

VORGEHENSMODELL RISIKOANALYSE

1	RISIKOANALYSE	4
1.1	Risikoanalysestrategien	4
1.1.1	Detaillierte Risikoanalyse	4
1.1.2	Grundschatzansatz	4
1.1.3	Kombinierter Ansatz	4
1.2	Detaillierte Risikoanalyse	5
1.2.1	Abgrenzung des Analysebereiches	6
1.2.2	Identifikation der bedrohten Objekte (Werte, assets)	7
1.2.3	Wertanalyse	7
1.2.3.1	Festlegung der Bewertungsbasis für Sachwerte	8
1.2.3.2	Festlegung der Bewertungsbasis für immaterielle Werte	8
1.2.3.3	Ermittlung der Abhängigkeiten zwischen den Objekten	9
1.2.3.4	Bewertung der bedrohten Objekte	9
1.2.4	Bedrohungsanalyse	9
1.2.4.1	Identifikation möglicher Bedrohungen	10
1.2.4.2	Ermittlung der Eintrittswahrscheinlichkeiten	10
1.2.5	Schwachstellenanalyse	11
1.2.6	Identifikation bestehender Sicherheitsmaßnahmen	12
1.2.7	Risikobewertung	13
1.2.8	Auswertung und Aufbereitung der Ergebnisse	13
1.3	Grundschatzanalyse und Auswahl von Maßnahmen	13
1.3.1	Abbildung des IT-Systems durch vorhandene Bausteine	14
1.3.2	Lesen des jeweiligen Bausteins	14
1.3.3	Lesen der Maßnahmenbeschreibungen	15
1.3.4	Soll-Ist-Vergleich zwischen vorhandenen und empfohlenen Maßnahmen	15
1.4	Kombinierter Ansatz	16
1.4.1	Stärken und Schwächen eines kombinierten Ansatzes:	17
1.4.2	Festlegung von Schutzbedarfskategorien	17
1.4.3	Schutzbedarfsfeststellung	19
1.4.3.1	Erfassung aller vorhandenen oder geplanten IT-Systeme	19
1.4.3.2	Erfassung der IT-Anwendungen und Zuordnung zu den einzelnen IT-Systemen	19
1.4.3.3	Schutzbedarfsfeststellung für jedes IT-System	20
1.4.4	Durchführung von Grundschatzanalysen	21
1.4.5	Durchführung von detaillierten Risikoanalysen	21
1.5	Akzeptables Restrisiko	21
1.6	Akzeptanz von außergewöhnlichen Restrisiken	21
1.7	Literatur	21
1.8	Muster für eine Klassifizierung	22
1.8.1	Zielsetzung	23
1.8.2	Anwendung	23

1.8.3	Dokumentation der Klassifizierung	23
1.8.4	Sicherheitsziel Vertraulichkeit	24
1.8.5	Sicherheitsziel Verfügbarkeit	25
1.8.6	Sicherheitsziel Integrität	26

1 Risikoanalyse

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

1.1 Risikoanalysestrategien

Es ist empfehlenswert, eine Strategie zur Risikoanalyse festzulegen. Diese sollte für das gesamte Unternehmen gültig sein und festlegen, wie die Ziele der Risikoanalyse - Erkennen und Bewerten von Einzelrisiken und Gesamtrisiko - erreicht werden sollen. Die aktuelle Literatur kennt verschiedene Optionen für solch eine Strategie, von denen die wichtigsten drei im Rahmen dieses Dokumentes behandelt werden.

1.1.1 Detaillierte Risikoanalyse

Für alle IT-Systeme wird eine detaillierte Risikoanalyse durchgeführt. Diese Methode führt zu effektiven und angemessenen Sicherheitsmaßnahmen, benötigt jedoch viel Zeit und Aufwand, so dass neben hohen Kosten auch die Gefahr besteht, dass für kritische Systeme nicht schnell genug Schutzmaßnahmen ergriffen werden können.

1.1.2 Grundschutzansatz

Unabhängig vom tatsächlichen Schutzbedarf wird für alle IT-Systeme von einer pauschalisierten Gefährdungslage ausgegangen. Als Sicherheitsmaßnahmen kommen Grundschutzmaßnahmen zum Einsatz. Durch den Verzicht auf eine detaillierte Risikoanalyse spart diese Vorgehensweise Ressourcen und führt schnell zu einem relativ hohen Niveau an Sicherheit. Der Nachteil liegt darin, dass der Grundschutzlevel für das betrachtete IT-System nicht angemessen sein könnte.

1.1.3 Kombiniertes Ansatz

In einem ersten Schritt wird in einer Schutzbedarfsfeststellung (*High Level Risk Analysis*) der Schutzbedarf für die einzelnen IT-Systeme ermittelt. Für IT-Systeme der Schutzbedarfskategorie "niedrig bis hoch" wird auf eine detaillierte Risikoanalyse verzichtet. Dies erlaubt eine schnelle und effektive Auswahl von grundlegenden Sicherheitsmaßnahmen bei gleichzeitiger Gewährleistung eines angemessenen Schutzniveaus. IT-Systeme der Schutzbedarfskategorie „sehr hoch“ sind einer detaillierten Risikoanalyse zu unterziehen, auf deren Basis individuelle Sicherheitsmaßnahmen ausgewählt werden.

Diese Option kombiniert die Vorteile des Grundschutz- und des Risikoanalyseansatzes, da alle IT-Systeme mit hohem Schutzbedarf wirksam und angemessen geschützt werden. Maßnahmen können für die anderen Systeme mit Hilfe des Grundschutzes schnell und effektiv ausgewählt werden. Sie wird in den meisten Einsatzumgebungen die empfehlenswerte Strategie zur Risikoanalyse darstellen.

Bei der Durchführung einer Risikoanalyse sind folgende Prinzipien zu beachten:

Das gesamte Verfahren muss transparent gemacht werden. Es dürfen keine versteckten Annahmen gemacht werden, die z.B. dazu führen, dass Bedrohungen unbetrachtet bleiben. Alle Bewertungen müssen begründet werden, um subjektive Einflüsse zu erkennen und so weit wie möglich zu vermeiden. Alle Schritte müssen so dokumentiert werden, dass sie später auch für andere nachvollziehbar sind. Ein derartiges Vorgehen erleichtert auch eine spätere Überarbeitung des IT-Sicherheitskonzeptes.

Der Aufwand für die Durchführung des Verfahrens sollte dem Wert der IT-Anwendungen und den Werten des Unternehmens im Allgemeinen angemessen sein.

Im Folgenden werden die drei angeführten Risikoanalysestrategien näher erläutert.

1.2 Detaillierte Risikoanalyse

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

Die erstmalige Durchführung einer detaillierten Risikoanalyse und die anschließende Erstellung eines Sicherheitskonzeptes erfordert einen Aufwand, der zumindest im Bereich von Wochen, eventuell auch von Monaten liegt. Zur Reduktion des Aufwandes kann man für IT-Systeme, auf denen Anwendungen mit niedrigem bis hohem Schutzbedarf laufen, auch auf eine detaillierte Risikoanalyse verzichten und Grundschutzmaßnahmen zum Einsatz bringen.

IT-Systeme, auf denen Anwendungen sehr hohem Schutzbedarf installiert sind, erfordern hingegen eine genaue Analyse der bestehenden Werte, Bedrohungen und Schwachstellen 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 und in welchem Maße auch andere Objekte (z.B. Gebäude und Infrastruktur) in die Analyse einbezogen werden sollen.

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

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

Schritt 3: Wertanalyse

In diesem Schritt wird der Wert der bedrohten Objekte ermittelt. Die Wertanalyse umfasst im Einzelnen:

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

Schritt 4: Bedrohungsanalyse

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

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

Schritt 5: Schwachstellenanalyse

Eine Bedrohung kann nur durch die Ausnutzung einer vorhandenen Schwachstelle wirksam werden. Es ist daher erforderlich, mögliche Schwachstellen des Systems in den Bereichen

- Organisation
- Hard- und Software
- Personal und
- Infrastruktur
-

zu identifizieren und ihre Bedeutung zu klassifizieren.

Schritt 6: Identifikation bestehender Sicherheitsmaßnahmen

Zur Vermeidung unnötiger Aufwendungen und Kosten sind die bereits existierenden Sicherheitsmaßnahmen zu erfassen und auf ihre Auswirkungen hinsichtlich der Gesamtsystemsicherheit sowie auf korrekte Funktion zu prüfen. Geplante neue Sicherheitsmaßnahmen müssen mit den existierenden kompatibel sein und eine wirtschaftlich und technisch sinnvolle Ergänzung darstellen.

Schritt 7: Risikobewertung

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

Schritt 8: Auswertung

Eine Auswertung und Aufbereitung des Ergebnisses schließt die Risikoanalyse ab.

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

1.2.1 Abgrenzung des Analysebereiches

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

1.2.2 Identifikation der bedrohten Objekte (Werte, assets)

In diesem Schritt sind alle bedrohten Objekte (assets), die innerhalb des festgestellten Analysebereiches liegen, zu erfassen. Unter den bedrohten Objekten eines Unternehmensbereiches ist alles zu verstehen, was für diese schutzbedürftig ist, also alle Objekte, von denen der Betrieb des IT-Systems und seine Anwendungen und damit die Funktionsfähigkeit der Organisation abhängen. Dazu zählen etwa:

- physische Objekte:
(Gebäude, Infrastruktur, Hardware, Datenträger, Paperware,...)
- logische Objekte:
(Software, Daten, Information,...)
- Personen
Fähigkeiten: (Herstellen eines Produktes, Erbringen einer Dienstleistung,...)
- immaterielle Güter:
(Image, Vertrauen in das Unternehmen, gute Beziehungen zu anderen Organisationen,...)

Zwischen den bedrohten Objekten bestehen grundsätzlich komplexe Abhängigkeiten; die Vertraulichkeit, Integrität oder Verfügbarkeit eines Objektes setzt vielfach die Vertraulichkeit, Integrität oder Verfügbarkeit eines anderen Objektes voraus.

Beispiele dafür sind etwa

- die Erfordernis einer funktionsfähigen Infrastruktur (Stromversorgung, Klimaanlage,...) für den Betrieb eines IT-Systems,
- die Abhängigkeit der Software von unversehrter und verfügbarer Hardware oder
- die Voraussetzung korrekter Applikations- und Betriebssystemsoftware für die Integrität der Anwendungsdaten.

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

1.2.3 Wertanalyse

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

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

1.2.3.1 Festlegung der Bewertungsbasis für Sachwerte

Zunächst ist zu entscheiden, ob die Bewertung quantitativ oder qualitativ erfolgen soll. Eine quantitative Bewertung kann etwa beruhen auf

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

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

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

1.2.3.2 Festlegung der Bewertungsbasis für immaterielle Werte

Auch für immaterielle Werte, wie etwa Bewahrung des guten Rufes oder Gewährleistung der Vertraulichkeit, kann eine quantitative oder eine qualitative Bewertungsbasis festgelegt werden. Eine quantitative Bewertung kann in diesem Fall beruhen auf dem Wert, den das Objekt für einen potentiellen Angreifer hätte (z.B. vertrauliche Information), oder dem Schaden, der sich aus einem Angriff auf das zu schützende Objekt für die betroffene Organisation ergibt. Eine qualitative Bewertung erfolgt wiederum durch Zuordnung diskreter Werte und damit einer Einteilung in Klassen. Beispiele hierfür sind etwa:

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

1.2.3.3 Ermittlung der Abhängigkeiten zwischen den Objekten

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

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

1.2.3.4 Bewertung der bedrohten Objekte

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

Die Bewertung sollte durch die Applikations-/Projektverantwortlichen sowie die betroffenen Benutzer vorgenommen werden.

Unterstützung in der Bewertung kann von verschiedenen Abteilungen, etwa Finanzen, Einkauf, EDV,... kommen.

Es ist Aufgabe desjenigen, der die Risikoanalyse durchführt, die einzelnen Bewertungen auf Plausibilität und Konsistenz zu prüfen und ein konsolidiertes Ergebnis zu erarbeiten.

Ergebnis der Wertanalyse:

Aufstellung der bedrohten Objekte und ihres Wertes für die Organisation.

1.2.4 Bedrohungsanalyse

Eine Bedrohung ist ein "möglicher Anlass für ein unerwünschtes Ereignis, das zu einem Schaden für das System oder das Unternehmen führen kann".

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

Bedrohungen sind charakterisiert durch:

- Ihren Ursprung:
Bedrohungen durch die Umwelt oder durch den Menschen, wobei letztere wieder in absichtliche oder zufällige Bedrohungen zu unterteilen sind; im Falle absichtlicher Bedrohungen ist ferner zwischen Innentätern und Außentätern zu unterscheiden
- die Motivation:
etwa finanzieller Gewinn, Wettbewerbsvorteil, Rache, Geltungssucht, Publicity...
- die Häufigkeit des Auftretens
die Größe des Schadens, der durch diese Bedrohung verursacht werden kann

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

Die Bedrohungsanalyse umfasst im Einzelnen:

- Die Identifikation möglicher Bedrohungen
- Die Ermittlung der Eintrittswahrscheinlichkeiten

1.2.4.1 Identifikation möglicher Bedrohungen

Bedrohungen können unterteilt werden in:

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

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

Bei der Identifikation von möglichen Bedrohungen können Bedrohungskataloge hilfreich sein, die den Charakter von Checklisten haben. Solche Kataloge finden sich etwa im IT-Sicherheitshandbuch oder in der [ISO/IEC 13335-3], Anhang C. Es ist jedoch zu betonen, dass keine derartige Liste vollständig sein kann, und darüber hinaus auch Bedrohungen einem ständigen Wandel und einer ständigen Weiterentwicklung unterworfen sind. Es ist daher immer notwendig, über Bedrohungskataloge hinaus auch die Möglichkeit weiterer Bedrohungen in Betracht zu ziehen.

In diesem Schritt ist auch zu überlegen, von wem eine Bedrohung jeweils ausgehen kann (etwa Mitarbeiter, Leasingpersonal, Externe). Der Schutz gegen Innentäter ist mit technischen Maßnahmen oft nur unzureichend oder mit sehr hohem Aufwand zu bewerkstelligen, hier wird in verstärktem Maß auf personelle und organisatorische Maßnahmen zurückzugreifen sein.

1.2.4.2 Ermittlung der Eintrittswahrscheinlichkeiten

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

- der Häufigkeit der Bedrohung (Wahrscheinlichkeit des Auftretens anhand von Erfahrungen, Statistiken,...),

- der Motivation und den vorausgesetzten Fähigkeiten und Ressourcen eines potentiellen Angreifers,
- Einschätzung der Attraktivität und Verwundbarkeit des IT-Systems bzw. seiner Komponenten,
- Umweltfaktoren und organisationspezifischen Einflüssen.

Auch die Eintrittswahrscheinlichkeit kann quantitativ oder qualitativ bewertet werden. Da eine quantitative Bewertung in vielen Fällen eine Genauigkeit vortäuschen könnte, die durch die ungenaue Methode der Schätzung nicht zu rechtfertigen ist, ist in den letzten Jahren ein Trend in Richtung 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 Anwendungsbereich zu konkretisieren. Im Allgemeinen werden sie in "Anzahl pro Zeiteinheit" angegeben. Sie sollten so festgelegt werden, dass die Bedeutung der Ziffern von 0 bis 4 gleichmäßig zunimmt.

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 Anwendungsbereiche unterschiedliche Auslegungen der Werteskala zu definieren.

Ergebnis der Bedrohungsanalyse:

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

1.2.5 Schwachstellenanalyse

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 Organisation und Verwaltung sowie beim Personal auftreten.

Typische Beispiele für Schwachstellen sind etwa:

- Mangelnder baulicher Schutz von Räumen mit IT-Einrichtungen (Bereich Gebäude)
- Nachlässige Handhabung von Zutrittskontrollen (Bereich Gebäude)
- Spannungs- oder Temperaturschwankungen (Bereich Hardware)
- kompromittierende Abstrahlung (Bereich Hardware)

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

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

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

Beispielhafte Auflistungen von Schwachstellen, die auf typische Problembereiche hinweisen, finden sich etwa in [ISO/IEC 13335-3], Anhang D sowie im IT-Sicherheitshandbuch und im Grundschutzhandbuch.

Ergebnis der Schwachstellenanalyse:

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

1.2.6 Identifikation bestehender Sicherheitsmaßnahmen

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

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

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

Da die Sicherheitsmaßnahmen, die aufgrund einer Risikoanalyse ausgewählt werden, im allgemeinen zusätzlich zu bereits bestehenden Maßnahmen eingeführt werden sollen, ist es notwendig, alle bereits existierenden oder geplanten Sicherheitsmaßnahmen zu identifizieren und ihre Auswirkungen zu überprüfen, um unnötigen Aufwand zu vermeiden. Stellt sich heraus, dass eine bereits existierende oder geplante Maßnahme ihren Anforderungen nicht gerecht wird, so ist zu prüfen, ob sie ersatzlos entfernt, durch andere Maßnahmen ersetzt oder aus Kostengründen belassen werden soll.

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

Ergebnis:

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

1.2.7 Risikobewertung

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

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

Risiken sind eine Funktion folgender Parameter:

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

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

Im IT-Sicherheitshandbuch des BSI wird eine quantitative Bewertung des Risikos anhand von Wertepaaren (Schadensausmaß, Eintrittswahrscheinlichkeit) und anschließend eine Einteilung der Risiken in "tragbare" und "untragbare" vorgenommen

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

Ergebnis:

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

1.2.8 Auswertung und Aufbereitung der Ergebnisse

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

1.3 Grundschutzanalyse und Auswahl von Maßnahmen

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

Die im Folgenden beschriebene Vorgehensweise ist dem IT-Grundschutzhandbuch des BSI [BSI GSHB] entnommen und baut auch auf den dort vorgesehenen sehr umfangreichen Maßnahmenkatalogen auf.

Bei Bedarf können einer Grundschutzanalyse -ergänzend oder alternativ - auch andere Maßnahmenkataloge zugrunde gelegt werden.

Vorgehensweise (lt. [BSI GSHB]):

- Abbildung des IT-Systems durch vorhandene Bausteine
- Lesen des jeweiligen Bausteins
- Lesen der Maßnahmenbeschreibungen
- Soll-Ist-Vergleich zwischen vorhandenen und empfohlenen Maßnahmen

1.3.1 Abbildung des IT-Systems durch vorhandene Bausteine

Unter Rückgriff auf das IT-Grundschutzhandbuch des BSI, das nach einem "Baukastensystem" aufgebaut ist, wird auf die dort bestehenden Kataloge (siehe auch Kap. 4.1.4 dieses Handbuches) verwiesen. Die einzelnen "Bausteine", also die entsprechenden Kapitel und Unterkapitel des Handbuches, mit denen ein reales IT-System nachgebildet werden kann, sind in drei Gruppen zusammengefasst

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

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

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

1.3.2 Lesen des jeweiligen Bausteins

Nun werden die in ausgewählten Kapitel (= Bausteine) bearbeitet. Jedes dieser Kapitel ist gleichermaßen aufgebaut: nach einer einführenden Beschreibung folgt eine Aufzählung

pauschal für den IT-Grundschutz angenommener Gefährdungen und die Empfehlung der hiergegen wirkenden Maßnahmen.

Es werden 5 Gruppen von Gefährdungen unterschieden:

- Höhere Gewalt
- Organisatorische Mängel
- Menschliche Fehlhandlungen
- Technisches Versagen
- Vorsätzliche Handlungen

Die Maßnahmen sind in 6 Bereiche gegliedert:

- Infrastruktur
- Organisation
- Personal
- Hardware/Software
- Kommunikation
- Notfallvorsorge

Eine ausführliche Beschreibung der Maßnahmen und Gefährdungen ist auch in den Katalogen des IT-Grundschutzhandbuches enthalten.

1.3.3 Lesen der Maßnahmenbeschreibungen

Bei der Bearbeitung eines Kapitels ist es unbedingt erforderlich, die empfohlenen Maßnahmen **und** die dazu existierenden Maßnahmenbeschreibungen in den Katalogen sorgfältig zu lesen. Nur so kann der angestrebte Soll-Ist-Vergleich erfolgreich durchgeführt werden.

Neben der eigentlichen Empfehlung, wie die einzelnen Maßnahmen umzusetzen sind, werden beispielhaft Verantwortliche genannt, die die Initiierung bzw. die Umsetzung der Maßnahmen typischerweise bewerkstelligen sollen. Weiterhin werden ergänzende Kontrollfragen angeführt, die zur Beurteilung der umgesetzten Maßnahmen und für Revisionszwecke hilfreich sein können.

1.3.4 Soll-Ist-Vergleich zwischen vorhandenen und empfohlenen Maßnahmen

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

Vorgehen bei Abweichungen:

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

Ergebnis:

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

1.4 Kombiniertes Ansatz

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

Dabei wird zunächst ermittelt, welche IT-Systeme

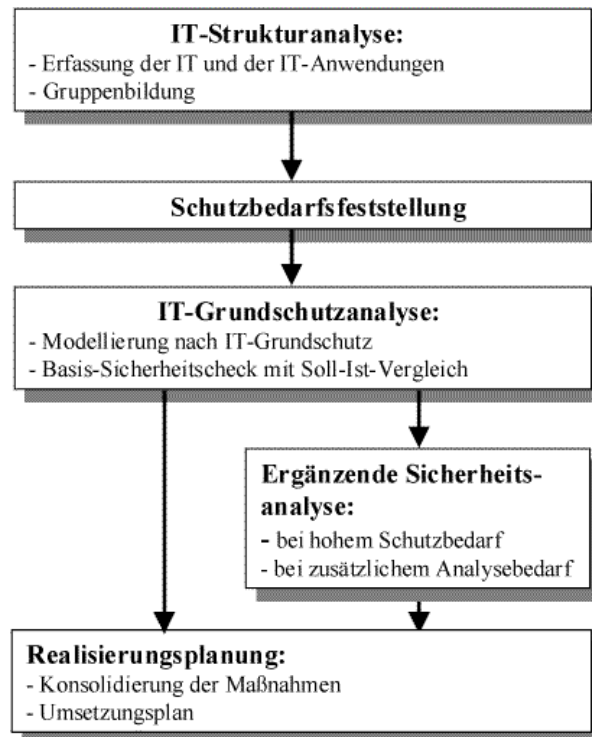
- welche niedrige bis hohe Sicherheitsanforderungen,
- und welche sehr hohe Sicherheitsanforderungen haben.

Das Ergebnis dieses Schrittes ist eine Einteilung in zwei Schutzbedarfskategorien:

- "niedrig bis hoch" und
- „sehr hoch“.

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

Die nachfolgende Abbildung verdeutlicht den Zusammenhang zwischen beiden Vorgehensweisen.



1.4.1 Stärken und Schwächen eines kombinierten Ansatzes:

Die Vorgehensweise ermöglicht es, rasch einen relativ guten Sicherheitslevel für alle IT-Systeme zu realisieren.

Die in der Schutzbedarfsfeststellung erarbeiteten Erkenntnisse können die Grundlage für eine Prioritätenreihung für die nachfolgenden Aktivitäten bilden.

Der Aufwand kann auf hochsicherheitsbedürftige Systeme konzentriert werden.

Das Verfahren findet im Allgemeinen hohe Akzeptanz, da es mit verhältnismäßig geringem Initialaufwand rasch sichtbare Erfolge bringt.

Grundsätzlich besteht beim kombinierten Ansatz das Risiko, dass ein hochschutzbedürftiges IT-System fälschlicherweise in die Schutzbedarfskategorie "niedrig bis hoch" eingeordnet wird. Da solche Systeme aber auf jeden Fall durch Grundschutzmaßnahmen geschützt werden, besteht zumindest ein gewisses Sicherheitsniveau. Außerdem ist zu erwarten, dass im Rahmen einer Grundschutzanalyse eventuell bestehende höhere Sicherheitsanforderungen erkannt werden und damit in einem nächsten Schritt behandelt werden können.

1.4.2 Festlegung von Schutzbedarfskategorien

Voraussetzung für eine Schutzbedarfsfeststellung ist die Festlegung von Schutzbedarfskategorien.

Schutzbedarfskategorien	
"niedrig bis mittel"	Die Schadensauswirkungen sind begrenzt und überschaubar.
"hoch"	Die Schadensauswirkungen können beträchtlich sein.
"sehr hoch"	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Orientierungshilfe:

Die nachfolgende Tabelle gibt eine Orientierungshilfe für die Festlegung der Schutzbedarfskategorien und damit die Klassifizierung der Anwendungen anhand der maximal möglichen Schäden anhand von beispielhaften Grenzwerten. Jede Organisation sollte für sich prüfen, ob diese Klassifikation ihren Anforderungen entspricht und gegebenenfalls eigene Grenzwerte und Einordnungen festlegen.

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

Schutzbedarfskategorie "niedrig bis mittel"	
1. Verstoß gegen Gesetze/Vorschriften/Verträge	- Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen - Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	- Eine Beeinträchtigung des informationellen Selbstbestimmungsrechts würde durch den Einzelnen als tolerabel eingeschätzt werden. - Ein möglicher Missbrauch personenbezogener Daten hat nur geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.
3. Beeinträchtigung der persönlichen Unversehrtheit	- Eine Beeinträchtigung erscheint nicht möglich.
4. Beeinträchtigung der Aufgabenerfüllung	- Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. - Die maximal tolerierbare Ausfallzeit ist größer als 24 Stunden.
5. Negative Außenwirkung	- Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
6. Finanzielle Auswirkungen	- Der finanzielle Schaden ist tolerabel.

Schutzbedarfskategorie "hoch"	
1. Verstoß gegen Gesetze/Vorschriften/Verträge	- Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen - Vertragsverletzungen mit hohen Konventionalstrafen
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	- Eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich. - Ein möglicher Missbrauch personenbezogener Daten hat erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.
3. Beeinträchtigung der persönlichen Unversehrtheit	- Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.
4. Beeinträchtigung der Aufgabenerfüllung	- Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. - Die maximal tolerierbare Ausfallzeit liegt zwischen einer und 24 Stunden.
5. Negative Außenwirkung	- Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
6. Finanzielle Auswirkungen	- Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.

Schutzbedarfskategorie "sehr hoch"	
1. Verstoß gegen Gesetze/Vorschriften/Verträge	- Fundamentaler Verstoß gegen Vorschriften und Gesetze - Vertragsverletzungen, deren Haftungsschäden ruinös sind
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	- Eine besonders bedeutende Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich. - Ein möglicher Missbrauch personenbezogener Daten würde für den Betroffenen den gesellschaftlichen oder wirtschaftlichen Ruin bedeuten.
3. Beeinträchtigung der persönlichen Unversehrtheit	- Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. - Gefahr für Leib und Leben
4. Beeinträchtigung der Aufgabenerfüllung	- Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. - Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde.
5. Negative Außenwirkung	- Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, evtl. sogar existenzgefährdender Art, ist denkbar.
6. Finanzielle Auswirkungen	- Der finanzielle Schaden ist für die Institution existenzbedrohend.

1.4.3 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

1.4.3.1 Erfassung aller vorhandenen oder geplanten IT-Systeme

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

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

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

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

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

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

1.4.3.3 Schutzbedarfsfeststellung für jedes IT-System

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

Als Orientierungshilfe für die Einordnung von IT-Anwendungen in Schutzbedarfskategorien kann die in Abbildung 3.4 angeführte Tabelle bzw. eine den spezifischen Anforderungen einer Organisation entsprechende modifizierte Tabelle dienen. Die Ermittlung des Schutzbedarfes erfolgt nach dem Maximum-Prinzip. Sind für alle auf einem System laufenden Anwendungen nur niedrige bis mittlere potentielle Schäden erhoben worden, so ist das gesamte System in die Schutzbedarfskategorie "niedrig bis hoch" einzuordnen. Die Realisierung von Grundschutzmaßnahmen bietet hier im Allgemeinen einen ausreichenden Schutz. Wurde dagegen mindestens eine Applikation mit sehr hohem Schutzbedarf ermittelt, so sollte zusätzlich zum IT-Grundschutz eine detaillierte Risikoanalyse durchgeführt werden.

Anmerkungen:

Abhängigkeiten:

Bei der Betrachtung der möglichen Schäden und ihrer Folgen ist auch zu beachten, dass IT-Anwendungen Arbeitsergebnisse anderer Applikationen als Input nutzen können. Diese Informationen können dabei auch auf anderen IT-Systemen erarbeitet worden sein. Eine für sich betrachtet weniger bedeutende IT-Anwendung kann wesentlich an Wert gewinnen, wenn eine andere wichtige IT-Anwendung auf ihre Ergebnisse angewiesen ist. In diesem Fall muss der ermittelte Schutzbedarf auch für die abhängigen IT-Anwendungen und Informationen sichergestellt werden. Handelt es sich dabei um Applikationen verschiedener IT-Systeme, dann müssen Schutzbedarfsanforderungen des einen Systems auch auf das andere übertragen werden.

Kumulationseffekte:

Werden mehrere IT-Anwendungen/Informationen auf einem IT-System verarbeitet, so ist zu überlegen, ob durch Kumulation mehrerer kleinerer Schäden auf einem IT-System ein insgesamt höherer Gesamtschaden entstehen kann. In einem solchen Fall erhöht sich der Schutzbedarf des IT-Systems entsprechend.

Verlagerung von Anwendungen mit hohen Risiken:

Zeigt die Schutzbedarfsfeststellung, dass die meisten Anwendungen auf einem System nur niedrigen bis hohen Schutzbedarf haben und nur eine oder wenige hochschutzbedürftig sind, so ist die Möglichkeit einer Auslagerung dieser Anwendungen auf ein isoliertes System oder eine

Zusammenfassung diverser hochschutzbedürftiger Anwendungen auf einem dann besonders zu schützenden System zu prüfen.

1.4.4 Durchführung von Grundschutzanalysen

Für alle IT-Systeme der Schutzbedarfskategorie "niedrig bis hoch" ist eine Grundschutzanalyse vorzunehmen.

1.4.5 Durchführung von detaillierten Risikoanalysen

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

Die Auswahl einer konkreten Methode zur Risikoanalyse sowie der eventuelle Einsatz eines Tools zur Unterstützung dieser Analyse bleiben der durchführenden Institution überlassen. Details dazu finden sich in der Methode eines dieses Dokumentes beschrieben.

1.5 Akzeptables Restrisiko

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

Um ein ressortweit einheitliches Niveau des Restrisikos zu gewährleisten, ist es hilfreich, diesen Prozess durch generelle Richtlinien zu unterstützen. Diese sollten im Rahmen der IT-Sicherheitspolitik definiert werden und festlegen, welche Risiken die betroffene Organisation im allgemeinen zu akzeptieren bereit ist.

Auch dabei ist zu beachten, dass durch Kumulationseffekte oder gegenseitige Beeinflussungen eine Reihe von kleinen Einzelrisiken zu einem inakzeptablen Restrisiko führen kann. Die Entscheidung über die Akzeptanz von Restrisiken ist daher immer eine für das spezielle System zu treffende Managemententscheidung.

1.6 Akzeptanz von außergewöhnlichen Restrisiken

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

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

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

1.7 Literatur

Grundschutzhandbuch des BSI
IT-Sicherheitshandbuch des BSI
ISO/IEC Norm 13335

1.8 *Muster für eine Klassifizierung*

Klassifizierung von Anwendungen IT-Systemen oder IT-Systemgruppen

1.8.1 Zielsetzung

Damit überhaupt ein Schutz- und Verfügbarkeitsbedarf von Anwendungen, IT-Systemen oder IT-Systemgruppen festgelegt werden kann, muss in einem ersten Schritt ermittelt werden wie wichtig die einzelnen Komponenten für das Unternehmen und die Abläufe im Unternehmen sind.

Während ein Produktionssteuerungssystem immer zur Verfügung stehen muss, kann z.B. auf die Möglichkeit der Arbeit mit dem Lohn- und Gehaltsabrechnungssystem zu bestimmten Zeiten durchaus verzichtet werden.

1.8.2 Anwendung

Bezeichnung der Anwendung, des IT-Systems oder der IT-Systemgruppe	
Abteilung / Bereich	
Die Klassifizierung wurde durchgeführt von	
Datum der Klassifizierung	
Die Anwendung wurde folgendermaßen eingestuft:	

1.8.3 Dokumentation der Klassifizierung

Sicherheitsziel	Klasse I (Die Folgen eines Schadensereignisses wären zu verkraften)	Klasse II (Ein Schadensereignis hätte ernsthafte Folgen)	Klasse III (Ein Schadensereignis hätte schwerwiegende oder existenzbedrohende Folgen)
Vertraulichkeit			
Verfügbarkeit			
Integrität			

1.8.4 Sicherheitsziel Vertraulichkeit

1. Werden mit dieser Anwendung, dem IT-Gerät oder der IT-Gerätegruppe personenbezogene Daten verarbeitet?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
2. Werden mit dieser Anwendung, dem IT-Gerät oder der IT-Gerätegruppe finanzwirksame Daten verarbeitet?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
3. Muss die Vertraulichkeit aufgrund von gesetzlichen Anforderungen gewährleistet werden?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
4. Besteht bei dieser Anwendung eine vertragliche Verpflichtung, die Vertraulichkeit zu wahren?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
5. Enthält diese Anwendung, das IT-Gerät oder der IT-Gerätegruppe Detailinformationen über Produktionsprozesse?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
6. Enthält die Anwendung Informationen über Einkaufskonditionen, Lieferbedingungen oder Zahlungskonditionen?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
7. Enthält die Anwendung Informationen über die Qualität von Lieferanten oder Kunden?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
8. Könnte ein Informationsabfluss zu einer Verschlechterung der Wettbewerbsposition führen?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
9. Enthält diese Anwendung Informationen über Löhne und Gehälter von Mitarbeitern?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
10. Enthält diese Anwendung Informationen über Zeugnisse und Beurteilungen von Mitarbeitern?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein

Wie würden Sie aufgrund der Antworten die unmittelbaren und mittelbaren Folgen eines Vertraulichkeitsverlustes bei dieser Anwendung, des IT-Systems oder der IT-Systemgruppe beurteilen?

- Ein Vertraulichkeitsverlust wäre zu verkraften (*Klasse I*)
- Ein Vertraulichkeitsverlust hätte ernsthafte Folgen (*Klasse II*)
- Ein Vertraulichkeitsverlust hätte schwerwiegende oder existenzbedrohende Folgen (*Klasse III*)

1.8.5 Sicherheitsziel Verfügbarkeit

1. Wie groß ist die Zeit des maximalen Verfügbarkeitsverlustes in Stunden?	
2. Könnte ein Verfügbarkeitsverlust zu einer Verschlechterung des Geschäftsergebnisses führen?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
3. Hätte ein Verfügbarkeitsverlust zur Folge, dass vertragliche Verpflichtungen nicht mehr eingehalten werden könnten?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
4. Würde bei einem Verfügbarkeitsverlust die eigene Abteilung bei ihrer Aufgabenerfüllung behindert?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
5. Würden bei einem Verfügbarkeitsverlust andere Abteilungen bei ihrer Aufgabenerfüllung behindert?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
6. Existieren für diese Anwendung spezielle, über das normale gesetzliche Maß hinausgehende, Aufbewahrungsfristen?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
7. Dienen Informationen aus dieser Anwendung der Erfüllung von Meldepflichten?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
8. Könnte ein Verfügbarkeitsverlust den Erhalt oder die Durchführung von Aufträgen gefährden?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
9. Unterliegt die Anwendung einer regelmäßigen kontrollierten Datensicherung?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
10. Würde ein Verfügbarkeitsverlust dazu führen, dass unternehmensrelevante Daten nicht mehr rekonstruierbar wären?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein

Wie würden Sie aufgrund der antworten die unmittelbaren und mittelbaren Folgen eines Verfügbarkeitsverlustes bei dieser Anwendung beurteilen?

- Ein Verfügbarkeitsverlust wäre zu verkräften (*Klasse I*)
- Ein Verfügbarkeitsverlust hätte ernsthafte Folgen (*Klasse II*)
- Ein Verfügbarkeitsverlust hätte schwerwiegende oder existenzbedrohende Folgen (*Klasse III*)

1.8.6 Sicherheitsziel Integrität

1. Ist für die Anwendung, das IT-Gerät oder die IT-Gerätegruppe ein wirkungsvolles Controlling vorhanden?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
2. Enthält diese Anwendung, das IT-Gerät oder die IT-Gerätegruppe finanzwirksame Daten?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
3. Werden mit dieser Anwendung, dem IT-Gerät oder der IT-Gerätegruppe Zahlungsvorgänge ausgelöst?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
4. Wäre bei einer Manipulation die Integrität anderer Anwendungen gefährdet?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
5. Ist bei einer Manipulation der Betrieb des Systems gefährdet?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
6. Findet ein Datenträger- oder Dateiaustausch mit anderen Stellen statt?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
7. Könnte eine Manipulation dazu führen, dass falsche unternehmerische Entscheidungen getroffen werden?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
8. Hätte eine Manipulation Auswirkungen auf das Geschäftsergebnis?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
9. Hätte eine Manipulation Auswirkungen auf das Lagerhaltungssystem?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
10. Könnte eine Manipulation Auswirkungen auf den Produktionsprozess oder die Auftragsbearbeitung haben?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein

Wie würden Sie aufgrund der antworten die unmittelbaren und mittelbaren Folgen einer Manipulation bei dieser Anwendung, des IT-Gerätes oder der IT-Gerätegruppe beurteilen?

- Ein Integritätsverlust wäre zu verkraften (*Klasse I*)
- Ein Integritätsverlust hätte ernsthafte Folgen (*Klasse II*)
- Ein Integritätsverlust hätte schwerwiegende oder existenzbedrohende Folgen (*Klasse III*)