Sicherheit zu
  diesem Fall sollte aber in einem nachfolgenden Schritt geprüft werden, ob da
  Niveau bereits ausreichend ist oder weitere Analysen und Maßnahmen erforder

ü Als Teil eines umfassenden Risikoanalysekonzeptes ("kombinierter Ansatz"):
Wird zunächst in einem ersten Schritt festgestellt, welche IT-Systeme besonc
schutzbedürftig sind ("Schutzbedarfsfeststellung"), so besteht die Möglichke
aufwand für die Risikoanalyse und die Auswahl spezifischer Sicherheitsmaßnah
diese hochschutzbedürftigen Systeme zu konzentrieren. Für alle anderen Syste
Grundschutzmaßnahmen eingesetzt werden, ohne damit unangemessene Sicherheits
einzugehen. Details dazu s. Kap. 3.4.

3.3.2 Grundschutzanalyse und Auswahl von Maßnahmen

Im Folgenden wird ein reiner Grundschutzansatz beschrieben, d.h. es wird davor
dass entweder bereits eine Schutzbedarfsfeststellung erfolgt ist und damit di
identifiziert sind, für die der IT-Grundschutz zu konzipieren ist, oder dass l
ein reiner Grundschutzansatz gewählt wird. Ein kombinierter Ansatz und die Ste
Grundschutzes in einem solchen wird im nachfolgenden Kapitel beschrieben.

Die im Folgenden beschriebene Vorgehensweise ist dem IT-Grundschutzhandbuch de
[BSI GSHB] entnommen und baut auch auf den dort vorgesehenen sehr umfangreiche
Maßnahmenkatalogen auf. Bei Bedarf können einer Grundschutzanalyse - ergänzend
alternativ - auch andere Maßnahmenkataloge zugrunde gelegt werden.

Eine kurze Beschreibung der heute bekanntesten Standardwerke dazu, die jeweil
Inhaltsverzeichnisse sowie die Kontaktadressen finden sich im PDTR [ISO/IEC 1
Dort werden auch weitere, sektorspezifische Dokumente zum IT-Grundschutz angef
Darüber hinaus kann es auch sinnvoll sein, für einzelne Bereiche eigene, an di
Anforderungen angepasste Maßnahmenkataloge zu erstellen.

Anmerkung:
In Teil 2 des gegenständlichen Sicherheitshandbuches werden spezifische Maßnah
für die öffentliche Verwaltung in Österreich erarbeitet.

Vorgehensweise (lt. [BSI GSHB]):
Aktion 1: Abbildung des IT-Systems durch vorhandene Bausteine
Aktion 2: Lesen des jeweiligen Bausteins
Aktion 3: Lesen der Maßnahmenbeschreibungen
Aktion 4: Soll-Ist-Vergleich zwischen vorhandenen und empfohlenen Maßnahmen

Das folgende Bild (aus [BSI GSHB]) gibt eine graphische Darstellung des Ablau

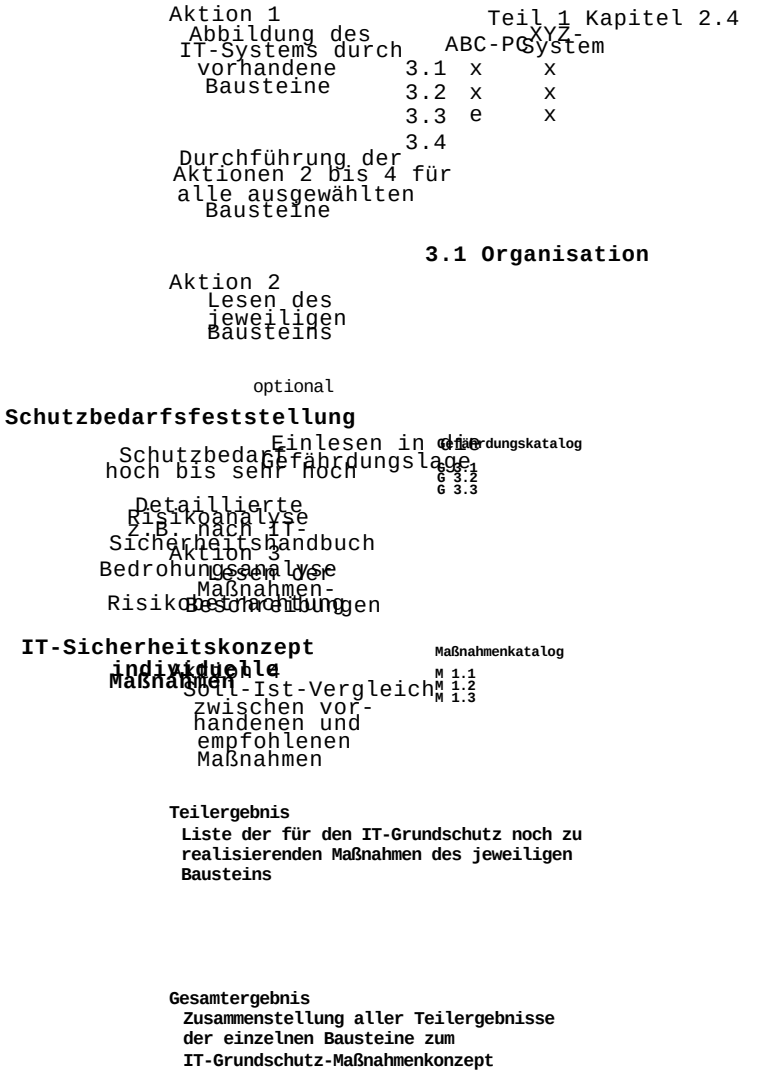


Abbildung 3.2: Vorgehensweise zur IT-Grundschutzanalyse nach dem IT-Grundschutzhandbuch des BSI

3.3.2.1 Abbildung des IT-Systems durch vorhandene Bausteine

Unter Rückgriff auf das IT-Grundschutzhandbuch des BSI, das nach einem "Baukas aufgebaut ist, wird bis zum Erscheinen des Teiles 2 dieses Sicherheitshandbuc dort bestehenden Kataloge (siehe auch Kap. 4.1.4 dieses Handbuches) verwiesen einzelnen "Bausteine", also die entsprechenden Kapitel und Unterkapitel des Ha denen ein reales IT-System nachgebildet werden kann, sind in drei Gruppen zusa (Stand des IT-Grundschutzhandbuches 1998):

* übergeordnete oder grundlegende Komponenten:
  * Organisation
  * Personal
  * Notfallvorsorge-Konzept
  * Datensicherungskonzept
  * Datenschutz
* Infrastruktur:
  * Gebäude
  * Verkabelung
  * Räume
  * Schutzschränke
  * Häuslicher Arbeitsplatz
* IT-spezifische Bausteine aus folgenden Bereichen:
  * nicht-vernetzte Systeme
  * vernetzte Systeme
  * Datenübertragungseinrichtungen
  * Telekommunikation
  * sonstige IT-Komponenten

So wie das IT-Grundschutzhandbuch des BSI ständig fortgeschrieben und um neue
ergänzt wird, ist auch dieses Handbuch nicht statisch, sondern erfolgt eine l
Aktualisierung (siehe insbesondere Teil 2).

Die in dieser Aktion zu leistende Aufgabe besteht darin, das reale IT-System
handenen Bausteine möglichst genau nachzubilden.

Wurde bereits ein IT-Grundschutz-Maßnahmenkonzept für das IT-System erstellt,
überprüft werden, ob in der aktuellen Version des IT-Grundschutzhandbuches ne
beschrieben werden, die zusätzlich zur Abbildung des IT-Systems genutzt werde
damit zusätzlich bearbeitet werden sollten.

3.3.2.2 Lesen des jeweiligen Bausteins

Nun werden die in Aktion 1 ausgewählten Kapitel (= Bausteine) bearbeitet. Jed
Kapitel ist gleichermaßen aufgebaut: nach einer einführenden Beschreibung fol
Aufzählung pauschal für den IT-Grundschutz angenommener Gefährdungen und die
Empfehlung der hiergegen wirkenden Maßnahmen.

Es werden 5 Gruppen von Gefährdungen unterschieden:
ü Höhere Gewalt
ü Organisatorische Mängel
ü Menschliche Fehlhandlungen
ü Technisches Versagen
ü Vorsätzliche Handlungen

Die Maßnahmen sind in 6 Bereiche gegliedert:
ü Infrastruktur
ü Organisation
ü Personal

ü Hardware/Software
ü Kommunikation
ü Notfallvorsorge

Eine ausführliche Beschreibung der Maßnahmen und Gefährdungen wird in Teil 2 d
gegenständlichen Sicherheitshandbuches vorgenommen und ist auch in den Katalo
bzw. M1 M6 des IT-Grundschutzhandbuches enthalten.

3.3.2.3 Lesen der Maßnahmenbeschreibungen

Bei der Bearbeitung eines Kapitels ist es unbedingt erforderlich, die empfohl
und die dazu existierenden Maßnahmenbeschreibungen in den Katalogen sorgfältig
Nur so kann der angestrebte Soll-Ist-Vergleich erfolgreich durchgeführt werde

Neben der eigentlichen Empfehlung, wie die einzelnen Maßnahmen umzusetzen sin
beispielhaft Verantwortliche genannt, die die Initiierung bzw. die Umsetzung
typischerweise bewerkstelligen sollen. Weiterhin werden ergänzende Kontrollfra
die zur Beurteilung der umgesetzten Maßnahmen und für Revisionszwecke hilfrei
können.

3.3.2.4 Soll-Ist-Vergleich zwischen vorhandenen und empfohlenen Maßnahmen

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

Vorgehen bei Abweichungen:
Für die Errichtung eines IT-Grundschutzes sollten alle im Baustein vorgeschla
Grundschutzmaßnahmen umgesetzt werden, es besteht jedoch die Möglichkeit, dass
bestimmten Einsatzumgebungen empfohlene Grundschutzmaßnahmen nicht umgesetzt
können oder sollten. Diese Abweichung von der Empfehlung ist dann zu dokument
begründen.
An dieser Stelle sollten auch eventuell vorhandene über den IT-Grundschutz hi
IT-Sicherheitsmaßnahmen herausgearbeitet und dokumentiert werden.

Ergebnis:

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

3.4 Kombinierter Ansatz

Die Stärken beider oben diskutierter Risikoanalysestrategien - Zeit sparende A
günstiger IT-Sicherheitsmaßnahmen durch Grundschutzanalysen und wirksame Redu
hoher Sicherheitsrisiken durch detaillierte Risikoanalysen - kommen in einem

höher Sicherheitsrisiken durch detaillierte Risikoanalysen - kommen in einem s
kombinierten Ansatz zum Tragen.

Dabei wird zunächst ermittelt, welche IT-Systeme hohe oder sehr hohe Sicherhe
anforderungen haben, und welche niedrige bis mittlere haben (Schutzbedarfsfes
Ergebnis dieses Schrittes ist eine Einteilung in zwei Schutzbedarfskategorien
mittel" und "hoch bis sehr hoch".
IT-Systeme der Schutzbedarfskategorie "niedrig bis mittel" werden einer Grund
unterzogen, während IT-Systeme der Schutzbedarfskategorie "hoch bis sehr hoch
detaillierten Risikoanalyse zu unterziehen sind, auf deren Basis individuelle
maßnahmen ausgewählt werden.

Die nachfolgende Abbildung (aus [BSI GSHB]) verdeutlicht den Zusammenhang zwi
beiden Vorgehensweisen.

Abbildung 3.3: Zusammenhang zwischen IT-Grundschutz und detaillierter R

Stärken und Schwächen eines kombinierten Ansatzes:

- ü Die Vorgehensweise ermöglicht es, rasch einen relativ guten Sicherheitslevel für alle I Systeme zu realisieren.
- ü Die in der Schutzbedarfsfeststellung erarbeiteten Erkenntnisse können die Grundlage für eine Prioritätenreihung für die nachfolgenden Aktivitäten bilden.
- ü Der Aufwand kann auf hochsicherheitsbedürftige Systeme konzentriert werden.
- ü Das Verfahren findet i.a. hohe Akzeptanz, da es mit verhältnismäßig geringem Initial- aufwand rasch sichtbare Erfolge bringt.
- ü Grundsätzlich besteht beim kombinierten Ansatz das Risiko, dass ein hochschutzbedürftig IT-System fälschlicherweise in die Schutzbedarfskategorie "niedrig bis mittel" eingeor wird. Da solche Systeme aber auf jeden Fall durch Grundschutzmaßnahmen geschützt werden, besteht zumindest ein gewisses Sicherheitsniveau. Außerdem ist zu erwarten, das im Rahmen einer Grundschutzanalyse eventuell bestehende höhere Sicherheits- anforderungen erkannt werden und damit in einem nächsten Schritt behandelt werden können.

Empfehlung:

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

3.4.1 Festlegung von Schutzbedarfskategorien

Voraussetzung für eine Schutzbedarfsfeststellung ist die Festlegung von Schutz
kategorien.

Abweichend vom [BSI GSHB], das drei Schutzbedarfskategorien vorsieht, geht die
Handbuch von zwei Kategorien aus:

Schutzbedarfskategorie "niedrig bis mittel":
Die Schadensauswirkungen sind begrenzt und überschaubar. Maßnahmen des IT-Grun
schutzes reichen im Allgemeinen aus.

Schutzbedarfskategorie "hoch bis sehr hoch":
Die Schadensauswirkungen können beträchtlich sein oder sogar ein existentiell
katastrophales Ausmaß erreichen. IT-Grundschutzmaßnahmen alleine reichen ggf.
die erforderlichen Sicherheitsmaßnahmen sollten individuell auf Basis einer Ri
ermittelt werden.

Orientierungshilfe:
Die nachfolgende Tabelle gibt eine Orientierungshilfe für die Festlegung der S
kategorien und damit die Klassifizierung der Anwendungen anhand der maximal mö
Schäden anhand von beispielhaften Grenzwerten. Jede Organisation sollte für si
diese Klassifikation ihren Anforderungen entspricht und gegebenenfalls eigene
Einordnungen festlegen.
Weiters ist darauf hinzuweisen, dass die in der Tabelle angeführten sieben Sch
nicht vollständig sein müssen. Für alle Schäden, die sich nicht in diesen Kate
lassen, ist ebenfalls eine Aussage zu treffen, wo die Grenze zwischen "niedrig
"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 des Betroffenen.	* Schwere Verstöße gegen Gesetze und Vorschriften (Strafverfolgung) * Vertragsverletzungen mit hohen Konventionalstrafen oder Haftungsschäden * Ein möglicher Missbrauch personenbezogener Daten hat erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen (Verlust der Vertraulichkeit oder Integrität sensibler Daten)

	OFFEN / VERTRAULICH	GEHEIM / SENSIBEL
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 VERTRAULICH verarbeitet bzw. gespeichert.	* Es werden auch Daten der Sicherheitsklassen GEHEIM und/oder SENSIBEL verarbeitet bzw. gespeichert.
5. Dauer der Verzichtbarkeit	* Die maximal tolerierbare Ausfallszeit der Anwendung beträgt mehrere Stunden bis mehrere Tage (d.h. die Applikation ist in Verfügbarkeitsklasse 2 oder 3 lt. Bsp. in Kap. 2.2.6 eingestuft)	* Die maximal tolerierbare Ausfallszeit des Systems beträgt lediglich einige Minuten (Verfügbarkeitsklasse 1 lt. Bsp. in Kap. 2.2.6)
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.) ATS 1.000.000.-	* Der zu erwartende finanzielle Schaden ist größer als (z.B.) ATS 1.000.000.-

Abbildung 3.4: Beispiel für die Festlegung der Schutzbedarfskategorien

3.4.2 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

3.4.2.1 Erfassung aller vorhandenen oder geplanten IT-Systeme

Zunächst werden die vorhandenen und geplanten IT-Systeme aufgelistet. Hierbei
technische Realisierung eines IT-Systems im Vordergrund, z. B. stand-alone PC,
Client, Unix-Server, TK-Anlage. An dieser Stelle soll nur das System als solch
werden (z. B. Unix-Server), nicht die einzelnen Bestandteile, wie Rechner, Tas
Bildschirm, Drucker etc., aus denen das IT-System zusammengesetzt ist.

Sollte eine so große Anzahl von IT-Systemen vorhanden sein, dass eine vollstän
nicht angemessen erscheint, so kann man gleiche IT-Systeme zu Gruppen zusammen
wenn von Anwendungsstruktur und -ablauf vergleichbare IT-Anwendungen auf diese
Systemen laufen. Dies gilt insbesondere für PCs, die oft in großer Anzahl vorh

3.4.2.2 Erfass ung der IT-Anwendungen und Zuordnung zu den einzelnen IT-Syste

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

Diese sollten anschließend - soweit zu diesem Zeitpunkt bereits möglich - nach
Sicherheitsbedarf vorsortiert werden. Dabei sind zuerst diejenigen Anwendunge
jeweiligen IT-Systems zu benennen,
ü deren Daten/Informationen und Programme den höchsten Bedarf an Vertraulichke
ü deren Daten/Informationen und Programme den höchsten Bedarf an Integrität au
ü die die kürzeste tolerierbare Ausfallszeit haben.

Anmerkung:
Als Basis für die Erfassung der IT-Systeme und der darauf laufenden oder gepla
Anwendungen können im Bereich der öffentlichen Verwaltung in Österreich beispi
4-Jahres-Konzepte (strategische IT-Planung) sowie der jährliche ADV-Bericht fü
dienen.

3.4.2.3 Schutzbedarfsfeststellung für jedes IT-System

In dieser Phase soll die Frage beantwortet werden, welche Schäden zu erwarten
Vertraulichkeit, Integrität oder Verfügbarkeit einer IT-Anwendung und/oder der
Informationen ganz oder teilweise verloren gehen. Die zu erwartenden Schäden b
Schutzbedarf. Dabei ist es unbedingt auch erforderlich, die Applikations-/Proj
lichen und die Benutzer der betrachteten IT-Anwendungen nach ihrer Einschätzun
befragen.

Als Orientierungshilfe für die Einordnung von IT-Anwendungen in Schutzbedarfsk
kann die in Abbildung 3.4 angeführte Tabelle bzw. eine den spezifischen Anfor
Organisation entsprechende modifizierte Tabelle dienen.

Die Ermittlung des Schutzbedarfes erfolgt nach dem Maximum-Prinzip. Sind für a

System laufenden Anwendungen nur niedrige bis mittlere potentielle Schäden erl
so ist das gesamte System in die Schutzbedarfskategorie "niedrig bis mittel"
Realisierung von Grundschutzmaßnahmen bietet hier i.a. einen ausreichenden Sc
dagegen mindestens eine Applikation mit hohem oder sehr hohem Schutzbedarf er
sollte zusätzlich zum IT-Grundschutz eine detaillierte Risikoanalyse durchgefü

Anmerkungen:

* Abhängigkeiten:
  Bei der Betrachtung der möglichen Schäden und ihrer Folgen ist auch zu beach
  Anwendungen Arbeitsergebnisse anderer Applikationen als Input nutzen können.
  Informationen können dabei auch auf anderen IT-Systemen erarbeitet worden se
  sich betrachtet weniger bedeutende IT-Anwendung kann wesentlich an Wert gewi
  wenn eine andere wichtige IT-Anwendung auf ihre Ergebnisse angewiesen ist.
  Fall muss der ermittelte Schutzbedarf auch für die abhängigen IT-Anwendunger
  Informationen sichergestellt werden. Handelt es sich dabei um Applikationen
  IT-Systeme, dann müssen Schutzbedarfsanforderungen des einen Systems auch a
  andere übertragen werden.

* Kumulationseffekte:
  Werden mehrere IT-Anwendungen/Informationen auf einem IT-System verarbeitet,
  überlegen, ob durch Kumulation mehrerer kleinerer Schäden auf einem IT-Syste
  insgesamt höherer Gesamtschaden entstehen kann. In einem solchen Fall erhöht
  Schutzbedarf des IT-Systems entsprechend.

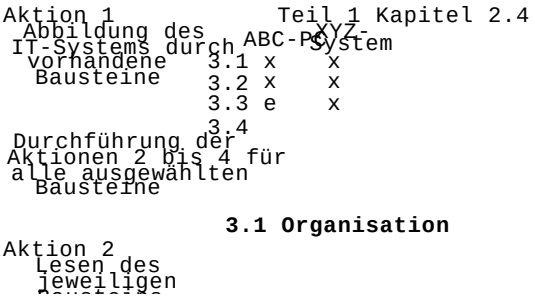
* Verlagerung von Anwendungen mit hohen Risiken:
  Zeigt die Schutzbedarfsfeststellung, dass die meisten Anwendungen auf einem
  niedrigen bis mittleren Schutzbedarf haben und nur eine oder wenige hochschu
  sind, so ist die Möglichkeit einer Auslagerung dieser Anwendungen auf ein is
  oder eine Zusammenfassung diverser hochschutzbedürftiger Anwendungen auf ein
  besonders zu schützenden System zu prüfen.

3.4.3 Durchführung von Grundschutzanalysen

Für alle IT-Systeme der Schutzbedarfskategorie "niedrig bis mittel" ist eine
analyse vorzunehmen. Die Vorgehensweise entspricht dabei der in Kapitel 3.3 b

---

Die folgenden Graphik zeigt die Einbettung des IT-Grundschutzes in die Gesamtv
weise des kombinierten Ansatzes.



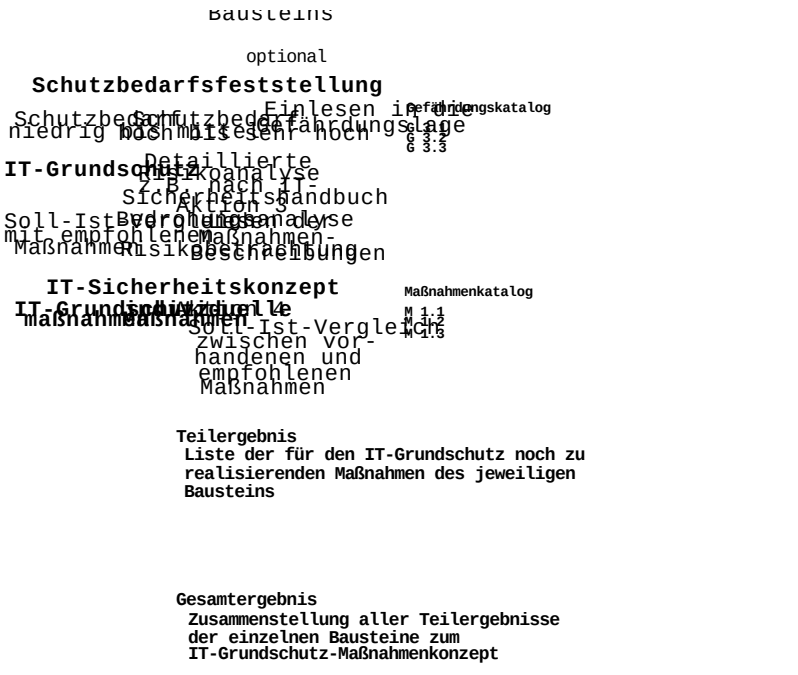
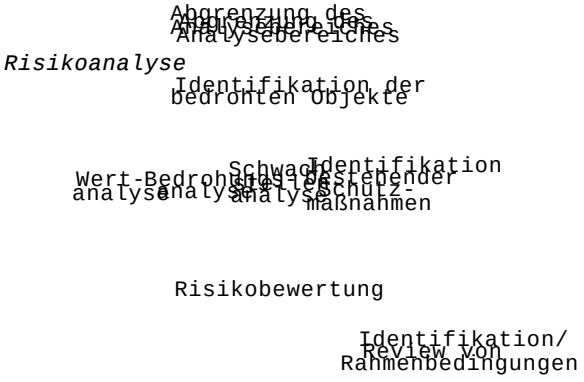


Abbildung 3.5: IT-Grundschutz als Bestandteil des kombinierten Ansatzes (aus [BSI GSHB])

3.4.4 Durchführung von detaillierten Risikoanalysen

Alle IT-Systeme der Schutzbedarfskategorie "hoch bis sehr hoch" sind einer de
Risikoanalyse zu unterziehen.

Die Auswahl einer konkreten Methode zur Risikoanalyse sowie der eventuelle Ei
Tools zur Unterstützung dieser Analyse bleiben der durchführenden Institution
Details dazu finden sich in Kap. 3.2 dieses Handbuches.



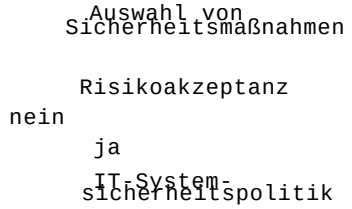


Abbildung 3.6: Einbettung der detaillierten Risikoanalyse in den kombinierten Ansatz

---

3.5 Akzeptables Restrisiko

Sicherheitsmaßnahmen können für gewöhnlich Risiken nur teilweise mindern. Im A
verbleibt ein Restrisiko, dessen Abdeckung wirtschaftlich nicht mehr vertretba
notwendig, diese Restrisiken so exakt wie möglich zu quantifizieren und sie da
akzeptieren. Dieser Prozess wird als "Risikoakzeptanz" bezeichnet.

Um ein ressortweit einheitliches Niveau des Restrisikos zu gewährleisten, ist
diesen Prozess durch generelle Richtlinien zu unterstützen. Diese sollten im R
Sicherheitspolitik definiert werden (vgl. Kap. 2.2.3) und festlegen, welche R
betroffene Organisation i.a. zu akzeptieren bereit ist.

Auch dabei ist zu beachten, dass durch Kumulationseffekte oder gegenseitige Be
eine Reihe von kleinen Einzelrisiken zu einem inakzeptablen Restrisiko führen

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

3.6 Akzeptanz von außergewöhnlichen Restrisiken

Verbleibt nach Durchführung aller vorgesehenen Sicherheitsmaßnahmen ein Restri
höher ist als das generell akzeptable, so sollten zusätzliche Sicherheitsmaßna
und damit das Risiko weiter reduziert werden (vgl. Kap. 4.2).

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

Die Entscheidung über die Akzeptanz eines außergewöhnlichen Restrisikos ist du
Management zu treffen, die genauen Verantwortlichkeiten dafür sind in der IT-S
politik festzulegen. Die Entscheidung ist schriftlich zu begründen und durch
Organisation in schriftlicher Form zu akzeptieren.

4 Erstellung von IT-Sicherheitskonzepten

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

Die Erstellung eines IT-Sicherheitskonzeptes erfolgt in vier Schritten:
Schritt 1: Auswahl von Maßnahmen
Schritt 2: Risikoakzeptanz
Schritt 3: Erstellung von IT-Systemsicherheitspolitiken
Schritt 4: Erstellung eines IT-Sicherheitsplanes

Diese vier Schritte werden in den folgenden Kapiteln näher beschrieben.

4.1 Auswahl von Maßnahmen

Sicherheitsmaßnahmen sind Verfahrensweisen, Prozeduren und Mechanismen, die die Sicherheit eines IT-Systems erhöhen. Dies kann auf unterschiedliche Arten erreicht werden. Sicherheitsmechanismen können
- ü Risiken vermeiden,
- ü Bedrohungen oder Schwachstellen verkleinern,
- ü unerwünschte Ereignisse entdecken,
- ü die Auswirkung eines unerwünschten Ereignisses eingrenzen,
- ü Risiken überwälzen oder
- ü es möglich machen, einen früheren Zustand wiederherzustellen.

4.1.1 Klassifikation von Sicherheitsmaßnahmen

Je nach Betrachtungsweise kann eine Klassifikation von Sicherheitsmaßnahmen h
folgender Kriterien getroffen werden.

4.1.1.1 Klassifikation nach Art der Maßnahmen

Dies ist die "klassische" Einteilung der Sicherheitsmaßnahmen. Man unterscheic

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

Die letzten drei Maßnahmenbündel gemeinsam werden auch als nicht-technische b
operationale Maßnahmen bezeichnet.

4.1.1.2 Klassifikation nach Anwendungsbereichen

Man unterscheidet:

ü Maßnahmen, die organisationsweit (oder in Teilen der Organisation) einzuset
gehören:
  * Etablierung eines IT-Sicherheitsmanagementprozesses und Erstellung von IT-
Sicherheitspolitiken
  * organisatorische Maßnahmen (z.B. Kontrolle von Betriebsmitteln, Dokumenta
Rollentrennung)
  * Überprüfung der IT-Sicherheitsmaßnahmen auf Übereinstimmung mit den IT-
Sicherheitspolitiken (Security Compliance Checking), Auditing
  * Reaktion auf sicherheitsrelevante Ereignisse (Incident Handling)
  * personelle Maßnahmen (incl. Schulung und Bildung von Sicherheitsbewusstse
  * bauliche Sicherheit und Infrastruktur
  * Notfallvorsorge

ü Systemspezifische Maßnahmen.
Die Auswahl systemspezifischer Maßnahmen hängt in hohem Maße vom Typ des zu
schützenden IT-Systems ab. Der Entwurf zu [ISO/IEC 13335-4] unterscheidet e
  * Nicht-vernetzte Systeme (Stand alone PCs)
  * Workstations in einem internen Netzwerk
  * Server in einem internen Netzwerk
  * Workstations, die mit einem externen Netzwerk verbunden sind

* Server, die mit einem externen Netzwerk verbunden sind
* Workstations, die sowohl mit einem internen als auch mit einem externen Netzwerk verbunden sind
* Server, die sowohl mit einem internen als auch einem externen Netzwerk verbunden sin

4.1.1.3 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 unterscl daher:

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

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

4.1.2 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 bes Schutzmaßnahmen" (vgl. Kap. 3.2.6), die als Ergebnis eine Aufstellung aller existierende bereits geplanten Schutzmaßnahmen mit Angaben über ihren Implementierungsstatus und ihre Einsatz liefern soll.
Bei einer Grundschutzanalyse werden die vorhandenen Maßnahmen im Rahmen des Soll-Ist-Vergleiches (vgl. Kap. 3.3.2.4) ermittelt.

* Ergebnisse der Risikobewertung:

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

Diese Auswahl wird von einer Reihe von Faktoren beeinflusst:
ü der Stärke der einzelnen Maßnahmen
ü ihrer Benutzerfreundlichkeit und Transparenz für den Anwender

ü in der Benutzerfreundlichkeit und Transparenz für den Anwender
ü der Art der Schutzfunktion (Verringerung von Bedrohungen, Erkennen von Verletzungen,...)

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

4.1.3 Auswahl von Maßnahmen auf Basis einer detaillierten Risikoanalyse

Wurde eine detaillierte Risikoanalyse durchgeführt, so stehen für die Auswahl Sicherheitsmaßnahmen detailliertere und spezifischere Informationen zur Verfüg einer Grundschutzanalyse. Je genauer und aufwendiger die Risikoanalyse durchg umso qualifizierter ist im Allgemeinen die für den Auswahlprozess zur Verfügur Information.

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

Welche der in Frage kommenden Maßnahmen tatsächlich ausgewählt und implementie werden, hängt von den speziellen Umständen ab. Generell ist festzuhalten, dass maßnahmen einen oder mehrere der folgenden Aspekte abdecken können:
ü Vorbeugung (präventive Maßnahmen)
ü Aufdeckung (detektive Maßnahmen)
ü Abschreckung
ü Schadensbegrenzung
ü Wiederherstellung eines früheren Zustandes
ü Bildung von Sicherheitsbewusstsein
ü Risikoüberwälzung

Welche dieser Eigenschaften notwendig bzw. wünschenswert ist, ist vom spezifis abhängig. Im Allgemeinen wird man Maßnahmen bevorzugen, die mehrere dieser Asp abdecken. Es ist aber auch darauf zu achten, dass die Gesamtheit der ausgewäh Maßnahmen ein ausgewogenes Verhältnis der einzelnen Aspekte aufweist, dass al

---

beispielsweise ausschließlich detektive oder ausschließlich präventive Maßnahr kommen.

4.1.4 Auswahl von Maßnahmen im Falle eines Grundschutzansatzes

Grundsätzlich ist die Auswahl von Sicherheitsmaßnahmen im Falle eines Grundsch relativ einfach. In Maßnahmenkatalogen werden eine Reihe von Schutzmaßnahmen g meisten üblichen Bedrohungen angeführt. Die betreffenden Bedrohungen werden a ohne weitere Risikoanalyse, als relevant für die durchführende Organisation ar empfohlenen Maßnahmen werden mit den existierenden oder bereits geplanten Maßr verglichen. Die noch nicht existierenden bzw. geplanten Maßnahmen werden in ei noch zu realisierenden Maßnahmen zusammengefasst.

In Teil 2 dieses Sicherheitshandbuches werden die wichtigsten Grundschutzmaßna
öffentliche Verwaltung in Österreich aufgeführt. Bis zum Erscheinen dieses Te
empfohlen, auf bereits bestehende Kataloge zurückzugreifen.

Ein sehr umfangreicher Katalog von Grundschutzmaßnahmen, der kontinuierlich we
entwickelt wird, ist im Grundschutzhandbuch des BSI enthalten (vgl. Kap. 3.3
Handbuches). Der Entwurf zu [ISO/IEC 13335-4] gibt eine gut strukturierte und
Anleitung zum Vorgehen bei der Auswahl von Grundschutzmaßnahmen und verweist
auf bereits existierende Grundschutzkataloge.

4.1.5 Auswahl von Maßnahmen im Falle eines kombinierten Risikoanalyseansatze

Im Falle eines kombinierten Ansatzes werden zunächst anhand des zugrundliegend
Grundschutzhandbuches oder -kataloges (etwa [BSI GSHB] oder spezifische Maßnah
kataloge) entsprechende Schutzmaßnahmen ausgewählt und umgesetzt, die einerse
adäquates Sicherheitsniveau für Systeme der Schutzbedarfsklasse "niedrig bis
gewährleisten, andererseits auch für hochschutzbedürftige Systeme bereits ein
an Schutz bieten. Anschließend werden die noch fehlenden Sicherheitsmaßnahmen
Systeme mit hohen bis sehr hohen Sicherheitsanforderungen ausgewählt.

4.1.6 Bewertung von Maßnahmen

Unabhängig von der verfolgten Strategie ist es in jedem Fall notwendig, die A
ausgewählten Maßnahmen zu analysieren. Damit soll gewährleistet werden, dass
lichen Maßnahmen mit dem IT-Gesamtkonzept und den bereits bestehenden Sicherh
nahmen verträglich sind, d.h. dass sie einander ergänzen und unterstützen und
gegenseitig behindern oder in ihrer Wirkung schwächen. In diesem Stadium ist

---

Einbeziehung der betroffenen Benutzer zu empfehlen, da die Wirksamkeit von Si
maßnahmen stark davon abhängt, in welchem Maß sie akzeptiert oder aber abgele
umgangen werden. Die Akzeptanz von Maßnahmen steigt, wenn ihre Notwendigkeit
Benutzer 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 vorhande Sicherheitsmaßnahmen,
- Überprüfung, ob und inwieweit die Maßnahmen zu Behinderungen beim Betrieb d Systems führen können,
- Überprüfung der Vereinbarkeit der Maßnahmen mit geltenden rechtlichen Vorsc Richtlinien und
- Bewertung, in welchem Ausmaß die Maßnahmen eine Reduktion der Risiken bewir

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

4.1.7 Rahmenbedingungen

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

Beispiele für solche Rahmenbedingungen sind:

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

Weitere Einschränkungen können organisatorischer, personeller, gesetzlicher o Natur sein.
Auch Rahmenbedingungen können im Laufe der Zeit, durch soziale Veränderungen Veränderungen im technischen oder organisatorischen Umfeld, einem Wandel unte sind daher regelmäßig zu überprüfen und zu hinterfragen.

4.2 Risikoakzeptanz

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

Schritt 1: Quantifizierung des Restrisikos

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

Schritt 2: Bewertung der Restrisiken

Die verbleibenden Restrisiken sind als "akzeptabel" oder "nicht-akzeptabel" zu Die Entscheidungsgrundlage dafür sollte in der (organisationsweiten) IT-Siche festgelegt sein (vgl. Kap 2.2.3, Schritt 2, sowie Kap. 3.5). Akzeptable Restr 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 Ma
Entscheidung sein. Es besteht die Möglichkeit, zu untersuchen, wie weit und m
Kosten nicht-akzeptable Restrisiken weiter verringert werden können, und zusä
hohen Kosten verbundene Maßnahmen auszuwählen. Die Alternative dazu ist eine
und dokumentierte Akzeptanz des erhöhten Restrisikos.

Schritt 4: Akzeptanz von außergewöhnlichen Restrisiken

Ist eine weitere Reduktion des Restrisikos nicht möglich, unwirtschaftlich od
gegebener Rahmenbedingungen nicht wünschenswert, so besteht in begründeten Au
fällen die Möglichkeit einer bewussten Akzeptanz dieses erhöhten Restrisikos.

---

dabei und die Verantwortlichkeiten dafür sind in der IT-Sicherheitspolitik fe
Kap. 2.2.3, Schritt 3 und Kapitel 3.6).

4.3 IT-Systemsicherheitspolitiken

4.3.1 Aufgaben und Ziele

Eine IT-Systemsicherheitspolitik stellt ein Basisdokument dar, in dem
- die grundlegenden Vorgaben und Leitlinien zur Sicherheit in einem IT-System werden,
- Details über die ausgewählten Sicherheitsmaßnahmen beschrieben sind und
- die Gründe für die Auswahl der Sicherheitsmaßnahmen dargelegt werden.

IT-Systemsicherheitspolitiken sollten für alle komplexen oder stark verbreite
erarbeitet werden. Typische Beispiele sind etwa eine PC-Sicherheitspolitik, e
Netzsicherheitspolitik oder eine Internet-Sicherheitspolitik.
IT-Systemsicherheitspolitiken stellen keine isolierten Einzeldokumente dar, s
einen Kontext von Regelungen einzubetten. Sie leiten sich von der organisatio
Sicherheitspolitik ab, müssen mit dieser kompatibel sein und dürfen keine Wid
dieser aufweisen. Abbildung 4.1 zeigt den Zusammenhang zwischen den einzelnen
Policies in einer Organisation.

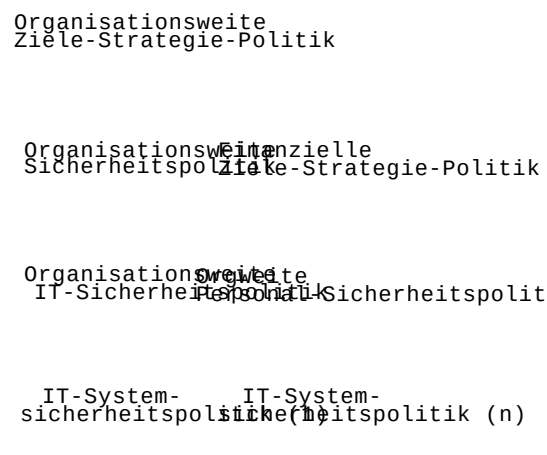


Abbildung 4.1: Einbettung von IT-Sicherheitspolitik und IT-Systemsicherheitspolit in einen Kontext von organisationsweiten Regelungen

4.3.2 Inhalte

Eine IT-Systemsicherheitspolitik sollte Aussagen zu folgenden Bereichen treffe

ü Definition und Abgrenzung des Systems, Beschreibung der wichtigsten Kompone
ü Definition der wichtigsten Ziele und Funktionalitäten des Systems
ü Festlegung der IT-Sicherheitsziele des Systems
ü Abhängigkeit der Organisation vom betrachteten IT-System;
  Dabei ist zu untersuchen, wie weit die Aufgabenerfüllung der Organisation du
  Verletzung der Vertraulichkeit, Verfügbarkeit oder Integrität des Systems od
  verarbeiteter Information gefährdet wird.
ü Investitionen in das System
  (Entwicklungs-, Beschaffungs- und Wartungskosten, Kosten für den laufenden B
ü Risikoanalysestrategie
ü Werte, Bedrohungen und Schwachstellen lt. Risikoanalyse
ü Sicherheitsrisiken
ü Beschreibung der bestehenden und der noch zu realisierenden Sicherheitsmaßna
ü Gründe für die Auswahl der Maßnahmen
ü Kostenschätzungen für die Realisierung und Wartung (Aufrechterhaltung) der
  Sicherheitsmaßnahmen
ü Verantwortlichkeiten

4.3.3 Fortschreibung der IT-Systemsicherheitspolitik

Auch eine IT-Systemsicherheitspolitik stellt kein einmal erstelltes, unveränder
dar, sondern ist regelmäßig auf Aktualität zu überprüfen und bei Bedarf entspr
anzupassen.

Insbesondere ist es von Bedeutung, dass die Liste der existierenden bzw. noch
Sicherheitsmaßnahmen stets dem tatsächlich aktuellen Stand entspricht. Unters
dieser Aufgabe bieten mehrere auf dem Markt befindliche Tools, wie etwa das "I
Grundschutz".

4.3.4 Verantwortlichkeiten

Die Verantwortlichkeiten für die Erstellung und Fortschreibung der IT-Systems
politiken sind im Einzelnen in der IT-Sicherheitspolitik festzulegen (vgl. da
Allgemeinen wird diese Verantwortung beim für das gegenständliche System zustä
Bereichs-IT-Sicherheitsbeauftragten liegen, der sie mit dem Datenschutz-/IT-S

beauftragten abstimmen wird. Letzterer hat dafür Sorge zu tragen, dass die ei
Systemsicherheitspolitiken mit der organisationsweiten IT-Sicherheitspolitik
und auch untereinander ein einheitliches, vergleichbares Niveau aufweisen.

4.4 IT-Sicherheitsplan

Der IT-Sicherheitsplan beschreibt, wie die ausgewählten Sicherheitsmaßnahmen
werden. Er enthält eine Prioritäten- und Ressourcenplanung sowie einen Zeitpl
Umsetzung der Maßnahmen.

Im Detail sind für jedes System zu erstellen:

- ü eine Liste der vorhandenen sowie eine Liste der noch zu implementierenden Sicherheitsmaßnahmen;
  Für jede dieser Maßnahmen sollte eine Aussage über ihre Wirksamkeit sowie m
  weise notwendige Verbesserungen oder Verstärkungen getroffen werden.
- ü eine Prioritätenreihung für die Implementierung der ausgewählten Sicherheit
  bzw. die Verbesserung bestehender Maßnahmen
- ü eine Kosten- und Aufwandsschätzung für Implementierung und Wartung der Sicherheitsmaßnahmen
- ü 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
- ü eine Bewertung des nach der Implementierung aller Maßnahmen zu erwartenden

Weiters sollte der Sicherheitsplan auch die Kontrollmechanismen festlegen, di
der Implementierung der ausgewählten Maßnahmen bewerten, und Möglichkeiten de
Eingriffes bei Abweichungen vom vorgesehenen Prozess oder bei notwendigen Änd
definieren.

4.5 Fortschreibung des IT-Sicherheitskonzeptes

Auch das IT-Sicherheitskonzept muss laufend fortgeschrieben werden. Anlässe fü
Untersuchung und das Fortschreiben des Konzeptes können sein:

ü Ablauf eines vorgeschriebenen oder vereinbarten Zeitraumes (z.B. jährliches
ü Eintritt von Ereignissen, die die Bedrohungslage verändern, wie etwa politis
schaftliche Entwicklungen oder das Bekanntwerden neuer Attacken oder Tätergr
ü Eintritt von Ereignissen, die die Werte verändern können, wie etwa die Ände
Organisationszielen oder Aufgabenbereichen, Änderungen am Markt oder die Ein
neuer Applikationen
ü Ereignisse, die die Eintrittswahrscheinlichkeit von Bedrohungen verändern, w
Entwicklung neuer Techniken oder veränderte Einsatzbedingungen (Einsatzort,
Ausstattung, ...)
ü neue Möglichkeiten für Sicherheitsmaßnahmen, etwa aufgrund von Preisänderung
der Verfügbarkeit neuer Technologien

Voraussetzungen für eine effiziente und zielgerichtete Fortschreibung des IT-
Sicherheitskonzeptes sind (vgl. dazu auch Kap. 6 "IT-Sicherheit im laufenden B
- die laufende Überprüfung von Akzeptanz und Einhaltung der IT-Sicherheitsmaß
- die Protokollierung von Schadensereignissen
- die Kontrolle der Wirksamkeit und Angemessenheit der Maßnahmen

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

---

5 Umsetzung des IT-Sicherheitsplanes

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

Bei der Umsetzung des Planes ist zu beachten, dass

ü Verantwortlichkeiten rechtzeitig und eindeutig festgelegt werden,
ü finanzielle und personelle Ressourcen rechtzeitig zugewiesen werden,
ü die Maßnahmen korrekt umgesetzt werden,
ü die Kosten sich in dem vorher abgeschätzten Rahmen halten und
ü 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 zu erreichen.

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

Es empfiehlt sich, die Umsetzung des IT-Sicherheitsplanes im Rahmen eines Projektes abzuwickeln.

5.1 Implementierung von Maßnahmen

Sobald der IT-Sicherheitsplan erstellt und verabschiedet wurde, sind die einzelnen Maßnah
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 andere
Teil aber organisationsweit einzusetzen ist (vgl. dazu auch Kap. 4.1).

Die Abstimmung der einzelnen systemspezifischen IT-Sicherheitspläne für die Gesamtorganisation obliegt i.a. dem Datenschutz-/IT-Sicherheitsbeauftragten. Er hat dafür Sorge zu tragen, dass
ü die systemübergreifenden, organisationsweiten Maßnahmen
  * vollständig und angemessen,
  * nicht redundant oder widersprüchlich sind, und

ü die systemspezifischen Maßnahmen
  * kompatibel sind und
  * ein einheitliches, angemessenes Sicherheitsniveau haben.

Besonderer Wert ist auf eine detaillierte, korrekte und aktuelle Dokumentatio
mentierungen zu legen.

Schritt 1: Implementierung der Sicherheitsmaßnahmen

Die Implementierung der ausgewählten Sicherheitsmaßnahmen hat anhand des IT-S
planes, 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
wurde.
Es wird empfohlen, für die Tests einen Testplan zu erstellen, der
ü die Testmethoden,

ü die Testumgebung sowie
ü die Zeitpläne für die Durchführung der Tests
beinhaltet.

Die durchgeführten Tests sind im Detail zu beschreiben und die Ergebnisse in d
disierten Testbericht festzuhalten.

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

*Schritt 3: Prüfung der Maßnahmen auf Übereinstimmung mit der IT-Sicherheitspo
(Security Compliance Checking)*

Security Compliance Checks sind sowohl im Rahmen der Implementierung der Maßna
auch als wiederholte Aktivität zur Gewährleistung der IT-Sicherheit im laufend
dazu auch Kap. 6) durchzuführen.

Dabei sind zu prüfen:
ü die vollständige und korrekte Umsetzung der Sicherheitsmaßnahmen
ü der korrekte Einsatz der implementierten Sicherheitsmaßnahmen
ü die Einhaltung der organisatorischen Sicherheitsmaßnahmen im täglichen Betri

---

Dokumentation

Die Dokumentation der implementierten Maßnahmen stellt einen wichtigen Teil de
IT-Sicherheitsdokumentation dar und ist notwendige Voraussetzung für die Konti
Konsistenz des Sicherheitsprozesses. Die wichtigsten Anforderungen an die Dok
ü Aktualität:
Alle Sicherheitsmaßnahmen sind stets auf dem aktuellen Stand der Realisierur
beschreiben.
ü Vollständigkeit
ü Hoher Detaillierungsgrad:
Die Sicherheitsmaßnahmen sind so detailliert zu beschreiben, dass zum einen
stehende Sicherheitslücken erkannt werden können, zum anderen ausreichend In
für einen korrekten und effizienten Einsatz der Maßnahmen zur Verfügung steh
ü Gewährleistung der Vertraulichkeit:
Dokumentation über Sicherheitsmaßnahmen kann unter Umständen sehr vertraulic
Information enthalten und ist daher entsprechend zu schützen. So weit wie mö
bei der Klassifikation und Behandlung solcher Dokumente auf die Vorgaben im
IT-Sicherheitspolitik oder der Informationssicherheitspolitik der Organisati
zurückgegriffen werden (vgl. dazu Kap. 2.2.4). Es kann im Einzelfall notwend
weitere Verfahrensweisen zur Erstellung, Verteilung, Benutzung, Aufbewahrung
Vernichtung von sicherheitsrelevanter Dokumentation zu entwickeln. Diese
Verfahrensweisen sind ebenfalls entsprechend zu dokumentieren.
ü Konfigurations- und Integritätskontrolle:
Es ist sicherzustellen, dass keine unauthorisierten Änderungen der Dokumenta
die eine - beabsichtigte oder unbeabsichtigte - Beeinträchtigung der impleme
Maßnahmen nach sich ziehen könnten.

5.2 Sensibilisierung

5.2 Sensibilisierung

Nur durch Verständnis und Motivation ist eine dauerhafte Einhaltung und Umset
Richtlinien und Vorschriften zur IT-Sicherheit zu erreichen. Um das Sicherhei
aller Mitarbeiter zu fördern und den Stellenwert der IT-Sicherheit innerhalb e
zu betonen, sollte ein umfassendes, organisationsweites Sensibilisierungsprog
werden, das zum Ziel hat, IT-Sicherheit zu einem integrierten Bestandteil der
zu machen.

Das Sensibilisierungsprogramm sollte systemübergreifend sein. Es ist Aufgabe d
verantwortlichen Mitarbeiters - dies wird im Allgemeinen der Datenschutz-/IT-S
beauftragte sein - die Anforderungen aus den einzelnen Teilbereichen und syste
Anforderungen hier einfließen zu lassen und entsprechend zu koordinieren.

Das Sensibilisierungsprogramm sollte folgende Punkte umfassen:

ü Information aller Mitarbeiter über die IT-Sicherheitspolitik der Organisatio
einer Einführung sollten insbesondere folgende Punkte erläutert werden:
* die IT-Sicherheitsziele und -politik der Institution sowie deren Erläuteru
* die Bedeutung der IT-Sicherheit für die Institution,
* Organisation und Verantwortlichkeiten im Bereich der IT-Sicherheit,
* die Risikoanalysestrategie,
* die Sicherheitsklassifikation von Daten,
* ausgewählte Sicherheitsmaßnahmen (insbesondere solche, die für die gesamte
Organisation Gültigkeit haben),
ü die wichtigsten Ergebnisse der Risikoanalysen (Bedrohungen, Schwachstellen,
ü die Pläne zur Implementation und Überprüfung der Sicherheitsmaßnahmen,
ü die Auswirkungen von sicherheitsrelevanten Ereignissen für einzelne Anwende
gesamte Institution,
ü die Notwendigkeit, Sicherheitsverstöße zu melden und zu untersuchen, und
ü die Konsequenzen bei Nichteinhaltung von Sicherheitsvorgaben.

Zur Sensibilisierung der Mitarbeiter können u.a. folgende Maßnahmen beitragen

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

Das Sensibilisierungsprogramm sollte jeden Mitarbeiter der Institution auf se
lichkeit für IT-Sicherheit hinweisen. Dabei ist insbesondere die Verantwortun
Managements für IT-Sicherheit zu betonen ("IT-Sicherheit als Managementaufgabe
organisationsweite Planung dieser Veranstaltungen sollte der Datenschutz-/IT-S
beauftragte übernehmen. Gegebenenfalls liefern Bereichs-IT-Sicherheitsbeauftra
tionen, wann und wo solche Veranstaltungen nötig sind.

Die Veranstaltungen zum Sensibilisierungsprogramm sollten in regelmäßigen Zeit
wiederholt werden, um das vorhandene Wissen aufzufrischen und neue Mitarbeite
informieren. Darüber hinaus sollte jeder neue, beförderte oder versetzte Mita
Fragen der IT-Sicherheit geschult werden, wie es der neue Arbeitsplatz verlan

Das Sensibilisierungsprogramm ist regelmäßig auf seine Wirksamkeit und Aktual

überprüfen und laufend an Veränderungen in der IT-Sicherheitspolitik sowie an
logien anzupassen.

5.3 Schulung

Über das allgemeine Sensibilisierungsprogramm hinaus sind spezielle Schulunge
bereichen der IT-Sicherheit erforderlich, wenn sich durch Sicherheitsmaßnahme
schneidende Veränderungen, z.B. im Arbeitsablauf, ergeben.

Weiters sind Personen, die in besonderem Maße mit IT-Sicherheit zu tun haben,
auszubilden und zu schulen. Dazu zählen etwa:
- ü der Datenschutz-/IT-Sicherheitsbeauftragte und die Bereichs-IT-Sicherheitsbe
- ü die Mitglieder des IT-Sicherheitsmanagement-Teams
- ü Mitarbeiter mit spezieller Verantwortung für die Systementwicklung (z.B. Pro
- ü Mitarbeiter mit spezieller Verantwortung für den Betrieb eines IT-Systems od
  wichtigen Applikation (z.B. Applikationsverantwortliche)
- ü Mitarbeiter, die mit Aufgaben der IT-Sicherheitsverwaltung betraut sind (z.B
  Zutritts-, Zugangs- und Zugriffsrechten)

Das Schulungsprogramm ist von jeder Organistion spezifisch für ihren Bedarf zu
Besondere Betonung ist dabei auf die Schulung der korrekten Implementierung un
Anwendung von Sicherheitsmaßnahmen zu legen. Typische Beispiele für die Themen
Rahmen von Schulungsveranstaltungen behandelt werden sollten, sind:
- ü Sicherheitspolitik und -infrastruktur:
  Rollen und Verantwortlichkeiten,
  Organisation des IT-Sicherheitsmanagements,
  Behandlung von sicherheitsrelevanten Vorfällen,
  regelmäßige Überprüfung von Sicherheitsmaßnahmen,...
- ü Bauliche Sicherheit:
  Schutz von Gebäuden, Serverräumen, Büroräumen und Versorgungseinrichtungen m
  besonderer Betonung der Verantwortung der einzelnen Mitarbeiter (z.B. Handha
  Zutrittskontrollmaßnahmen, Brandschutz,...)
- ü Personelle Sicherheit
- ü Hardware- und Softwaresicherheit:
  Identifikation und Authentisierung, Berechtigungssysteme, Protokollierung,
  Wiederaufbereitung, Virenschutz,...
- ü Netzwerksicherheit:
  Netzwerkinfrastruktur, LANs, Inter-/Intranets, Verschlüsselung, digitale Sig
- ü Disaster Recovery Planung

Schulungs- und Sensibilisierungsveranstaltungen zum Thema IT-Sicherheit müsse
geplant und umgesetzt werden, um keine Sicherheitslücken durch mangelndes Wiss
Sicherheitsbewusstsein entstehen zu lassen.

5.4 Akkreditierung

Unter Akkreditierung eines IT-Systems versteht man die Sicherstellung, dass di
Anforderungen der IT-Systemsicherheitspolitik und des IT-Sicherheitsplanes ge
insbesondere darauf zu achten, dass die Sicherheit des Systems
ü in einer bestimmten Betriebsumgebung,
ü unter bestimmten Einsatzbedingungen und
ü für eine bestimmte vorgegebene Zeitspanne
gewährleistet ist.

Erst nach erfolgter Akkreditierung kann das System - oder eine spezifische An
Echtbetrieb gehen.

Techniken zur Akkreditierung sind:

ü Prüfung der Maßnahmen auf Übereinstimmung mit der IT-Sicherheitspolitik (Sec
  Compliance Checking), vgl. auch Kap. 5.1 und 6.1.2
ü Tests
ü Evaluation und Zertifizierung von Systemen

Änderungen der eingesetzten Sicherheitsmaßnahmen oder der Betriebsumgebung kö
neuerliche Akkreditierung des Systems erforderlich machen. Die Kriterien, wan
akkreditierung durchzuführen ist, sollten in der IT-Systemsicherheitspolitik

6 IT-Sicherheit im laufenden Betrieb

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, Aktualitä und die Umsetzung in der täglichen Praxis überprüft werden. Weiters muss eine angemessene Reaktion auf alle sicherheitsrelevanten Änderungen sowie auf sicherheitsrelevante Ereign gewährleistet sein.

Ziel aller Follow-Up-Aktivitäten ist es, das erreichte Sicherheitsniveau zu erhalten bzw 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.

6.1 Aufrechterhaltung des erreichten Sicherheitsniveaus

Das nach der Umsetzung des IT-Sicherheitsplanes erreichte Sicherheitsniveau lässt sich nu dann aufrechterhalten, wenn

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

Die Verantwortlichkeiten für diese Aktivitäten müssen im Rahmen der organisationsweiten I Sicherheitspolitik bzw. der einzelnen IT-Systemsicherheitspolitiken detailliert festgeleg werden. Als Richtlinie kann wieder gelten, dass die Verantwortung für systemspezifische Maßnahmen bei den einzelnen Bereichs-IT-Sicherheitsbeauftragten - soweit definiert - lieg sollte, die Verantwortung für organisationsweite IT-Sicherheitsmaßnahmen sowie die Gesamt verantwortung beim Datenschutz-/IT-Sicherheitsbeauftragten.

Von besonderer Wichtigkeit für die Aufrechterhaltung oder weitere Erhöhung eines einmal erreichten Sicherheitsniveaus ist eine permanente Sensibilisierung aller betroffenen Mita für Fragen der IT-Sicherheit (vgl. dazu auch Kap. 5.2).

6.1.1 Wartung und administrativer Support von Sicherheitseinrichtungen

Viele Sicherheitsmaßnahmen erfordern zur Gewährleistung ihrer einwandfreien Fu fähigkeit Wartung und administrativen Support. Zu diesen Aufgaben zählen etwa mäßige Auswertung und Archivierung von Protokollen, Backup, Restore und Maint sicherheitsrelevanten Komponenten, die Überprüfung der Parametereinstellungen eventueller Rechte auf mögliche nichtautorisierte Änderungen, die Reinitialis

Startwerten oder Zählern sowie Updates der Sicherheitssoftware, wenn verfügbar
aber nicht ausschließlich, im Bereich Virenschutz) u.v.a.m.

Alle Wartungs- und Supportaktivitäten sollten nach einem detailliert festgeleg
und regelmäßig durchgeführt werden.

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

Die Kosten für Wartungs- und Supportaufgaben können im Einzelfall beträchtlich
sollten daher bereits bei der Auswahl der Sicherheitsmaßnahmen bekannt sein un
Entscheidungsprozess miteinfließen.

Um die Aufrechterhaltung eines einmal erreichten Sicherheitsniveaus zu gewähr
sicherzustellen, dass
- die erforderlichen finanziellen und personellen Ressourcen zur Wartung von
  einrichtungen zur Verfügung stehen,
- organisatorische Regelungen existieren, die die Aufrechterhaltung der IT-Sic
  nahmen im laufenden Betrieb ermöglichen und unterstützen,
- die Verantwortungen im laufenden Betrieb klar zugewiesen werden,
- die Maßnahmen regelmäßig daraufhin geprüft werden, ob sie wie beabsichtigt
  und
- Maßnahmen verstärkt werden, falls sich neue Schwachstellen zeigen.

Alle Wartungs- und Supportaktivitäten im IT-Sicherheitsbereich sollten protok
Der regelmäßigen Auswertung dieser Protokolle kommt besondere Bedeutung für d
IT-Sicherheit zu.

6.1.2 Überprüfung von Maßnahmen auf Übereinstimmung mit der IT-Sicherheitspo (Security Compliance Checking)

Zielsetzung

Zur Gewährleistung eines angemessenen und gleich bleibenden Sicherheitsniveaus
Sorge zu tragen, dass alle Maßnahmen so eingesetzt werden, wie es im IT-Sicher
und im IT-Sicherheitsplan vorgesehen ist. Dies muss für alle IT-Systeme, -Proj
Applikationen sowohl während der Planungsphase, als auch im laufenden Betrieb
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
  (Stichproben!) und
- die organisatorischen Sicherheitsvorgaben im täglichen Betrieb eingehalten
  werden.

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

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

Zeitpunkte

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

ü für neue IT-Systeme oder relevante neue Anwendungen:
  nach der Implementierung (vgl. dazu auch Kap. 5.1 und Kap. 5.4)

ü für bereits in Betrieb befindliche IT-Systeme oder Applikationen:
  * nach einer bestimmten, in der IT-Systemsicherheitspolitik vorzugebenden Ze
    (z.B. jährlich) und
  * bei signifikanten Änderungen.

6.1.3 Fortlaufende Überwachung der IT-Systeme (Monitoring)

Monitoring ist eine laufende Aktivität mit dem Ziel, zu überprüfen, ob das IT-
Benutzer und die Systemumgebung das im IT-Sicherheitsplan festgelegte Sicherhe

---

beibehalten. Dazu wird ein Plan für eine kontinuierliche Überwachung der IT-Sy
täglichen Betrieb erstellt.

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

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

* Wert der zu schützenden Objekte:
  Sowohl die Werte von Objekten als auch, daraus resultierend, die Sicherheits
  an das Gesamtsystem können im Laufe des Lebenszyklus eines IT-Projektes oder
  erheblichen Änderungen unterliegen.
  Mögliche Gründe dafür sind eine Änderung der IT-Sicherheitsziele, neue Appli
  oder die Verarbeitung von Daten einer höheren Sicherheitsklasse auf existier
  Systemen oder Änderungen in der HW-Ausstattung.
* Bedrohungen und Schwachstellen:
  Organisatorisch oder technologisch (hier insbesondere durch neue Technologie
  Außenwelt) bedingt können sowohl die Wahrscheinlichkeit des Eintritts einer
  auch die potentielle Schadenshöhe im Laufe der Zeit starken Änderungen unter
  sind daher regelmäßig zu evaluieren. Neue potentielle Schwachstellen sind so
  möglich zu erkennen und abzusichern.

* Sicherheitsmaßnahmen:
  Die Wirksamkeit der implementierten Sicherheitsmaßnahmen ist laufend zu über
  ist sicherzustellen, dass sie einen angemessenen und den Vorgaben der IT-Sys
  heitspolitik entsprechenden Schutz bieten. Änderungen in den Werten der bedr
  Objekte, den Bedrohungen und den Schwachstellen, aber auch durch den Einsatz
  Technologien, können die Wirksamkeit der Sicherheitsmaßnahmen nachhaltig bee

Durch ein kontinuierliches Monitoring soll die Leitung der Institution ein kla
bekommen, was durch die IT-Sicherheitsmaßnahmen erreicht wurde (Soll-/Ist-Verg
die Ergebnisse den Sicherheitsanforderungen der Institution genügen sowie über
einzelner spezifischer Aktivitäten zur IT-Sicherheit.

Werden im Rahmen des kontinuierlichen Monitoring signifikante Abweichungen des
lichen Risikos von dem im IT-Sicherheitskonzept festgelegten akzeptablen Restr
festgestellt, so sind entsprechende Gegenmaßnahmen zu setzen.

6.2 Change Management

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

Es ist dafür Sorge zu tragen, dass auf alle sicherheitsrelevanten Änderungen a
reagiert wird. Dazu gehören zum Beispiel:
ü Änderungen in der Aufgabenstellung oder in der Wichtigkeit der Aufgabe für d
ü räumliche Änderungen, z.B. nach einem Umzug,
ü Änderungen in der Bewertung der eingesetzten IT, der notwendigen Vertraulich
  Integrität oder Verfügbarkeit und
ü Änderungen bei Bedrohungen oder Schwachstellen.

Alle Änderungen und die dazugehörigen Entscheidungsgrundlagen sind schriftlich
dokumentieren.

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

6.3 Reaktion auf sicher heitsrelevante Ereignisse (Incident Handling)

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

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

Daher sind alle Mitarbeiter über ihre Verantwortung bei Eintreten sicherheitsr

Ereignisse, die vorgesehenen Meldewege und zu setzenden Aktionen zu unterrich

---

Incident Handling Plan

Zur Sicherstellung einer angemessenen Behandlung von sicherheitsrelevanten Er
empfehlenswert, detaillierte Vorgaben in Form eines *Incident Handling Plans* (IHP) auszu-
arbeiten und allen Mitarbeitern bekannt zu machen.

Der IHP legt in schriftlicher Form und verbindlich fest:
ü wie auf sicherheitsrelevante Ereignisse zu reagieren ist,
ü Verantwortlichkeiten für die Meldung bzw. Untersuchung sicherheitsrelevante
ü die einzuhaltenden Meldewege,
ü die Protokollierung und Dokumentation sicherheitsrelevanter Vorfälle sowie
ü 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
ü die Ursachen und Auswirkungen von sicherheitsrelevanten Vorfällen untersucht
ü Vorfälle aufzeichnet und auswertet,
ü Hilfestellung bei der Behandlung von sicherheitsrelevanten Vorfällen gibt.

Ob innerhalb einer Institution ein (oder ev. auch mehrere) CERT(s) eingerichte
erster Linie von der Größe dieser Institution und der erwarteten Anzahl und Sc
Vorfälle ab. In kleineren Institutionen wird eine Behandlung und Aufzeichnung
relevanten Vorfälle durch eine in der IT-Sicherheitspolitik zu benennende Pers
Allgemeinen der Datenschutz-/IT-Sicherheitsbeauftragte sein - angemessen sein,
oder besonders sicherheitssensiblen Institutionen ist die Einrichtung von CER

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

7 Anhang

7.1 Literatur

[BS 7799] "Code of practice for information security management", British Standards Institute, 1995 (entspricht ISO DIS 14980)

[BSI 7105] Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn: "IT-Sicherheitshandbuch", BSI 7105

[BSI GSHB] Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn: "IT-Grundschutzhandbuch", Bundesanzeiger Verlgsges.mbH, ISSN 0947-093X, erscheint jährlich

[DIN 66] DIN Fachbericht 66: "Leitfaden für das IT-Sicherheitsmanagement (GMITS) - Teil 1: Konzepte und Modelle für IT-Sicherheit", Deutsche Übersetzung von ISO/IEC TR 13335-1, Beuth Verlag GmbH, ISBN 3-410-14042-5, ISSN 0179-275X

[ISO/IEC 13335] International Organisation for Standardisation: "Information technology - Security techniques - Guidelines for the management of IT Security", Technical Report, ISO/IEC JTC1 / SC27
Part 1: Concepts and Models for IT Security
Part 2: Managing and Planing IT Security
Part 3: Techniques for the Management of IT Security
Part 4: Selection of Safeguards
Part 5: Safeguards for external Connections

[ISO 13569] International Organisation for Standardisation: "Banking, securities and other financial services - Information security guidelines", Technical Report, 1996

7.2 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 ei eingegrenzten fachlichen Bereich liegen und durch gemeinsame M male ausgezeichnet sind
Auswirkung (impact)	Folgen eines unerwünschten Vorfalls
Authentizität (authenticity)	Eigenschaft, die sicherstellt, dass die von einem Subjekt oder Ressource behauptete Identität zutrifft. Authentizität betriff wie Benutzer, 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
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 G dungslage ausgeht; Ergebnis ist eine Liste von umzusetzenden Standardsicherheitsmaßnahmen
Identifikation (identification)	Bestimmung der Identität eines Subjektes bzw. Objektes

(identification)

Informationssicherheit
(information security) Sammelbegriff aller Aspekte zum Schutz von Information
unbefugter Veränderung und unbefugter Kenntnisnahme;
umfasstumfaßt sowohl elektronisch gespeicherte und verarbeitet
Information als auch Information in verbaler oder schriftliche

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, Verfügbarke Zurechenbarkeit, Authentizität und Zuverlässigkeit in einem IT System

IT-Sicherheitspolitik, organisationsweite (IT security policy, corporate) Leitlinien und Vorgaben, die grundlegende Ziele, Strategien, V wortlichkeiten 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 Schutzwirkun ergeben; die Erstellung eines IT-Sicherheitskonzeptes umfasst Festlegung von Maßnahmen, Restrisikoakzeptanz und Erstellung v IT-Systemsicherheitspolitiken und eines Sicherheitsplanes

IT-System (IT system) Kombination von Hard- und Software mit einem bestimmten Zweck und einer spezifischen Betriebsumgebung

IT-Systemsicherheits-politik (IT system security policy) Leitlinien, Regeln und Praktiken, die vorschreiben, in welcher sensitive Informationen und Betriebsmittel innerhalb eines bes 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 Größen 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 Bedrohu

Schutzbedarf	Maß für die möglichen Schäden, die beim IT-Einsatz entstehen können, und für die Notwendigkeit, den Eintritt solcher Schäde verhindern
Schutzbedarfs-feststellung (high level risk analysis)	Ermittlung des Schutzbedarfes für ein IT-System; im Fall eines kombinierten Risikoanalyse-Ansatzes werden etwa die Schutzbeda kategorien "niedrig bis mittel" und "hoch bis sehr hoch" unter
Schutzmaßnahme (safeguard)	Verfahrensweise oder Mechanismus zur Verringerung von Risiken
Schwachstelle (vulnerability)	Sicherheitsschwäche eines oder mehrerer Objekte, die durch ein Bedrohung ausgenutzt werden kann
Sicherheits-management (security management)	