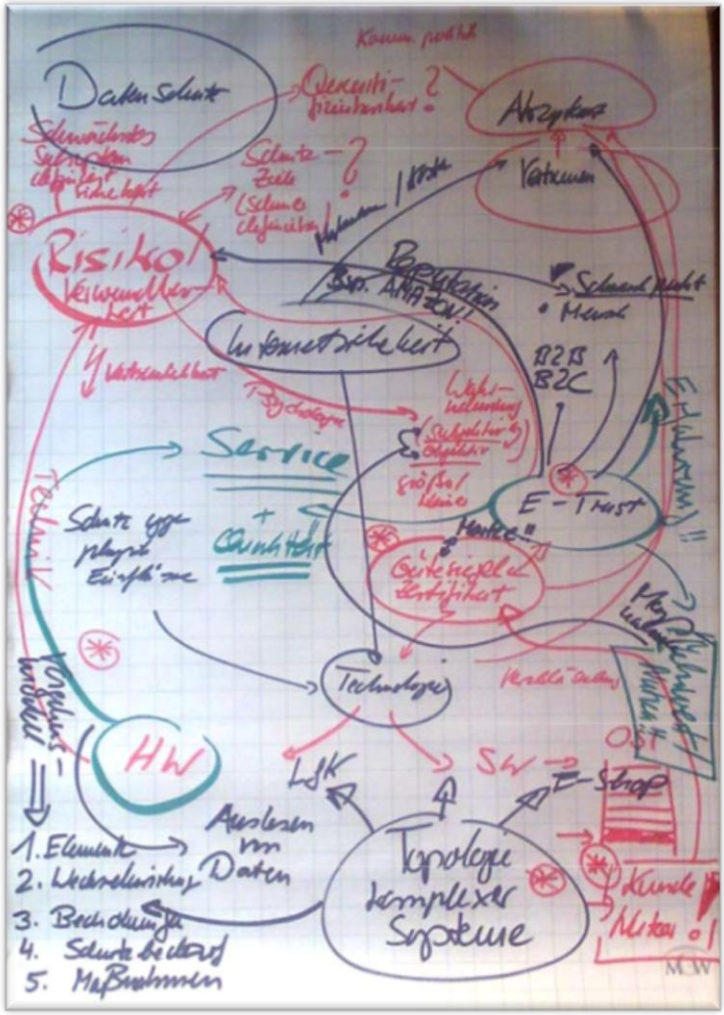
IWI Diskussionsbeiträge

32 (17. Februar 2009)[1]

ISSN 1612-3646

Entwicklung des Hannoveraner Referenzmodells für Sicherheit und Evaluation an Fallbeispielen

Sebastian Schmidt[2], **Hans-Jörg von Mettenheim**[3] und **Michael H. Breitner**[4]



[1] Kopien oder eine PDF-Datei sind auf Anfrage erhältlich: Institut für Wirtschaftsinformatik, Leibniz Universität Hannover, Königsworther Platz 1, 30167 Hannover (www.iwi.uni-hannover.de).

[2] Diplom-Ökonom

[3] Diplom-Mathematiker, Diplom-Ökonom, Institut für Wirtschaftsinformatik (mettenheim@iwi.uni-hannover.de).

[4] Professor für Wirtschaftsinformatik und Betriebswirtschaftslehre und Direktor des Instituts für Wirtschaftsinformatik (breitner@iwi.uni-hannover.de).

Inhaltsverzeichnis

Zusammenfassung

Spätestens seit den verheerenden Terroranschlägen vom 11. September 2001 gewinnt das Thema Sicherheit in Gesellschaft, Politik und Wissenschaft immer mehr an Bedeutung. Die Leibniz Universität Hannover hat aus diesem Grund die interdisziplinäre Forschungsinitiative zum Sicherheit unter der Leitung von Herrn Prof. Dr. Bach ins Leben gerufen. Ziel der Forschungsinitiative ist es, vorhandene technologische, naturwissenschaftliche sowie sozial- und geisteswissenschaftliche Kompetenzen zum Thema Sicherheit an der Leibniz Universität Hannover zu bündeln, um damit ein Forum für Fragen der Sicherheitsforschung zu schaffen, das sich besonders durch sein interdisziplinäres Profil auszeichnet.
Im Rahmen dieser Initiative haben sich Herr Prof. Dr. Breitner und Mitarbeiter des Instituts für Wirtschaftsinformatik mit der Entwicklung eines Referenzmodells Sicherheit befasst, um die komplexen Sachverhalte bei der Entstehung eines Sicherheitskonzeptes besser zu strukturieren und in zeitlich abgegrenzte Phasen zu unterteilen. Die Ergebnisse des ersten Brainstormings anlässlich eines Workshops am 10. Juli 2008 finden sich auf dem Deckblatt wieder. Bei einem zweiten Termin wurden die Gedanken weiter konkretisiert und das Modell grob entworfen. Dies ist in Abbildung 2 zu sehen.
Hauptanliegen der Arbeit ist, aus den ersten Ideen das sogenannte Hannoveraner Referenzmodell Sicherheit zu entwickeln, welches für möglichst viele Szenarien anwendbar sein soll. Zu diesem Zweck werden zuerst die relevanten Begriffe zum Thema Sicherheit definiert. Anschließend wird das grundlegende Modell in einer Abbildung dargestellt, um dann Schritt für Schritt ausführlich erläutert zu werden. Den Überlegungen des Modells folgend wird ein Excel-Tool erstellt, das über die Auswahl von Bedrohungen und Schwachstellen zu möglichen Schutzmaßnahmen führt. Im Weiteren werden zwei Fallbeispiele aus den Bereichen Videoüberwachung und Wasserversorgung vorgestellt und das erstellte Excel-Tool an diesen Beispielen getestet. Es folgt eine Auswahl von Standards, Zertifikate und Gütesiegel. Abschließend wird ein Fazit gezogen und ein Ausblick in die Zukunft gegeben.

1. Definition der grundlegenden Begriffe zum Thema Sicherheit

Bevor mit der Modellierung des Hannoveraner Referenzmodells Sicherheit begonnen wird, ist es notwendig, die grundlegenden Begriffe zu erläutern und zu definieren.

Der Begriff Sicherheit hat je nach Fachdisziplin sehr viele unterschiedliche Bedeutungen.

In dieser Arbeit bezeichnet **Sicherheit** den Zustand des Sicherseins vor Gefahr oder Schaden im öffentlichen Raum bzw. den Zustand, in dem Schutz vor Gefährdungen besteht.

Ein **öffentlicher Raum** ist ein der Öffentlichkeit zugänglicher Bereich einer Körperschaft des öffentlichen Rechts (Gemeinde, Land, Staat), z. B. Verkehrsflächen, Parkanlagen oder auch Gebäude, die von dieser Körperschaft unterhalten werden.[5] Auch das Internet kann zum öffentlichen Raum hinzugezählt werden, so dass z.B. auch das Betreten von Internet-Foren als das Betreten von öffentlichem Raum angesehen werden kann.

Wie aus der Definition von Sicherheit hervorgeht, hängt das Ausmaß von Sicherheit eng mit **Gefahren** und **Bedrohungen** zusammen.

Eine **Gefahr** bezeichnet die Möglichkeit eines Schadenseintritts.[6]

Unter einer **Bedrohung** versteht man ganz allgemein eine potentielle Gefahr, die durch eine Schwachstelle ausgelöst wird. Es kann sich dabei um ein Ereignis handeln, das Schaden verursacht. Dies kann z. B. auf Informationssysteme bezogen ein Angriff auf ein System, auf eine Übertragungsstrecke oder auf den Informationsinhalt einer Nachricht sein. Des Weiteren kann es sich um Spionage oder Sabotage oder auch um Gefahren handeln, die unbeabsichtigt oder durch höhere Gewalt wie Stromausfall eintreten, oder absichtlich bzw. vorsätzlich von Mitarbeitern ausgehen. Eine Bedrohung kann auch von der Technik selbst ausgehen, durch Fehlbedienungen oder Gewaltanwendung.[7]

Ein **Schaden** ist definiert als Nachteil, der durch Minderung oder Verlust von Vermögen entsteht. Schäden können materieller, aber auch immaterieller bzw. ideeller Natur sein.[8]

Ein eingetretenes Ereignis, das eine Abweichung vom geplanten Ziel darstellt (schlagend gewordenes Risiko), bezeichnet man ebenfalls als **Schaden**. Diese Abweichung kann im positiven oder negativen Bereich liegen. Der Schaden drückt dabei die absolute Differenz aus.[9]

Das **Risiko** ist die Möglichkeit (Wahrscheinlichkeit) einer Abweichung des tatsächlichen Ergebnisses vom erwarteten Ergebnis. Diese Abweichung kann positiv oder negativ sein.[10]

[5] Meyers Lexikon.
[6] Hoppe/Prieß, S. 28.
[7] Vgl. IT-Lexikon .
[8] Hoppe/Prieß, S. 28.
[9] Seibold, S. 13.
[10] Seibold, S. 8.

Ein **Schutz** ist das Ergebnis einer Verkleinerung des Risikos durch Maßnahmen, die entweder die Wahrscheinlichkeit des zum Schaden führenden Ereignisses oder das Schadensausmaß oder beides verkleinern.[11]

In der folgenden Abbildung sind einige der Begriffe noch einmal in einem Modell dargestellt, um ihren Zusammenhang zu verdeutlichen.[12]

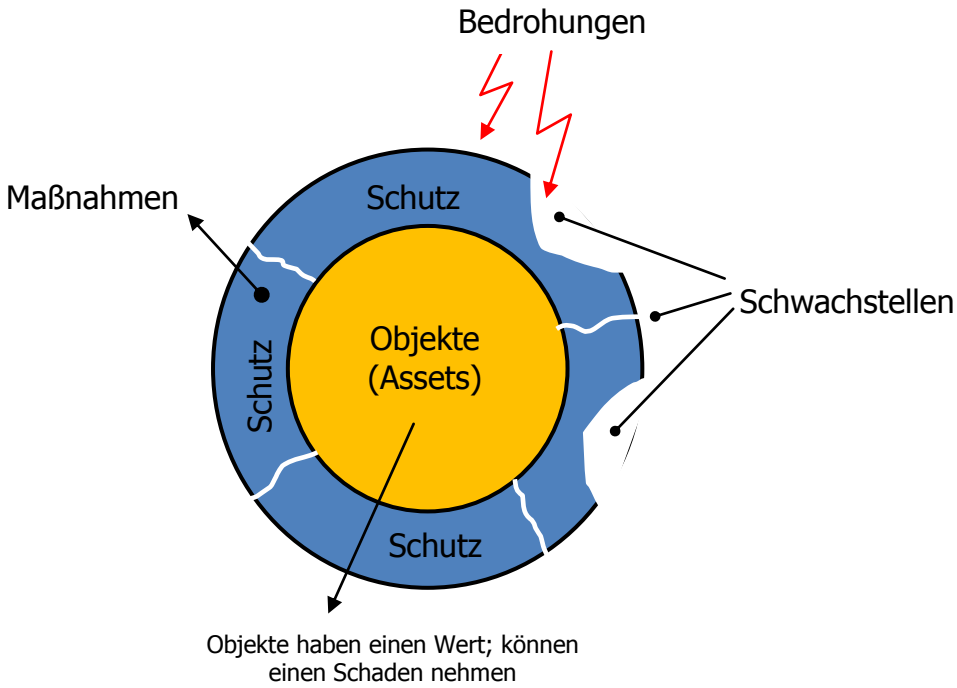


Abbildung 1: Risikomodell

[11] Vgl. Geiger/Kotte S. 128.
[12] In Anlehnung an Königs, S. 161.

2. Entwicklung des Hannoveraner Referenzmodells für Sicherheit

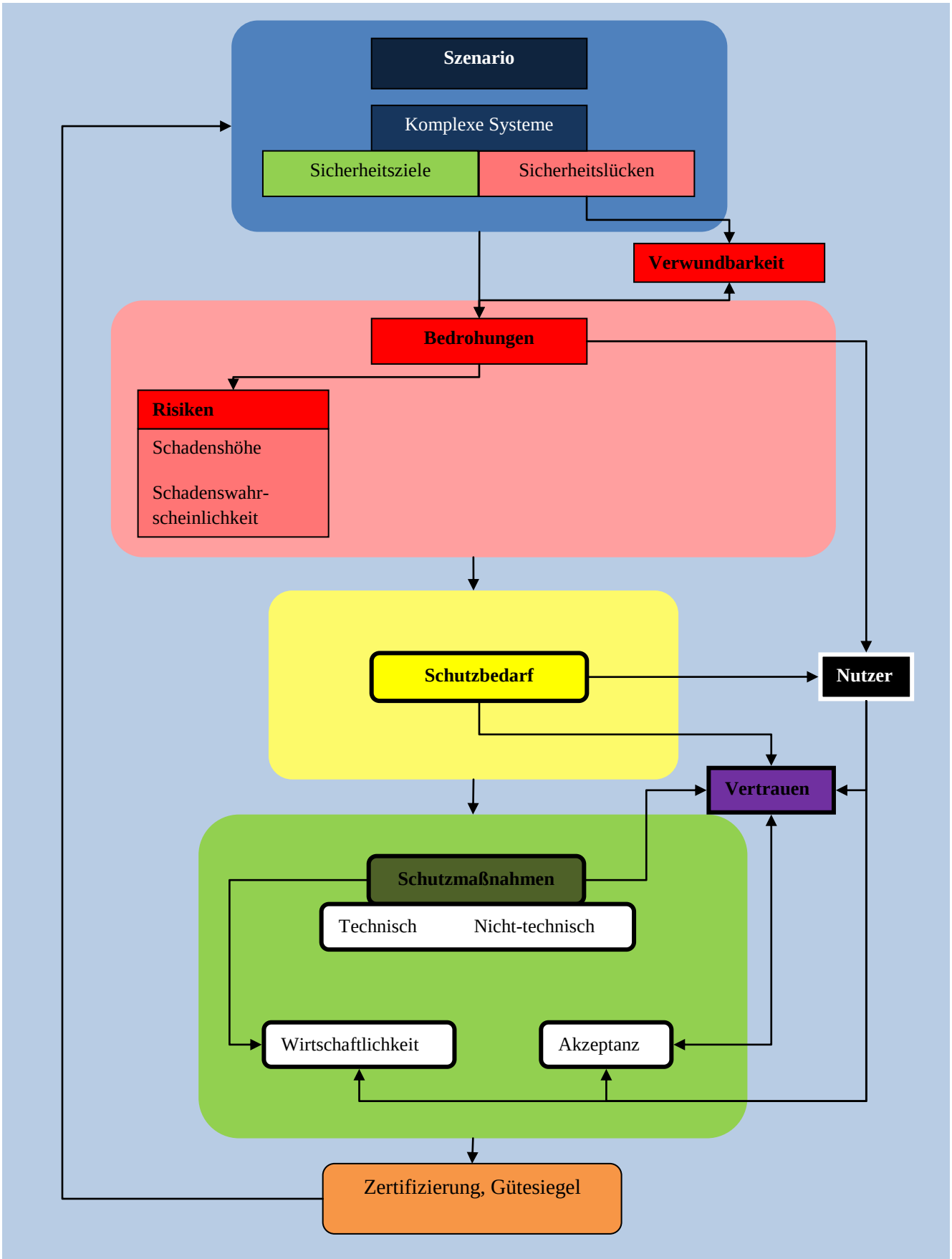


Abbildung 2: Referenzmodell Sicherheit, eigene Darstellung

2.1 Phase 1: Abgrenzung und Beschreibung des Szenarios

Ausgangspunkt für die Entwicklung eines Sicherheitskonzeptes für ein bestimmtes Szenario ist die bestehende Situation. Daher ist der erste Schritt die Abgrenzung des Analyseobjekts. Es muss also genau geklärt werden, was betrachtet werden soll. Dies kann z.B. ein Online-Shop mit seinen Geschäftsprozessen sein oder ein öffentlicher Platz, der überwacht werden soll.[13]

Desweiteren müssen die Sicherheitsziele festgelegt werden, damit später zur Festlegung des Schutzbedarfs und der Schutzmaßnahmen eine Bezugsbasis vorhanden ist. Für IT-Systeme z.B. sind dies üblicherweise Verfügbarkeit, Vertraulichkeit, Verbindlichkeit und Integrität.

2.2 Phase 2: Identifizierung und Quantifizierung von Bedrohungen und Risiken

Oftmals wird der Ansatz verfolgt, durch die direkte Umsetzung von Schutzmaßnahmen, Sicherheit zu erreichen. Dies führt allerdings dazu, dass die Auswahl der Komponenten nur auf der Basis ihrer Stärken und Schwächen getroffen wird. Dabei besteht allerdings die Gefahr, dass Bedrohungen unterschätzt bzw. übersehen werden oder dass Gefahren überbewertet werden und ein aus ökonomischer Sicht nicht akzeptabler Aufwand betrieben wird. Außerdem werden durch dieses Vorgehen eher die Symptome und nicht die Ursachen bekämpft. [14]
Ein Verfahren, das diese Fehler durch eine sorgfältige Planung im Voraus vermeiden soll, ist die Risikoanalyse mit dem Ziel, mit den zur Verfügung stehenden Mitteln, die größtmögliche Schutzwirkung zu erreichen.

2.2.1 Bedrohungs-/ Risikokategorien

Bedrohungen für ein System können von unterschiedlichen Quellen ausgehen. Diese lassen sich in verschiedene Kategorien einteilen.
Die folgende Abbildung zeigt die Kategorien:[15]

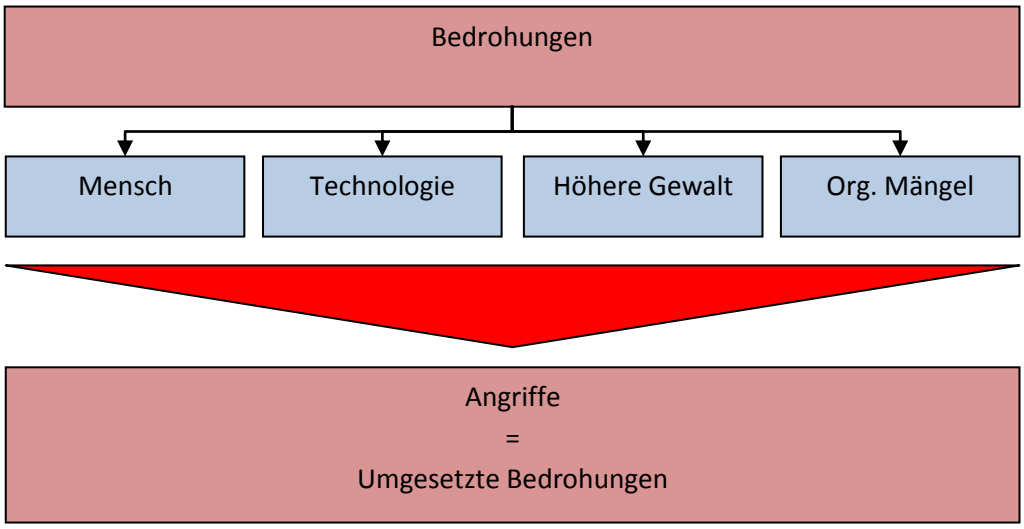


Abbildung 3: Bedrohungskategorien und Angriffe

[13] Vgl. Schmidt, S. 114.
[14] Vgl. Raepple, S. 9.
[15] In Anlehnung an Prokein, S. 14.

Mensch
Die erste Kategorie bildet der Mensch. Menschen können durch vorsätzliches oder fahrlässiges Handeln eine Gefahr für das zu betrachtende System darstellen. Wird bei fahrlässigem Handeln nicht die notwendige Sorgfalt beachtet (z.B. eine fehlerhafte Bedienung einer Anwendung oder das Vergessen, eine Tür abzuschließen), ist bei vorsätzlichem Handeln eine konkrete Absicht vorhanden, eine Handlung durchzuführen (z.B. ein Hackerangriff auf einen Online-Shop oder ein Anschlag auf die Trinkwasserversorgung).
Letzterer Typ von Angreifern lässt sich anhand von drei Eigenschaften kategorisieren:[16]
Die Stärke des Angreifers kann sehr unterschiedlich sein, so dass auch die möglichen Schäden mit der Stärke des Angreifers variieren.Zweitens lässt sich der Angreifer danach unterscheiden, ob es sich bei ihm um einen internen oder externen Angreifer handelt. Externe gehören dem System (z.B. ein Unternehmen) nicht an und versuchen von außen das System anzugreifen. Interne Angreifer hingegen gehören zum System und greifen es von innen an. Drittens ist eine Differenzierung bezüglich des Angreifertyps anhand von Motivation und Methoden des Angriffs vorzunehmen. So wird ein verärgerter Mitarbeiter einen anderen Angriff durchführen als ein Spion.

Technologie
Mit zunehmendem Einsatz von Technologie und großer Abhängigkeit von dieser steigt auch die Gefahr, dass bei Fehlern oder Ausfällen Risiken entstehen können. Diese können bspw. durch Softwarefehler, defekte Hardware oder auch andere Schäden der Infrastruktur entstehen.[17]

Höhere Gewalt
Die Schutzziele können auch von externen Einflüssen bedroht werden. Hierunter fallen zuallererst Naturkatastrophen wie Überschwemmungen, Wirbelstürme, Gewitter oder Erdbeben, und auch Stromausfälle.[18]

Organisatorische Mängel
Die letzte Kategorie, aus der Bedrohungen hervorgehen können, sind organisatorische Mängel. Liegen Schwächen in den Prozessen wie unzureichend ausgeprägte Kontrollmechanismen, unvollständig definierte Prozesse oder andere organisatorische Mängel (z.B. nicht geklärte Zuständigkeiten) vor, können Risiken entstehen.[19]

Bedrohungsobjekte
Ebenso wie es unterschiedliche Typen von Bedrohungen gibt, gibt es auch verschiedene Bedrohungsobjekte, da die Gefährdungen verschiedene Ziele haben können. Im Falle eines Informationssystems können dies z.B. die Hardware, Software, Daten, Kommunikation oder auch die Organisation sein.[20] In anderen Fällen wie in der Flugsicherheit sind die Objekte der Gefährdung Luftfahrzeuge, Personen oder Gebäude.

[16] Vgl. Prokein, S. 14.
[17] Vgl. Seibold, S. 17.
[18] Vgl. Prokein, S. 15.
[19] Vgl. Seibold, S. 18, Prokein, S. 15.
[20] Vgl. Lassmann, S. 351.

2.2.2 Identifizierung von Bedrohungen und Risiken

Ehe man sich mit dem Schutzbedarf und geeigneten Schutzmaßnahmen auseinandersetzt, ist es notwendig, dass man die Bedrohungen und Risiken für das jeweilige Szenario identifiziert und quantifiziert.
Ein Risiko entsteht durch das Zusammenwirken verschiedener Faktoren. Dies sind die Schwachstelle, der Angriffspfad und der Auslöser. Wenn alle drei Faktoren zusammentreffen, kommt es zu einer akuten Bedrohung. An diesem Punkt entsteht das Risiko und das Eintreten des negativen Ereignisses steht kurz bevor.[21]
Die Abbildung verdeutlicht das Zusammenwirken der Faktoren:[22]

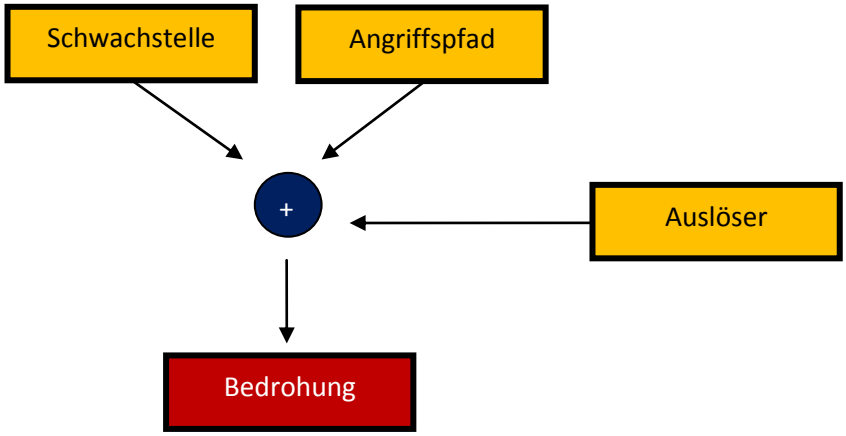


Abbildung 4: Entstehung einer Bedrohung

Angriffe nutzen Schwachstellen aus und können festgelegte Schutzziele verletzen.

Zur Identifikation der Risiken stehen mehrere Methoden zur Auswahl.[23]

Kollektions-methoden	**Suchmethoden**	
	Kreativitätsmethoden	**Analytische Methoden**
Checklisten	Brainstorming, -writing[24]	Fragenkatalog
Befragungen[25]	Synektik[26]	Angriffsbaumanalyse
SWOT-Analyse[27]	Delphi-Methode[28]	Fehlermöglichkeits- und Einflussanalyse (FMEA)[29]

Tabelle 1: Überblick der Methoden zur Risikoidentifikation

Die Kollektionsmethoden basieren alle auf der Sammlung von risikospezifischen Daten und eignen sich durch diese vergangenheitsorientierte Sicht vor allem für die Identifizierung bestehender bzw. offensichtlicher Risiken.[30]

[21] Vgl. Schmidt, S. 22ff.
[22] In Anlehnung an Schmidt, S. 24.
[23] Vgl. Piaz, S. 82.
[24] Siehe Piaz, S. 86.
[25] Siehe Seibold, S. 56ff.
[26] Siehe Romeike, S. 178.
[27] Siehe Seibold, S. 63ff.
[28] Siehe Prokein, S. 24f.
[29] Siehe Wikipedia „FMEA"
[30] Vgl. Prokein, S.20.

Die Kreativitätsmethoden und die analytischen Methoden konzentrieren sich vor allem darauf, zukünftige und bisher unbekannte Risikopotenziale zu identifizieren. Während die Kreativitätsmethoden auf kreativen Prozessen, die durch divergentes Denken charakterisiert sind, basieren, wird bei den analytischen Methoden ausgehend von den eingesetzten Systemen aktiv nach Schwachstellen und relevanten Bedrohungen gesucht.[31]
Im Weiteren werden die Checkliste, die Angriffsbaumanalyse und der Fragenkatalog näher vorgestellt.

Checkliste
Die in der Praxis am häufigsten anzutreffende Methode, um Risiken zu identifizieren ist die **Checkliste**.[32] Bei diesem Verfahren werden über die Zeit gewonnene Erfahrungen genutzt, um eine Liste von bekannten Schwachstellen und Angriffen zu erstellen. Diese Listen können dann durchgegangen werden und die Bedrohungen für die vorliegende Situation identifizieren. Für den Bereich IT-Sicherheit hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) bspw. einen Fragenkatalog entwickelt, der den Grundschutzbedarf für PCs erfassen soll.[33]
Die folgende Tabelle zeigt einige Beispiele von Fragen zur IT-Organisation:[34]

	Ja	Nein
Gibt es für die eingesetzten Datenträger ein Bestandsverzeichnis?	☐	☐
Sind die Datenträger gekennzeichnet?	☐	☐
Werden die Datenträger sachgerecht und vor unbefugtem Zugriff geschützt aufbewahrt?	☐	☐
Werden Vollständigkeitskontrollen des Datenträgerbestandes vorgenommen?	☐	☐
Werden von Dritten erhaltene Datenträger auf Computer-Viren überprüft?	☐	☐

Tabelle 2: Checkliste zur Identifikation von Risiken

An den Checklisten wird kritisiert, dass sie einen hohen Aggregationsgrad aufweisen und so regelmäßig nicht auf die Einzelrisiken und deren Wechselwirkungen geschlossen werden kann. Außerdem werden die mangelnde Vollständigkeit und die starre Vorgehensweise kritisiert.[35]

Angriffsbaumanalyse
Die **Angriffsbaumanalyse** gehört zu den analytischen Methoden und ist eine Top-Down-Methode. Sie wurde von Bruce Schneier entwickelt. Ausgehend von einem Angriffsziel eines potentiellen Angreifers werden alle möglichen Angriffswege hinsichtlich ihrer Verwundbarkeit und des nötigen Aufwands analysiert und in einer Baumstruktur dargestellt. Diese gefundenen Wege erfordern die entsprechenden Gegenmaßnahmen.[36]
Die Methodik ist recht schnell erläutert: Der Wurzelknoten stellt das Angriffsziel dar. Die daran angeschlossenen Knoten stellen Möglichkeiten dar, dieses Ziel zu erreichen. Sind

[31] Vgl. Prokein, S.20.
[32] Vgl. Romeike; S. 175.
[33] Vgl. BSI (A)
[34] In Anlehnung an BSI (A)
[35] Vgl. Romeike, S. 175.
[36] Vgl. Witt, S. 111.

diese trivial zu erreichen, werden sie als Blattknoten dargestellt und stellen die Schwachstellen dar, die auch dem Unternehmen Aufschluss darüber geben, wie geeignete Maßnahmen für die Bedrohungen gefunden werden können.[37]
Es ist zu beachten, dass es sogenannte oder-Knoten und und- Knoten gibt. Die oder-Knoten sind Alternativen, um das Ziel zu erreichen, und-Knoten müssen beide erfüllt werden, um das Ziel zu erreichen.
Um die Angriffsbäume zu erweitern, können sie mit quantitativen (z.B. entstehende Kosten) und qualitativen Faktoren (z.B. Schwierigkeitsmaß des Ausnutzens der Schwachstelle) beschrieben werden.
Der Vorteil der Methodik der Angriffsbäume liegt vor allem darin, dass man mit ihnen potentiell alle Einzelrisiken für ein System identifizieren kann. Werden alle Angriffswege aufgespürt, können die jeweiligen Schwachstellen und Bedrohungen erfasst und mit schützenden Maßnahmen bedacht werden. Als Kritikpunkt wird allerdings aufgeführt, dass sich für komplexe Systeme auch dementsprechend sehr komplexe Angriffsbäume ergeben und somit ein hoher Aufwand für die Erstellung verbunden ist.[38]

Fragenkatalog

Fragenkataloge sind den Checklisten recht ähnlich, erlauben jedoch eine tiefergehende Analyse, da sie eine derivative Methode von Checklisten, Interviews, Dokumentanalyse und Inspektionen sind.[39] Durch eine Serie von Fragen, deren Antworten Hinweise auf Schwachstellen und Bedrohungen aufweisen, wird der Risikomanager zur Entdeckung möglicher Risiken hingeführt.[40]
Das Bundesamt für Sicherheit in der Informationstechnik hat z.B. Fragenkataloge zur Informationssicherheit erstellt. Einige Fragen zur Datenträgerverwaltung werden in der folgenden Tabelle vorgestellt:[41]

	Ja	Teil-weise	Nein	Kommentar
Erlaubt die Art der Datenträgerkennzeichnung deren Identifizierung, ohne dass für Unbefugte Rückschlüsse auf den Inhalt möglich sind?	☐	☐	☐	
Werden alle Datenträger sachgerecht aufbewahrt?	☐	☐	☐	
Sind alle Datenträger vor unbefugtem Zugriff geschützt?	☐	☐	☐	

Tabelle 3: Fragenkatalog zur Risikoidentifikation

[37] Vgl. Prokein, S. 27.
[38] Vgl. Schneier, S. 315.
[39] Vgl. Piaz, S. 90.
[40] Vgl. Vaughan, S. 111.
[41] In Anlehnung an BSI (B)

Fragenkataloge stellen eine kostengünstige Alternative dar, um Risiken zu identifizieren. Allerdings setzen sie die Kenntnis potentieller Angriffe voraus und sind somit erst in der zweiten Phase einzusetzen, da Fragenkataloge auf den Ergebnissen der anderen Instrumente basieren.[42]
Werden standardisierte Fragebögen eingesetzt, entfällt dieser Nachteil. Es ergibt sich allerdings ein anderer Nachteil, da sie für einen weiten Einsatzbereich konzipiert sind, so dass seltene Risiken und systemspezifische Faktoren oftmals nicht berücksichtigt werden.[43]

2.2.3 Risikoeigenschaften

Risiken werden durch Eintrittswahrscheinlichkeit und erwartete Verlusthöhe charakterisiert. Diese werden im Folgenden vorgestellt:

Eintrittswahrscheinlichkeit
Die Eintrittswahrscheinlichkeit gibt die Häufigkeit eines Risikoeintritts an. Wahrscheinlichkeiten werden in der Mathematik mit einem Wahrscheinlichkeitswert angegeben, der zwischen 0 (ausgeschlossen) und 1 (absolut sicher) liegt. Zur Ermittlung der Wahrscheinlichkeit gibt es verschiedene Ansätze: Sind aus der Vergangenheit Werte bekannt, wie oft ein Ereignis eingetreten ist, kann daraus bestimmt werden, wie wahrscheinlich das Auftreten des Ereignisses in der Zukunft ist. Wichtig hierfür ist zum einen der Beobachtungszeitraum. Je länger der Beobachtungszeitraum, desto genauer und aussagekräftiger sind die Ergebnisse. Zum anderen ist die Anzahl der beobachteten Szenarien für die Genauigkeit relevant, da mehrere Szenarien ein exakteres Bild zeichnen als ein einzelnes.[44]

Ist keine ausreichende statistische Basis vorhanden, können die Eintrittswahrscheinlichkeiten häufig nicht genau bestimmt werden. In diesem Fall bietet sich eine Einteilung in Risikoklassen an, da diese einen Kompromiss zwischen Genauigkeit und Übersichtlichkeit bietet.
Die Abbildung zeigt exemplarisch Risikoklassen für die Eintrittswahrscheinlichkeit.[45]

Risikoklasse	Bezeichnung	Definition der Eintrittswahrscheinlichkeit
Extrem seltenes Risiko	a	25 Jahre
Sehr seltenes Risiko	b	10 Jahre
Seltenes Risiko	c	5 Jahre
Häufiges Risiko	d	Monatlich
Sehr häufiges Risiko	e	Wöchentlich
Extrem häufiges Risiko	f	Täglich

Tabelle 4: Exemplarische Risikoklassen nach Eintrittswahrscheinlichkeit

[42] Vgl. Piaz, S. 90.
[43] Vgl. Vaughan, S. 112.
[44] Vgl. Schmidt, S. 124.
[45] In Anlehnung an Seibold, S. 21.

Erwartete Verlusthöhe

Das zu erwartende Auswirkungsmaß gibt die zu erwartende Schadenshöhe an. Auch hier empfiehlt es sich, Risikoklassen zu erstellen. Hierbei ist es besonders wichtig, die Risikoklassen an die jeweiligen Szenarien anzupassen, da die Risikotragfähigkeit, d.h. der maximal tragbare Schaden, in den unterschiedlichen Szenarien sehr unterschiedlich ist. So kann ein mögliches Schadensvolumen für ein großes Unternehmen nur geringe Konsequenzen haben, aber für einen kleinen Online-Shop-Betreiber bereits die Insolvenz bedeuten.

Die Tabelle zeigt exemplarische Risikoklassen nach Auswirkungsmaß:[46]

Risikoklasse	Bezeichnung	Definition des Auswirkungsmaßes
Sehr geringes Risiko	A	≤ 1 T€
Geringes Risiko	B	> 1 T€ und ≤ 10 T€
Mittleres Risiko	C	> 10 T€ und ≤ 100 T€
Großes Risiko	D	> 100 T€ und ≤ 1 Mio. €
Sehr großes Risiko	E	> 1 Mio. € und ≤ 10 Mio. €
Ruinöses Risiko	F	> 10 Mio. €

Tabelle 5: Exemplarische Risikoklassen nach Schadensausmaß

Risikopotenzial

Das Risikopotenzial leitet sich aus den zwei oben beschriebenen Faktoren ab. Es ist das Produkt aus Eintrittswahrscheinlichkeit und Schadenshöhe. Je wahrscheinlicher es ist, einen Schaden oder Verlust zu erleiden, desto größer ist das Risiko. Je größer der Schaden oder Verlust ist, der entstehen könnte, desto größer ist das Risiko.[47]

$$\text{Risiko} = \text{Eintrittswahrscheinlichkeit} \cdot \text{Schadenshöhe}$$

Sind diese beiden Werte für ein Risiko genau bezifferbar, lässt sich das Risikopotenzial direkt errechnen. Sollten diese exakten Daten allerdings nicht vorliegen, erfolgt eine Einteilung in die Risikoklassen. Anhand von Rechenregeln, meist auf der Basis von Mittelwerten, lässt sich das Risikopotenzial berechnen.

[46] In Anlehnung an Seibold, S. 22.
[47] Vgl. Schmidt, S. 121.

2.2.4 Quantifizierung von Risiken

Für die Quantifizierung von Risiken werden verschiedene Methoden angewandt. Die folgende Tabelle gibt einen Überblick über Methoden zur Ermittlung operationeller Risiken:[48]

Indikator-Ansätze	**Befragungstechniken und Szenarioanalyse**	**Stochastische Methoden**	**Kausal-Methoden**
Schlüsselwert-Methode[49]	Befragungstechniken[50] - Experteninterviews - Self-Assesments	Vollenumeration[51]	Bayes-Netze[52]
Modifizierter Basisindikatoransatz nach Basel II[53]	Szenarioanalyse[54]	Monte-Carlo-Simulation	
Modifizierter Standard-Ansatz nach Basel II[55]		Extremwertmethode[56]	
Interner Bemessungsansatz			
Scorecard-Ansätze[57]			
Capital Asset Pricing Model[58]			

Tabelle 6: Überblick über die Methoden der Risikoquantifizierung

Bei den Indikatoransätzen wird anhand einer Kennzahl bzw. eines Kennzahlensystems versucht, das vorliegende Risiko indirekt zu ermitteln. Die Indikatoren basieren einerseits auf empirischen Untersuchungen und andererseits auf Expertenmeinungen.
Auch bei Befragungstechniken und der Szenarioanalyse werden Expertenbefragungen als Grundlage genommen, um Verluste aus Risiken zu quantifizieren.
Bei den Kausalmethoden werden die Zusammenhänge zwischen Risikoursachen und/oder – indikatoren und den entstehenden Schäden unter Zuhilfenahme statistischer Methoden untersucht.
Bei den stochastischen Methoden werden statistische Verteilungsfunktionen zur Schätzung der Verluste aus Risiken benutzt. Historische Daten bzgl. Verlusthäufigkeit und -höhe helfen dabei, Aussagen zur Quantifizierung der Risiken zu treffen.[59]

Der interne Bemessungsansatz und die Value-at-Risk Bestimmung über die Monte-Carlo-Simulation werden in dieser Arbeit näher vorgestellt, wobei letztere im späteren Verlauf der Arbeit genutzt wird, um die Risiken der Fallbeispiele zu quantifizieren.

[48] In Anlehnung an Faisst/Kovacs, S. 4.
[49] Siehe Seibold, S. 120ff.
[50] Siehe Seibold, S. 56ff.
[51] Siehe Hölscher, Kalhöfer und Bonn, S. 500ff.
[52] Siehe Alexander (2003a), S. 285ff.
[53] Siehe Prokein, S. 38f.
[54] Siehe Seibold, S. 72ff.
[55] Siehe Baseler Ausschuss für Bankenaufsicht, S. 129ff.
[56] Siehe Prokein, S. 58ff.
[57] Siehe Prokein, S.46.
[58] Siehe Schmid, Trede, S.195ff.
[59] Vgl. Prokein, S. 35f.

Monte-Carlo-Simulation und Value-at-Risk

Bei der Monte-Carlo-Simulation handelt es sich um ein stochastisches Verfahren. Auf der Grundlage von sehr häufig durchgeführten Zufallsexperimenten werden Schlussfolgerungen über den Zusammenhang zwischen Input- und Outputvariablen gezogen. Auf der Basis von Zufallszahlen für die Verlusthäufigkeits- und Verlusthöhenverteilung wird eine Gesamtverlustverteilung ermittelt.[60] Für die Verlusthäufigkeitsverteilungen sind die Binomial-, negative Binomial-, Poisson-, geometrische und die Pascalverteilung geeignet. Die Lognormal-, Wald-, Exponential-, Weibull-, Pareto- Gamma-, Cauchy-, Beta- sowie die Rayleigh-Verteilung sind gängige Verteilungen für die Verlusthöhen.[61]

Rommelfanger beschreibt die Vorgehensweise wie folgt:[62]
Ausgangspunkt der Monte-Carlo-Simulation ist ein deterministisches Modell.[63]

$$K = \begin{pmatrix} 1 & \rho_{x_1x_2} & \cdots & \rho_{x_1x_{m-1}} & \rho_{x_1x_m} \\ \rho_{x_2x_1} & 1 & \cdots & \rho_{x_2x_{m-1}} & \rho_{x_2x_m} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \rho_{x_{m-1}x_1} & \rho_{x_{m-1}x_2} & \cdots & 1 & \rho_{x_{m-1}x_m} \\ \rho_{x_mx_1} & \rho_{x_mx_2} & \cdots & \rho_{x_mx_{m-1}} & 1 \end{pmatrix}$$

Abbildung 5: Deterministisches Modell I

Hierbei werden zuerst die Variablen des Modells bestimmt und die Zusammenhänge zwischen den Variablen abgebildet.

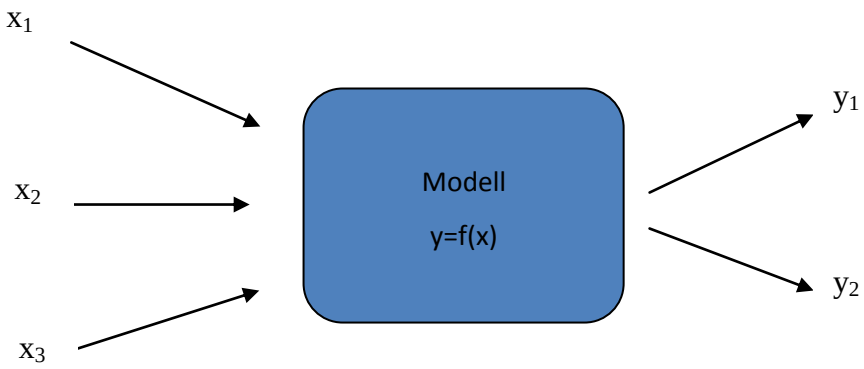


Abbildung 6: Deterministisches Modell II

Im zweiten Schritt wird eine Menge von Zufallsinputwerten generiert. Mit Hilfe dieser Zufallszahlen wird das deterministische Modell immer wieder berechnet und die Ergebnisse bewertet. Die Generierung und die Berechnung der Zufallszahlen werden heute von Computern vorgenommen. Durch die in den letzten Jahren stark gestiegene Rechenleistung können die Zufallsvorgänge fast in beliebigem Umfang durchgeführt werden.

[60] Vgl. Haubenstock/Hardin, S. 184.
[61] Vgl. Cruz, S. 49ff.
[62] Vgl. Rommelfanger, 39ff.
[63] Abbildungen 11-13 in Anlehnung an Rommelfanger, S. 39f.

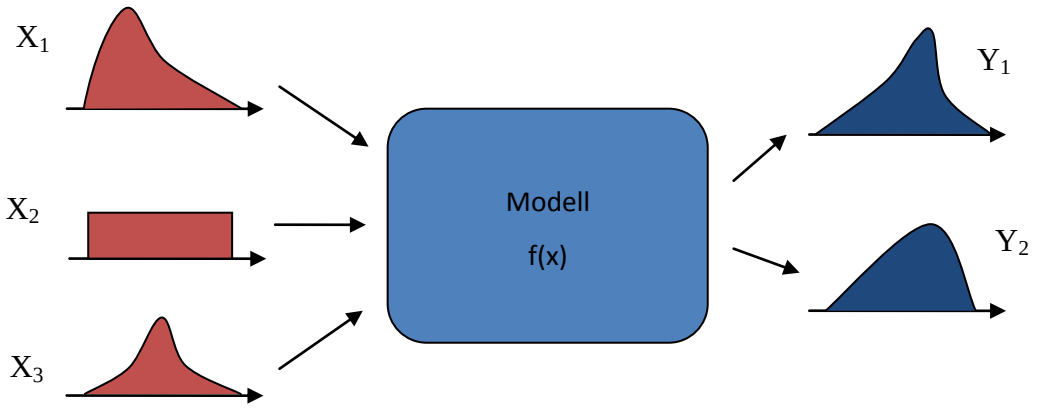


Abbildung 7: Stochastisches Modell

Im dritten Schritt wird das Modell evaluiert und die berechneten Bewertungsgrößen, z.B. die Risikoparameter, werden gespeichert.
Im anschließenden vierten Schritt werden mehrere Simulationsläufe durchgeführt, um eine stabile Basis für die Schlussfolgerungen zu erhalten.
Im letzten Schritt sind die Gesamtresultate zu analysieren. Zum Einsatz kommen häufig Histogramme und Konfidenzintervalle.

Der Value-at-Risk ist ein Risikomaß, welches eine Auskunft darüber gibt, wie hoch der maximale Verlust einer Einzelposition oder eines Portfolios bei einem gegebenen Konfidenzniveau ist. Für ein Konfidenzniveau von bspw. 95% ist man sich zu 95% sicher, dass der maximale Verlust am Ende eines Zeithorionts den Value-at-Risk nicht übersteigt.[64]

Für das folgende Beispiel und auch für die späteren Anwendungsfälle wird eine zweistufige Monte-Carlo-Simulation durchgeführt[65], bei der zunächst aus der Verlusthäufigkeitsverteilung eine zufällige Anzahl an Verlusten (N) gezogen wird. Im Anschluss wird aus der Verlusthöhenverteilung N-mal eine dazugehörige Verlusthöhe generiert. Daraus resultiert ein Szenario, das eine Anzahl (N) an Verlustereignissen und den dazugehörigen Verlusthöhen aufweist.[66]
Von diesen Szenarien wird eine hinreichend große Anzahl n erzeugt, so dass jedes Szenario eine Wahrscheinlichkeit von 1/n aufweist. Die Verlusthöhen können anschließend der Größe nach aufsteigend sortiert werden. Der Verlust für das gewünschte Konfidenzniveau α entspricht dem $[\alpha \cdot n]$-ten Wert der sortierten Liste. Bei z.B. 10.000 Simulationsläufen und einem Konfidenzniveau von 95% ist der 9500. Wert der Liste der gesuchte Verlust. Allerdings ist dieser Wert der Gesamtverlust, so dass zur Berechnung des Value-at-Risk noch der erwartete Verlust subtrahiert werden muss.[67]

Als Beispiel dient wieder der bereits vorgestellte Viren-Import durch E-Mail Empfang. Die Verlusthäufigkeitsverteilung sei poisson-verteilt, da Untersuchungen gezeigt haben, dass die Poisson-Verteilung bei operationellen Risiken eine geeignete Verteilung darstellt.[68] Im Bespiel sei angenommen, dass jede 100ste E-Mail mit einem Virus infiziert ist. Bei 4000

[64] Vgl. Rau-Bredow, S. 2.
[65] Vgl. Prokein, S. 53, zitiert nach Peter, Vogt und Kraß, S. 671.
[66] Vgl. Hölscher, Kalhöfer und Bonn, S. 501f.
[67] Vgl. Hölscher, Kalhöfer und Bonn, S. 502.
[68] Vgl. Chavez-Demoulin und Embrechts; Fontnouvelle et al.

betrachteten E-Mails im betrachteten Zeitraum ergibt sich also eine erwartete Verlusthäufigkeit von 40 pro Periode.
Die Verteilung nimmt folgenden Verlauf an:[69]

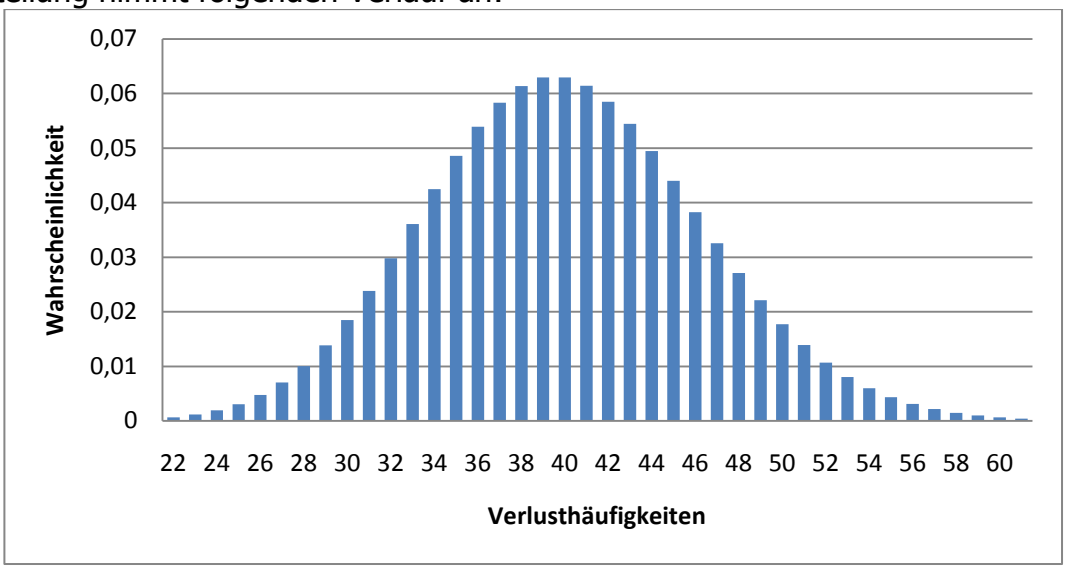


Abbildung 8: Verteilung der Verlusthäufigkeiten

Die Verlusthöhen werden durch eine Exponentialverteilung beschrieben. Der erwartete Verlust pro Ereignis liegt im Beispiel bei 4000 €. Daraus ergibt sich, dass der Parameter der Exponentialverteilung den Wert λ = 0,00025 annimmt.
Der Verlauf der Exponentialverteilung ist in nachstehender Abbildung veranschaulicht:[70]

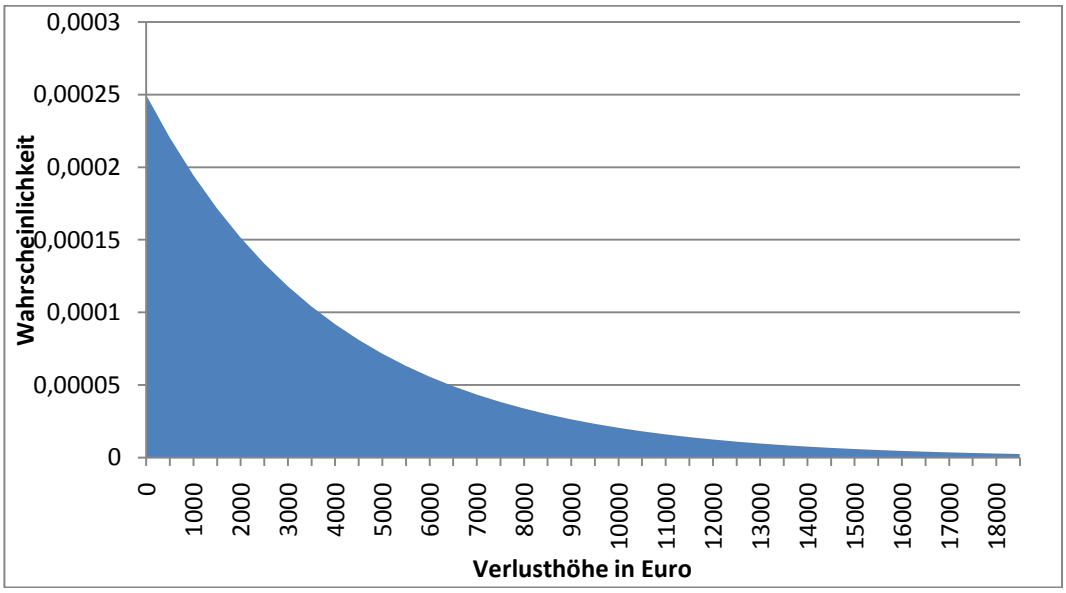


Abbildung 9: Verteilung der Verlusthöhen

Mittels Zufallszahlen der Verlusthäufigkeits- und Verlusthöhenverteilung wird die Gesamtverlustverteilung ermittelt. Sie nimmt bei 10000 Szenarien den in der folgenden Abbildung dargestellten Verlauf an.[71]

[69] Abbildung eigene Darstellung
[70] Abbildung eigene Darstellung
[71] Abbildung eigene Darstellung

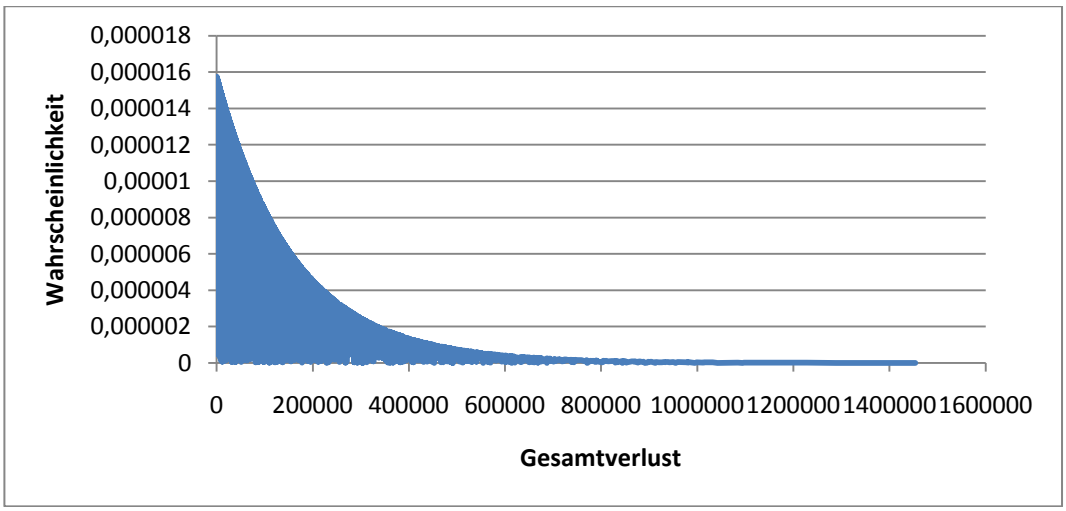


Abbildung 10: Verteilung des Gesamtverlustes

Der erwartete Verlust errechnet sich durch die Multiplikation der erwarteten Verlusthäufigkeit und Verlusthöhe, da angenommen wurde, dass die beiden Verteilungen unabhängig voneinander sind.

$P(A \cap B) = P(A) \cdot P(B)$

Der Wert der Gesamtverlustverteilung ist folglich 40 · 4000 = 160.000 €.
Bei einem Konfidenzniveau von 95% beträgt das maximal erwartete Verlustpotenzial 485.000 €. Die Differenz dieser beiden Werte ergibt den Value-at-Risk und beträgt im Beispiel 325.000 €.[72]

Durch die Verteilungsunabhängigkeit bietet die Monte-Carlo-Simulation eine sehr hohe Flexibilität bei der Quantifizierung von IT-Risiken.
Die Monte-Carlo-Simulation kann im Vergleich zu den anderen Methoden die genauesten Ergebnisse für die Value-at-Risk abliefern.
Als Kritik wird der hohe Rechenaufwand der Monte-Carlo-Simulation angeführt. Dies gilt sowohl für die Simulation selbst als auch für die Findung geeigneter Verteilungen und die Durchführung der notwendigen Anpassungstests.[73]

2.3 Phase 3: Ermittlung des Schutzbedarfs

Der Schutzbedarf für das zu schützende Objekt wird aufgrund des möglichen Schadensausmaßes bestimmt.[74] Wichtig hierbei ist nicht nur, das akute Schadensausmaß zu betrachten, sondern auch mögliche Schadensfolgen in die Schutzbedarfsanalyse mit einfließen zu lassen.
Vor der eigentlichen Schutzbedarfsanalyse ist eine Festlegung von Schutzbedarfsklassen sinnvoll. Die Schutzbedarfe der einzelnen Schutzobjekte sind üblicherweise unterschiedlich und so wäre es notwendig, für jedes Objekt ein individuelles Schutzkonzept und Schutzmaßnahmen zu entwickeln. Dadurch würde die Komplexität steigen und die Effizienz lei-

[72] Vgl. Prokein, S. 56.
[73] Vgl. Oehler/Unser, S.161.
[74] Vgl. Kersten, Reuter, Schröder, S. 27.

den. Die Einteilung in Schutzbedarfsklassen bietet daher einen Kompromiss, um die Komplexität zu beherrschen und Effizienz zu gewährleisten.[75]
Für jede Schutzbedarfsklasse ist festzulegen, welche Sicherheitsanforderungen sie erfüllt bzw. welche Auswirkungen von Sicherheitsverletzungen sie abdeckt.

2.4 Phase 4: Auswahl der Schutzmaßnahmen

Wie aus der in Kapitel 1 genannten Definition für Schutz folgt, können Schutzmaßnahmen die Schadenswahrscheinlichkeit und bzw. oder das Schadensausmaß verringern.
Generell ist zwischen präventiven, überwachenden und korrigierenden Schutzmaßnahmen zu unterscheiden.[76]
Aufgabe der präventiven Maßnahmen ist es, die Eintrittswahrscheinlichkeit von Gefahren bereits im Vorfeld zu verringern. Dabei sind verhindernde Maßnahmen, die darauf abzielen, Gefahren vollständig zu unterbinden, von behindernden Maßnahmen zu unterscheiden, deren Ziel es ist, die Durchführung von Angriffen zu erschweren.[77]
Überwachende Maßnahmen sollen eingetretene Gefahren erkennen und versuchen abzuwehren. In Verbindung mit behindernden Maßnahmen wirken überwachende Maßnahmen auch präventiv. Als Beispiel sei hier die Alarmanlage genannt. Ihr originärer Zweck ist die Entdeckung von Angriffen, sie kann aber auch abschreckend auf den Angreifer wirken. [78]
Korrigierende Maßnahmen haben die Aufgabe, nach bereits eingetretenen Schäden den Eintritt von Schadensfolgen zu verhindern und die Schäden zu minimieren.

Darüber hinaus ist eine weitere Klassifizierung der Sicherheitsmaßnahmen auf ihr Bezugsobjekt möglich. So ist eine erste grobe Abgrenzung von technischen und nicht-technischen Maßnahmen möglich. Beziehen sich die technischen Sicherheitsmaßnahmen vor allem auf Hard- und Software, umfassen die nicht-technischen Sicherheitsmaßnahmen Maßnahmen im Bereich Personen, Organisation, Räume und Gebäude, IT-Revision und Versicherungen.

Um ein hohes Sicherheitsniveau zu gewährleisten, müssen alle und nicht nur einzelne Bereiche betrachtet werden. Es ist beispielsweise nicht sinnvoll, sich nur auf die Qualität der technischen Sicherheitsmaßnahmen zu konzentrieren, da durch Mängel in den personenbezogenen Sicherheitsmaßnahmen die technischen Maßnahmen ihre Wirkung nicht entfalten können.
Als Beispiel sei an dieser Stelle die Nichtbeachtung von Sicherheitsmaßnahmen durch Mitarbeiter genannt. Dies wird häufig durch mangelndes Sicherheitsbewusstsein hervorgerufen.[79] An diesem Beispiel wird deutlich, dass der Mensch im Regelfall das schwächste Glied in einem Sicherheitssystem ist.

Es ist also notwendig, ein ganzheitliches Sicherheitsmanagement durchzuführen, d.h. nicht nur die technischen Voraussetzungen für Sicherheit zu schaffen, sondern auch Mitarbeiter durch Qualifizierung und Sensibilisierung in Hinblick auf sicherheitsrelevante Themen vorzubereiten. Die gleiche Sorgfalt ist für die anderen nicht-technischen Maßnahmen zu beachten. So muss auch den Maßnahmen in den organisatorischen Bereichen ebenso viel

[75] Vgl. Müller, S. 98.
[76] Vgl. Raeplle, S. 23.
[77] Vgl. Hoppe/Prieß, S. 55.
[78] Vgl. Hoppe/Prieß, S. 55.
[79] Vgl. BSI (C)

Aufmerksamkeit gewidmet werden, da fehlende Zuständigkeiten oder fehlerhafte Abläufe Risiken hervorrufen können.

2.4.1 Kosten und Nutzen der Sicherheitsmaßnahmen

Die Realisierung von Sicherheitsmaßnahmen kostet Geld. Da eine hundertprozentige Sicherheitslösung selbst mit unbegrenzten Mitteln kaum zu realisieren ist, ist es notwendig, das ideale Maß an Sicherheit in Abhängigkeit von den finanziellen Rahmenbedingungen zu ermitteln. Aufwand und Nutzen der Sicherheitsmaßnahmen müssen in einem ausgewogenen Verhältnis zueinander stehen.[80] Zu diesem Zweck ist eine Kosten-Nutzen-Analyse wichtig, um sicherzustellen, dass die für die jeweilige Situation geeigneten Sicherheitsmaßnahmen ausgewählt und implementiert werden, ohne die Kosten zu stark zu belasten.[81]
Die folgende Abbildung verdeutlicht diese Überlegungen grafisch:[82]

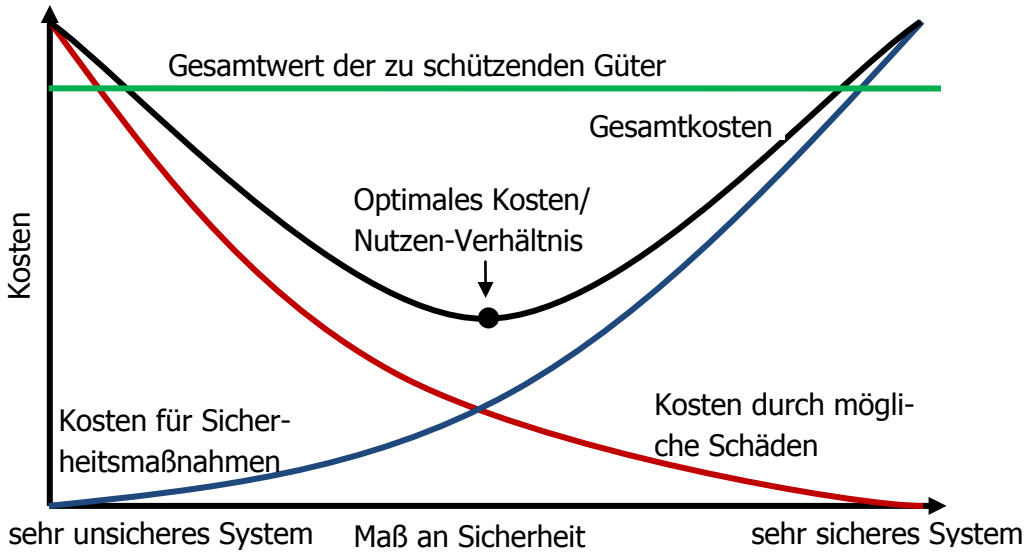


Abbildung 11: Kosten-Nutzen-Verhältnis von Schutzmaßnahmen

Return on Security Investment
Wie bereits beschrieben, müssen Sicherheitsmaßnahmen zum einen ein gewisses Maß an Sicherheit garantieren, zum anderen müssen sie aber auch wirtschaftlich sein. Mithilfe des **Return-on Security-Investment-Modells (ROSI)** wird der Nutzengewinn aus der Investition in Sicherheitsmaßnahmen berechnet. Wie beim bekannten ROI gilt auch hier die Annahme, dass eine Investition in Sicherheitsmaßnahmen nach einer gewissen Zeit einen positiven Nutzen generiert.[83] ROSI ist definiert als Differenz aus den Wiederherstellungskosten (R) und der jährlichen Verlusterwartung (ALE).[84]
Dies sind die eingesparten Kosten, die durch die Investition in die Sicherheitsmaßnahmen erreicht worden sind.

R-ALE=ROSI

[80] Vgl. Raepple, S. 8.
[81] Vgl. Laudon et al., S. 681.
[82] Abbildung in Anlehnung an Raepple, S. 9.
[83] Vgl. Müßig, S. 39.
[84] Vgl. Schadt, S. 22.

R-S+T=ALE

ROSI=S-T

R ist die Abkürzung für **Recovery Costs**. Diese Kosten beschreiben die Aufwendungen, die nötig sind, falls ein Schaden eingetreten ist und der ursprüngliche Zustand wieder hergestellt werden soll.
S steht für **Savings**, also für die Kosten, die durch den Einsatz von Sicherheitsmaßnahmen gespart werden.
T ist die Abkürzung für **Tool Costs**. Dies sind die gesamten Kosten für die Sicherheitsmaßnahmen, die dazu gedacht sind, potenzielle Angriffe mit einer hohen Wahrscheinlichkeit zu verhindern.
ALE sind die **Annual Loss Expenditures**, die Kosten, die auch nach einer Investition in Sicherheitsmaßnahmen verbleiben. ALE ist die Summe der negativen Auswirkungen multipliziert mit ihren Häufigkeiten pro Jahr. Ebenfalls ergibt sich ALE auch aus der Summe von Recovery Costs und Tool Costs abzüglich der Savings.

Solange die Kosten der Sicherheitsmaßnahmen kleiner als die Einsparungen durch die Sicherheitsmaßnahmen sind, ist ROSI positiv.

Abbildung 15 verdeutlicht die Rechnung grafisch:[85]

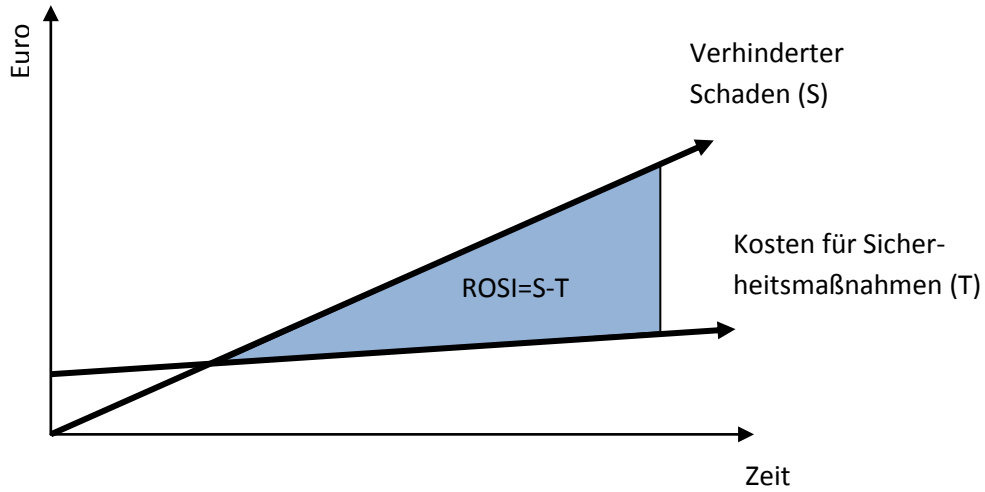


Abbildung 12: Return on Security Investment

Ein Beispiel über die Anschaffung von Viren-Scannern soll das ROSI-Konzept verdeutlichen. Den Zahlen aus der Monte-Carlo-Simulation folgend wird angenommen, dass jede 100ste E-Mail, die ein Unternehmen erreicht, mit einem Virus versehen ist. Über den beobachteten Zeitraum von einem Monat werden 4000 E-Mails empfangen. Um einen Virenbefall der 100 Unternehmensrechner zu verhindern, besteht die Möglichkeit, auf jedem Rechner einen Viren-Scanner zu installieren, der virenverseuchte E-Mails erkennt und automatisch aussortiert. Eine Lizenz des Viren-Scanners kostet 110 €. Für die Installation und Wartung fallen im ersten Monat 5.000 € und in den darauf folgenden Monaten jeweils 2000 € Kosten an.

[85] Abbildung in Anlehnung an Pohlmann, S. 28.

3. Excel-Tool „Sicherheit"

In diesem Kapitel wird das entwickelte Excel-Tool „Sicherheit" vorgestellt.
Das Tool hat die Aufgabe, durch die Auswahl und Bewertung von Bedrohungen und Schwachstellen die geeigneten Schutzmaßnahmen vorzuschlagen.
Zur Benutzung ist zum einen das Plug-In SimTools2007 von der CD zu installieren, zum anderen sind Makros zu aktivieren.

Blatt „Bedrohungen"
Das Blatt Bedrohungen zeigt eine Auswahl an verschiedenen Bedrohungen aus den Bedrohungskategorien Mensch, Technik, Organisation und höhere Gewalt.

Für die einzelnen Bedrohungen ist mittels einer Drop-Down-Liste eine Auswahl zu treffen, wie hoch der Grad der Bedrohung eingeschätzt wird. Die Bewertungsmöglichkeit geht von „sehr niedrig" über „mittel" bis „sehr hoch". Den jeweiligen Einschätzungen werden Punkte zugeordnet. „Sehr niedrig" erhält einen Punkt und „sehr hoch" fünf Punkte.

Blatt „Schwachstellen"
Auf dem zweiten Blatt ist ein Katalog von möglichen Schwachstellen zu sehen. Diese stammen aus den Kategorien personelle, bauliche, organisatorische, technische Schwachstellen und IT-Schwachstellen. Auch hier ist wiederum eine Auswahl vorzunehmen, ob die Schwachstelle vorhanden ist oder nicht. Liegt die Schwachstelle vor, wird der Schwachstelle eine 2 zugeordnet, ist sie nicht vorhanden, wird die Schwachstelle mit 0 bewertet.

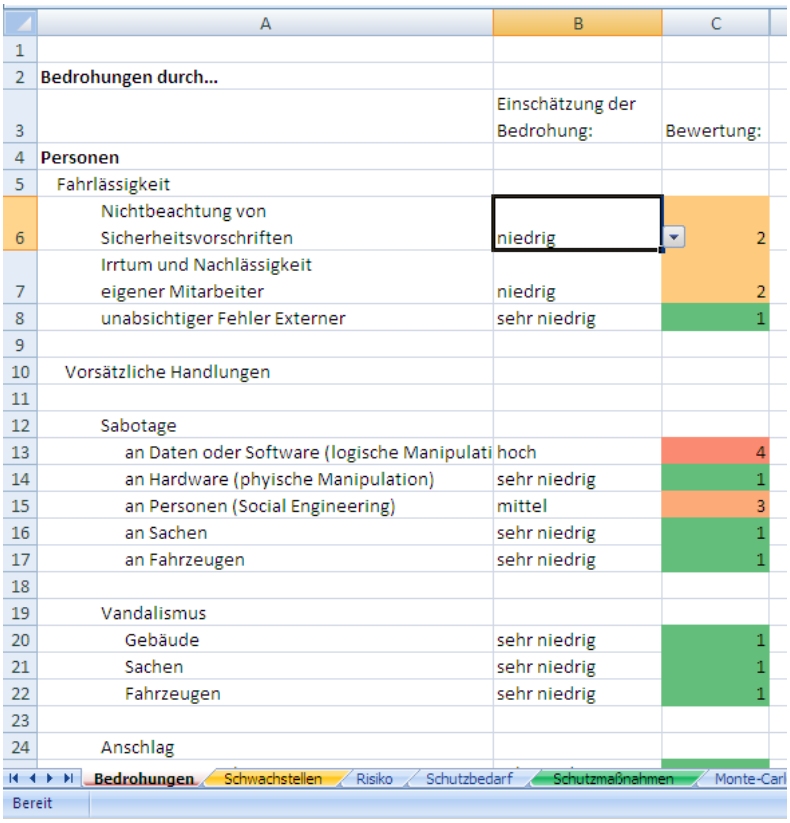
Da Bedrohungen alleine nicht zum Schaden führen, sondern Schwachstellen zum Angriff benötigen, wird die Beziehung zwischen Bedrohung und Schwachstelle berücksichtigt, indem jeder Wert einer Bedrohung mit dem Mittelwert der zugehörigen Schwachstellen multipliziert wird.

Blatt „Risiko"
Auf dem nächsten Blatt sind Angaben zu Schadenshäufigkeit und Schadenshöhe zu machen. Sind die absoluten Zahlen eingesetzt, wird durch das Anklicken des Pfeils die Berechnung der Gesamtverlustverteilung über eine Monte-Carlo-Simulation angestoßen, deren Rechnung sich auf dem Blatt Monte-Carlo befindet. Die Verteilung wird graphisch dargestellt. Der Value-at-Risk wird angegeben.

Blatt „Schutzbedarf"
Auf dem Blatt „Schutzbedarf" wird durch die Beantwortung von Fragen mit Ja/Nein der Schutzbedarf ermittelt und entsprechend angezeigt.

Blatt „Schutzmaßnahmen"
Das Blatt „Schutzmaßnahmen" weist aus verschiedenen Kategorien Schutzmaßnahmen auf. Hier ist keine Eingabe zu tätigen. Die Auswahl der Schutzmaßnahmen basiert auf den zuvor eingegebenen Bedrohungen und Schwachstellen. Durch eine Verknüpfung der Daten

aus Bedrohung und Schwachstelle werden die zugehörigen Schutzmaßnahmen mit einer Zahl versehen. Je höher diese ist, desto dringlicher ist die Einführung der Schutzmaßnahme.
Die Zahl für die Schutzmaßnahme generiert sich aus dem Produkt des Wertes der zugehörigen Schwachstelle und der zuvor ausgerechneten Kennzahl aus Schwachstelle und Bedrohung. Können mehrere Bedrohungen durch eine Schutzmaßnahme verkleinert werden, wird der Mittelwert gebildet und die Anzahl der Einflussfaktoren dazu addiert, um die Wichtigkeit der Maßnahme zu würdigen.



	A	B	C
1			
2	**Bedrohungen durch...**		
3		Einschätzung der Bedrohung:	Bewertung:
4	**Personen**		
5	Fahrlässigkeit		
6	Nichtbeachtung von Sicherheitsvorschriften	niedrig	2
7	Irrtum und Nachlässigkeit eigener Mitarbeiter	niedrig	2
8	unabsichtiger Fehler Externer	sehr niedrig	1
9			
10	Vorsätzliche Handlungen		
11			
12	Sabotage		
13	an Daten oder Software (logische Manipulati	hoch	4
14	an Hardware (phyische Manipulation)	sehr niedrig	1
15	an Personen (Social Engineering)	mittel	3
16	an Sachen	sehr niedrig	1
17	an Fahrzeugen	sehr niedrig	1
18			
19	Vandalismus		
20	Gebäude	sehr niedrig	1
21	Sachen	sehr niedrig	1
22	Fahrzeugen	sehr niedrig	1
23			
24	Anschlag		

Bedrohungen | Schwachstellen | Risiko | Schutzbedarf | Schutzmaßnahmen | Monte-Carl

Bereit

Abbildung 13: Excel-Tool Blatt Bedrohungen (eigene Darstellung)

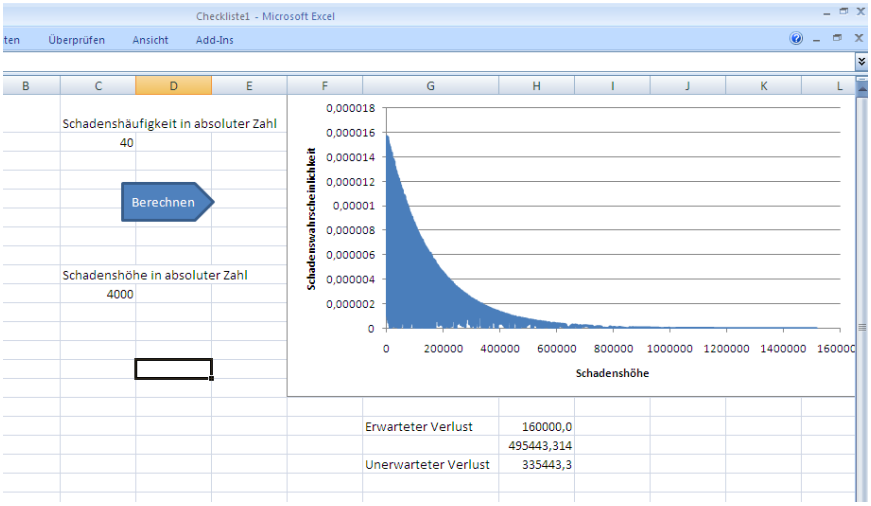


Abbildung 14: Excel-Tool Blatt Risiko (eigene Darstellung)

	A	B	C	D
1	**Schutzbedarfsfeststellung**			Wertung
2	**Verstoß gegen Gesetze/Vorschriften/Verträge**	**Bagatellverstöße** gegen Vorschriften und Gesetze		1
3		**Erheblicher** Verstoß gegen Vorschriften und Gesetze		2
4		**Fundamentaler** Verstoß gegen Vorschriften und Gesetze		4
5				
6	**Beeinträchtigung der persönlichen Unversehrtheit**	**Keine** Beeinträchtigung		1
7		Beeinträchtigungen der persönlichen Unversehrtheit sind **geringfügig** und unwahrscheinlich, aber nicht auszuschließen		2
8		Beeinträchtigungen der persönlichen Unversehrtheit sind gravierend. Es besteht **Gefahr für Leib und Leben**		4
9				
10	**Beeinträchtigung der Aufgabenerfüllung**	Die Beeinträchtigung würde von den Betroffenen als **tolerabel** eingeschätzt		1
11		Die Beeinträchtigung würde einzelnen Betroffenen als nicht-tolerabel eingeschätzt		2
12		Die Beeinträchtigung würde von allen Betroffenen als **nicht-tolerabel** eingeschätzt		4
13				
14	**Negative Außenwirkung**	Die Auswirkung bleibt lokal beschränkt		1
15		Breite Beeinträchtigung des Ansehens/Vertrauens		2
16		**Landes - bzw. bundesweite Ansehens- oder Vertrauensbeeinträchtigung**		4
17				
18	**Finanzielle Auswirkungen**	**Geringer** finanzieller Schaden		1
19		**Hoher** finanzieller Schaden		2
20		**Sehr hoher** finanzieller Schaden		4
21				
22			Ergebnis Schutzbedarf :	Sehr hoch
23				

Abbildung 15: Excel-Tool Blatt Schutzbedarf (eigene Darstellung)

	A	B	C
1	**Schutzmaßnahmen**		
2			
3	technische Maßnahmen		
4	Bereich Informationssicherheit		
5	Authentifizierung (Passwort, Biometrie, etc.)	16	
6	Autorisierung (Berechtigungen)	0	
7	Kryptographie (Verschlüsselungen, digitale Signatur)	0	
8	Firewalls	0	
9	Datensicherung (Backup	9	
10	Systemüberwachung (Virenscanner, Protokollierung)	16	
11	Sichere Netzwerkverbindungen (VPN)	16	
12			
13	nicht-technische Maßnahmen		
14	Maßnahmen im Bereich Personal		
15	Qualifizierung/Schulung	0	
16	Sensibilisierung	8	
17	Maßnahmen im Bereich Organisation		
18	Aufbauorganisatorisch		
19	Klare Verteilung von Aufgaben, Kompetenzen und Verantwortung	0	
20	Berechtigungskonzepte	0	
21	Prozesse vollständig definieren	0	
22			
23	Maßnahmen im Bereich Räume und Gebäude		
24	Zutrittsbarrieren		
25	Zutrittskontrollen	0	

Bedrohungen | Schwachstellen | Risiko | Schutzbedarf | **Schutzmaßnahmen**

Bereit

Abbildung 16: Excel-Tool Blatt Schutzmaßnahmen (eigene Darstellung)

4. Evaluation des Referenzmodells an Fallbeispielen

Im Anschluss an die Fertigstellung des Referenzmodells Sicherheit soll dieses nun an zwei Fallbeispielen aus verschiedenen Bereichen evaluiert werden. Dazu werden die einzelnen Phasen des Referenzmodells auf die einzelnen Beispiele angewendet und so Vorgehensmodelle mit konkreten Ergebnissen entwickelt. Die ausführlichen Ergebnisse des Excel-Tools für die jeweiligen Beispiele sind von den Autoren erhältlich.

4.1 Fallbeispiel 1: Videoüberwachung von öffentlichen Plätzen

Phase 1: Abgrenzung und Beschreibung des Szenarios

Sowohl bei öffentlichen Veranstaltungen, wie Konzerten und Sportveranstaltungen, oder auch bei stark besuchten öffentlichen Plätzen, z.B. Bahnhöfen und Fußgängerzonen, finden sich große Menschenmengen zusammen. Um die Sicherheit der Besucher zu gewährleisten und kriminellen Delikten vorzubeugen, müssen entsprechende Maßnahmen ergriffen werden.

Phase 2: Bedrohungen und Schwachstellen

Öffentliche Plätze und Veranstaltungen sind häufig Schauplätze von Straftaten. Besonders an Kriminalitätsbrennpunkten häufen sich Delikte wie Diebstahl, Raub, Körperverletzung, Vandalismus und Verstöße gegen das Betäubungsmittelgesetz.
Zur Identifikation von Bedrohungen und Schwachstellen wird ein Angriffsbaum modelliert:[86]

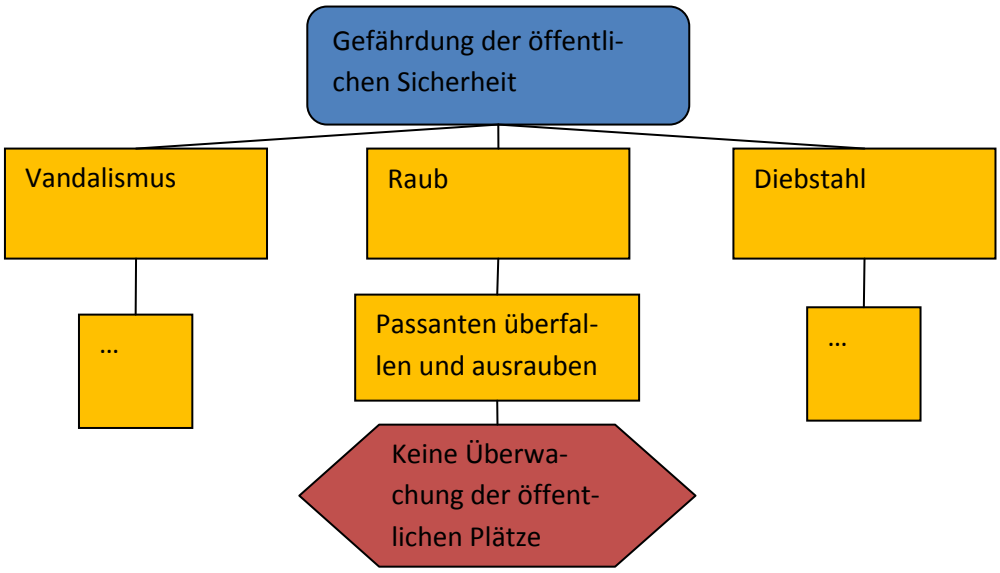


Abbildung 17: Angriffsbaum Beispiel Videoüberwachung A

Wie die Analyse durch den Angriffsbaum zeigt, ist eine mögliche Schwachstelle, die die Sicherheit auf öffentlichen Plätzen gefährdet, die Abwesenheit von Überwachung. Dies kann in Form von physischer Überwachung durch die Polizei oder auch durch Videoüberwachung sein.

Ergebnis Excel-Tool:
Bedrohungen:

[86] Eigene Darstellung

Sabotage an Sachen, Fahrzeugen
Vandalismus gegen Gebäude, Sachen und Fahrzeuge
Anschlag gegen Menschen, Gebäude, Infrastruktur und Fahrzeuge
Diebstahl, Raub, Körperverletzung

Schwachstellen:
Keine Überwachung
Keine Videoüberwachung
Keine Zugangsbarrieren
Keine Alarmanlage

Quantifizierung:
Schadenshöhe und Schadenshäufigkeit werden anhand eines konkreten Beispiels von der Polizei aus Leipzig berechnet, wobei die durchschnittliche Schadenshöhe geschätzt wird.[87]

Schadenshäufigkeit: 496 Diebstähle/Beschädigung an PKWs im Jahr
Nach Einführung der Videoüberwachung 197 Delikte
Schadenshöhe: 1000 € pro Delikt (geschätzt)

Erwartete Verlust: 496.000 €
Maximal erwartetes Verlustpotential: 1.448.816,4 €
Value-at-Risk: 952.816,4 €

ROSI 1. Periode: 199.000 €

Phase 3: Schutzbedarf
Das Ergebnis für den Schutzbedarf ist „sehr hoch". Dies ist darauf zurückzuführen, dass ein fundamentaler Verstoß gegen Gesetze vorliegt, eine Gefahr für Leib und Leben zu erwarten ist und ein sehr hoher finanzieller Schaden entstehen kann.

Ergebnis Excel-Tool
Sehr hoch

Phase 4: Schutzmaßnahmen
Geeignete Schutzmaßnahmen sind für diesen Bereich eine stärkere Überwachung der öffentlichen Plätze. Neben der physischen Überwachung durch verstärkten Polizeieinsatz in den Kriminalitätsbrennpunkten ist vor allem die Videoüberwachung als Mittel zur Prävention und zur besseren Aufklärung von Delikten geeignet.

Ergebnis Excel-Tool:
Zutrittskontrollen
Sicherheitstüren
Vergitterte Fenster
Zäune
Einbruchmeldesysteme
Überwachung
Videoüberwachung

[87] Vgl. Müller, R., S. 6ff.

4.2 Fallbeispiel 2: Sicherstellung der Wasserversorgung

Phase 1: Abgrenzung und Beschreibung des Szenarios

Wasser ist die Grundlage allen Lebens auf der Erde. Allerdings sind nur 0,3 % der weltweiten Wasservorräte als Trinkwasser geeignet und so stellt die Wasserversorgung nicht nur Entwicklungsländer vor eine logistische Herausforderung. Gebiete ohne ausreichende Trinkwasservorkommen müssen z.B. über die Fernwasserversorgung mit Wasser beliefert werden.
Aufgrund des lebensnotwendigen Charakters von Wasser ist die Sicherstellung der Trinkwasserversorgung von größter Bedeutung. Dies betrifft zum einen die Qualität des Wassers und zum anderen den sicheren Transport von der Quelle zum Endverbraucher. Für das Fallbeispiel wurde ein Gespräch mit einem Mitarbeiter der Harzwasserwerke aus dem Wasserwerk Granetalsperre geführt.

Phase 2: Bedrohungen und Schwachstellen

Modellierung des Angriffsbaums:[88]

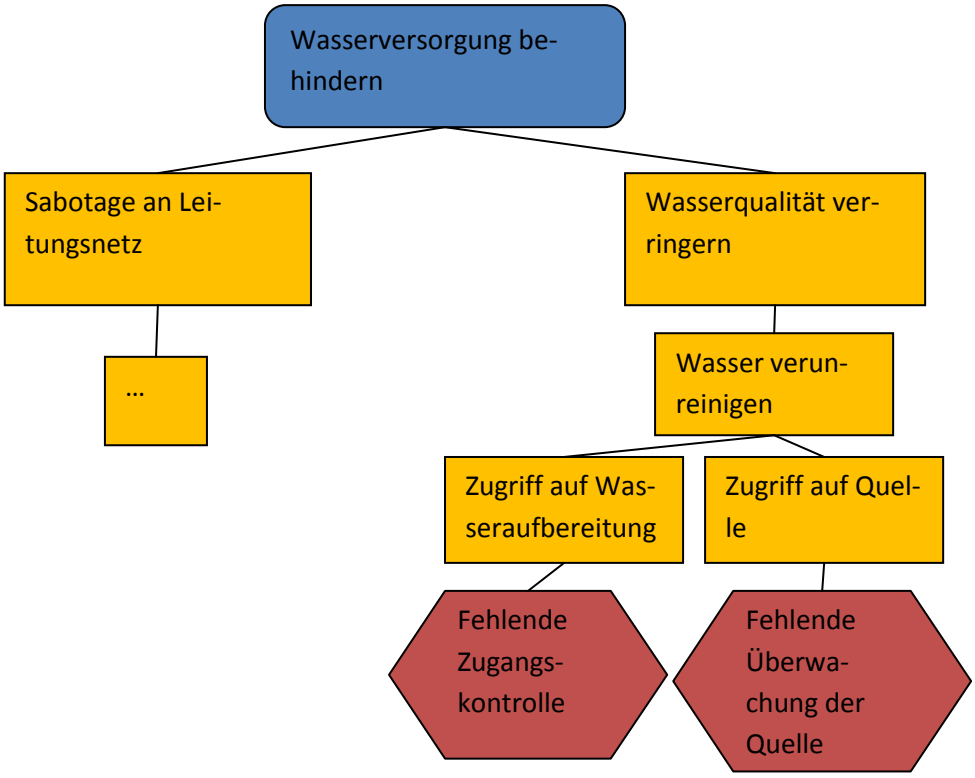


Abbildung 18: Angriffsbaum Fallbeispiel Wasser

Die Wasserversorgung kann sowohl durch die Verunreinigung des Wassers als auch durch die Störung des Leitungsnetzes bedroht werden. Der Angriffsbaum zeigt, dass eine Schwachstelle für die Wasserverunreinigung zum einen die Quelle des Wassers an sich sein kann. So wäre es denkbar, dass eine Talsperre durch das Hineingeben eines Giftes verunreinigt wird und das Wasser nicht mehr trinkbar wäre. Allerdings ist hier zu beachten, dass aufgrund der großen Wassermenge der Talsperre eine sehr große Menge an Gift notwendig wäre (Verdünnungseffekt). Eine weitere Schwachstelle ist die Trinkwasserauf-

[88] Eigene Darstellung

bereitung selbst. Hier wäre eine Verunreinigung durch Zusetzen eines Giftstoffes in die Aufbereitungsbecken denkbar.
Außerdem ist auch eine Vergiftung des Wassers über die Hydranten möglich, da diese öffentlich zugänglich sind. Hier wäre es möglich, einen Giftstoff in das Leitungsnetz zu pumpen.

Ergebnis Excel-Tool:
Bedrohungen:
Nichtbeachtung von Sicherheitsvorschriften
Sabotage an Sachen
Anschlag gegen Menschen, Gebäude, Infrastruktur
Fehlende Berechtigungen, Zutrittsbeschränkungen
Wasser verunreinigen an der Quelle
Wasser verunreinigen im Wasserwerk
Wasser im Leitungsnetz verunreinigen

Schwachstellen:
Personal hat ein mangelndes Sicherheitsbewusstsein
Personal lässt mangelnde Sorgfalt bei Sicherheitsmaßnahmen walten
Personal weist mangelnde Akzeptanz bei den Sicherheitsvorschriften auf"
Das zu sichernde Gelände wird nicht überwacht
Das zu sichernde Gelände wird nicht videoüberwacht
Die Bausubstanz hält Anschlägen nicht stand
Zugangsbarrieren zu sicherheitsrelevanten Bereichen sind nicht vorhanden
Keine Zutrittsberechtigungen
Keine Überprüfung der Wasserqualität
Keine Überwachung der Quelle
Keine Überwachung des Wasserwerks
Öffentliche Zugänge zum Versorgungsnetz

Phase 3: Schutzbedarf.
Ergebnis Excel Tool:
Sehr hoch

Phase 4: Schutzmaßnahmen:
Um das Eindringen von Fremden in das Wasserwerk Granetalsperre zu verhindern, werden einige Schutzmaßnahmen ergriffen. Zum einen sind alle Türen und Fenster, die in das Gebäude führen alarmgesichert. Der Zutritt durch den Haupteingang ist von außen nicht ohne Klingeln und Identifikation möglich.
Das erste Messinstrument sind heimische Fische, die in einem mit Rohwasser aus der Talsperre gefüllten Aquarium leben. Dieses Rohwasser wird kontinuierlich durch frisches Talsperrenwasser ausgetauscht. Sollten die sensiblen Fische sich nicht normal verhalten, wäre dies also schon ein erster Hinweis auf eine Veränderung des Wassers.
Des Weiteren werden öffentliche Bereiche wie der Ausstellungsraum durch Videokameras überwacht.
Um die Wasserqualität zu gewährleisten, wird im Wasserwerk das Wasser laufend durch Messgeräte überprüft, die die Ergebnisse an die angeschlossenen Computersysteme weiterleiten.

Die Schwachstelle der Hydranten kann durch keine Schutzmaßnahme gelöst werden, da diese jederzeit für die Feuerwehr im Falle eines Notfalls zugänglich sein müssen.

Ergebnis Excel-Tool:
Qualifizierung/Sensibilisierung Personal
Berechtigungskonzepte
Zutrittsbarrieren
Videoüberwachung/Bewachung
Sensoren/Detektoren zur Messung der Wasserqualität
Schutzgebiete um die Quelle herum aufbauen
Zugänge zu Hydranten erschweren

Quantifizierung
Eine Quantifizierung ist nicht möglich

5. Standards, Zertifizierungen und Gütesiegel

Um eine objektive Beurteilung der Sicherheit zu gewährleisten, werden Zertifizierungsrichtlinien geschaffen, die der Qualitätssicherung dienen. „Durch ein Zertifikat werden bestimmte Eigenschaften eines Objekts verifiziert und das Objekt wird einer bestimmten Sicherheitsstufe zugeordnet".[89]
Die Etablierung eines Sicherheitsmanagements ist eine komplexe Aufgabe, bei der Planungsfehler und unpraktikable Umsetzungen vermieden werden müssen. Eigene Vorgehensweisen sind meist sehr teuer und weisen erfahrungsgemäß Lücken auf. Daher bietet sich der Einsatz von standardisierten Vorgehensweisen an.
Die Ziele beim Einsatz von Standards lassen sich in drei Kategorien einteilen:[90]
Kosteneinsparung, Einführung eines angemessenen Sicherheitsniveaus und Wettbewerbsvorteile.

Einige Standards können als Grundlage für eine Zertifizierung herangezogen werden. „Ein Zertifikat ist eine unabhängige Bestätigung dafür, dass alle (soweit anwendbare) im Standard geforderten Sicherheitsmaßnahmen zum Zeitpunkt der Zertifizierung dokumentiert und tatsächlich umgesetzt sind. Durch die Ausstellung eines Zertifikates, mit dem die Umsetzung des Standards bestätigt wird, kann dies Dritten transparent gemacht werden. Dritte können hierbei Kunden, Banken, Versicherungen oder auch die Öffentlichkeit sein."[91]

Im Folgenden werden einige wichtige Standards und Zertifizierungen vorgestellt.

5.1 ISO/IEC 27001

Die ISO/IEC 27001 ist der grundlegende Standard für ein Informationssicherheits-Managementsystem (ISMS). Sie basiert auf dem 2. Teil des britischen Standards BS 7799-2 und beschreibt die Anforderungen an das Informationssicherheits-Management, welches mittelbar auf die Informationssicherheit wirkt. Hierbei ist zu bemerken, dass die Norm auf

[89] Hoppe/Prieß, S. 301.
[90] BITKOM, S. 8.
[91] BITKOM, S. 19.

alle Arten von Organisationen anwendbar sein soll und so die Anforderungen einen niedrigen technischen Detaillierungsgrad aufweisen.[92]

Die Gesamtheit aller Aktivitäten, ein ISMS einzuführen, wird als Prozess betrachtet. Dieser lässt sich gut beherrschen, wenn man einen bestimmten Zyklus von Aktivitäten auf ihn anwendet. Dies wird methodisch durch das PDCA-Modell gelöst. Der Zyklus beinhaltet vier Aktivtäten, PLAN, DO, CHECK und ACT. Sie stellen eine sich wiederholende, zyklische Folge von Aktivitäten dar, die solange angewandt wird, wie das ISMS betrieben wird. In der Phase PLAN wird das ISMS geplant, in der Phase DO wird das ISMS umgesetzt und betrieben, in der Phase CHECK wird das ISMS überwacht und überprüft und in der Phase ACT wird das ISMS instandgehalten und evtl. verbessert, um es an die veränderte Umwelt anzupassen.[93]

Die ISO/IEC 27001 ist von der Methodik eng an die Norm ISO 9000 angelehnt und kann daher als ein Qualitätsstandard für Managementsysteme bzgl. ihrer Informationssicherheit angesehen werden.[94]

Eine Zertifizierung kann durch akkreditierte Unternehmen erfolgen. Hierbei können neben dem gesamten Unternehmen auch nur einzelne Bereiche zertifiziert werden.[95]

5.2 IT-Grundschutz

Vom Bundesministerium für Informationssicherheit werden seit 1994 IT-Sicherheitsmaßnahmen aus den technischen und nicht-technischen Bereichen dargestellt und Anforderungen an das Sicherheitsmanagement beschrieben. Seit 2006 hat sich der sogenannte IT-Grundschutz an die ISO 27001 angenähert, wobei weiterhin die Gefährdungs- und Maßnahmenkataloge verfügbar sind.[96]
Dieser Schritt stellt in gewisser Weise eine Synthese aus Grundschutz und ISO/IEC 27001 dar. Die ISO/IEC 27001 gibt vor, welche Elemente ein ISMS enthalten muss und welche Anforderungen an das Management der IT-Sicherheit gestellt werden, ohne jedoch auf detaillierte Prozesse und zu wählende Sicherheitsmaßnahmen einzugehen. Hier greift dann der IT-Grundschutz ein und gibt für seinen Bereich Vorgehensweisen und Maßnahmen vor.[97]
Eine ISO/IEC 27001-Zertifizierung kann auf Basis des IT-Grundschutzes beantragt werden.

5.3 ISO 9001

Die ISO 9001 ist eine international gültige Norm, die die Anforderungen an ein Qualitätsmanagementsystem festlegt. Sie ist eine zwingende Norm und beschreibt jene Prozesse, die nötig sind, um die Kundenanforderungen zu erfüllen. Sie stellt somit einen Mindeststandard zum Qualitätsmanagement in einer Organisation dar.

---

[92] Vgl. BITKOM, S. 22.
[93] Vgl. Kersten/Reuter/Schröder, S. 37f.
[94] Vgl. ISO 27001 Security Online: What is ISO 27001?
[95] Vgl. BITKOM, S. 22.
[96] Kersten/Reuter/Schröder, S. VIII.
[97] Vgl. Kersten/Reuter/Schröder, S. VII.

Wie die ISO 27001 basiert die ISO 9001 auf dem zyklischen PCDA-Modell.

Durch die Prozessorientierung der ISO 9001 eignet sie sich als Grundlage zur Integration verschiedener Managementsysteme, z.B. der ISO/IEC 27001. Die Prozesslandschaft würde wiederum im Mittelpunkt stehen und könnte um weitere Prozesse erweitert werden.[98]

5.4 Gütesiegel

Für Online-Shops existieren eine Reihe von Gütesiegeln, die eine Schlüsselinformation oder Qualitätssignale für den Verbraucher darstellen. Sie bündeln wichtige Informationen über die Leistungen und Qualität und sollen so den Verbraucher von der Informationssuche befreien.

Eine Definition für das Internet-Gütesiegel liefert Rüdiger:

„Internet-Gütesiegel sind im Rahmen einer Selbstregulierung von einer unabhängigen Institution herausgegebene Wort- und/oder Bildzeichen, die Online-Händler zur Kennzeichnung auf ihren Webseiten einsetzen und die gegenüber den Kunden bzw. potentiellen Kunden in verdichteter Form darüber Auskunft geben, dass der betreffende Online-Händler die vom Zeichengeber (in Form von Verhaltenskodizes, Kriterienkatalogen, Normen, Leitfäden o. Ä.) festgelegten Kriterien/(Qualitäts-)Anforderungen bezüglich seiner Geschäftspraktiken insbesondere im Hinblick auf die Informations-Privatheit, die IT-Sicherheit und den Verbraucherschutz einhält."[99]

Die Kriterien basieren neben europäischen und deutschen Gesetzen auch auf Empfehlungen von Verbraucherschützern. Sie verfolgen das Ziel, den Kunden des Online-Shops vor den typischen Risiken des Internetkaufs, z.B. Verstöße gegen Datenschutzbestimmungen, intransparente Preisangaben oder Einschränkungen des Widerrufsrechts zu schützen.[100]

6. Fazit und Ausblick

Sicherheit erlangt einen immer höher werdenden Stellenwert. Angesichts der Komplexität der Erstellung von Sicherheitskonzepten ist es sinnvoll, ein Referenzmodell zu entwickeln, das auf möglichst viele Situationen und Szenarien anwendbar ist.
Zu diesem Zweck wurde ausgehend von den Überlegungen von Prof. Dr. Breitner und seinen Mitarbeitern ein Modell entwickelt, welches sich durch abgrenzbare Phasen auszeichnet.
Als erste Phase des Modells ist die Szenariobeschreibung und –abgrenzung identifiziert worden. Darauf aufbauend lassen sich Bedrohungen, Schwachstellen und Risiken identifizieren. In diesem Aufsatz geschieht dies über Angriffsbäume und Fragenkataloge. Die Quantifizierung der Risiken, sofern möglich, erfolgt über das Value-at-Risk Risikomaß in Verbindung mit einer Monte-Carlo-Simulation. Diese Methode wurde gewählt, da sie neben der leichten Verständlichkeit anschauliche Ergebnisse liefert.
Aufbauend auf der Risikoanalyse lässt sich der Schutzbedarf bestimmen, um in der letzten Phase die geeigneten Schutzmaßnahmen auszuwählen und zu implementieren. Die Aus-

[98] Vgl. Wagner, S. 110.
[99] Rüdiger, S. 6
[100] Vgl. www.trustedshops.de

wahl der Schutzmaßnahmen ist vor allem auf den Schutzbedarf auszurichten, da die Wirtschaftlichkeit der Maßnahmen eine große Rolle spielt. Auch die Akzeptanz der Maßnahmen darf nicht vernachlässigt werden, um sicherzustellen, dass die Maßnahmen insgesamt zu einem positiven Ergebnis führen und ruinöse Schäden vermieden werden.

Die Anwendung des Referenzmodells und Excel-Tools an den Fallbeispielen, zeigt die gute Einsetzbarkeit des Modells in vielfältigen Situationen. Allerdings ist zu beachten, dass durch den Charakter eines Fragenkatalogs nur bereits bekannte Bedrohungen, Schwachstellen und Schutzmaßnahmen zur Verfügung stehen. Deshalb ist eine ständige Weiterentwicklung und Erweiterung der Fragenkataloge notwendig.

Des Weiteren wurde deutlich, dass die Quantifizierung der Risiken teilweise nur sehr schwer möglich ist, da manche Risiken nicht zu quantifizieren sind, z.B. Menschenleben. Zertifizierungen und Gütesiegel sind erforderlich, um die Vergleichbarkeit der Sicherheitskonzepte zu gewährleisten, die Objektivität zu erhöhen und das Vertrauen in die Systeme zu stärken. Durch die Ergebnisse der Experteninterviews wurde deutlich, dass auch andere Wissenschaften das Modell als Grundlage akzeptieren. Allerdings wurde angemerkt, dass sich die Ingenieurwissenschaften naturgemäß vor allem auf die technische Umsetzung der Schutzmaßnahmen konzentrieren.

Schlussendlich ist zu bemerken, dass das Referenzmodell nicht als final zu betrachten ist. Es muss vielmehr als ein wiederkehrender Kreislauf verstanden werden, da auch die Umwelt sich fortlaufend ändert und weiterentwickelt. Ständig entstehen durch den technischen Fortschritt neue Bedrohungen und lassen Schwachstellen relevant werden, die vorher als nicht bedeutsam eingestuft worden sind. Auch werden durch die Weiterentwicklung neue Schutzmaßnahmen möglich, die wiederum andere obsolet werden lassen.

7. Literaturverzeichnis

1. Alexander, C. (2003a): Managing Operational Risks with Bayesian Networks. In: Alexander, C.: Operational Risk; Regulation, Analysis and Management. London et al., S. 285-295, 2003.
2. Basler Ausschuss für Bankenaufsicht : Internationale Konvergenz der Eigenkapitalmessung und der Eigenkapitalanforderungen. http://www.bis.org/publ/bcbs107ger.pdf, abgerufen am 10.12.2008.
3. BITKOM: Kompass der IT-Sicherheitsstandards: Leitfaden und Nachschlagewerk, 2007, http://www.bitkom.org/files/documents/Kompass_der_IT_Sicherheitstandards_final_12_11_2007.pdf, abgerufen am 05.12.2008.
4. Bundesamt für Sicherheit in der Informationstechnik (BSI (A)): http://www.bsi.bund.de/gshb/deutsch/hilfmi/check/04pc_f.pdf, abgerufen am 12.11.2008.
5. Bundesministerium für Sicherheit in der Informationstechnik(BSI (B)): Fragenkatalog Organisation - Revision Stufe 3 http://www.bsi.de/gshb/deutsch/hilfmi/archiv/24_org3.pdf, abgerufen am 10.11.2008.
6. Bundesamt für Sicherheit in der Informationstechnik (BSI (C)): G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen, http://www.bsi.de/gshb/deutsch/g/g03003.htm, abgerufen am 20.10. 2008.
7. Chavez-Demoulin, V./ Embrechts, P.: Advanced extremal models for operational risk. http://www.math.ethz.ch/%7Ebaltes/ftp/opriskevt.pdf, abgerufen am 25.10.2008.
8. Cruz, M.G.: Modeling, Measuring and Hedging Operational Risk. Chichester, 2003.
9. Faisst, U. / Kovacs, M.: Quantifizierung operationelle Risiken - Ein Methodenvergleich. In: Die Bank, Heft 5, S. 342-349, 2003.
10. Geiger, W. / Kotte, W.: Handbuch Qualität. Wiesbaden, 2008.
11. Haubenstock, M. / Hardin, L.: The Loss Distrubution Approach. In: Alexander, C.: Operational Risk: Regulation, Analysis and Management. London et al., S. 171-190, 2003.
12. Hölscher, R. / Kalhöfer, C. / Bonn, R.: Die Bewertung operationeller Risiken in Kreditinstituten. In: FINANZ BETRIEB, Heft 7-8, S. 490-504, 2005.

13. ISO 27001 Security: http://www.27001-online.com, abgerufen am 10.12.2008.
14. IT-Lexikon: http://www.itwissen.info/definition/lexikon/Bedrohung-threat.html, abgerufen am 30.09.2008.
15. Kersten, H., / Reuter, J., / Schröder, K.W.: IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz – Der Weg zur Zertifizierung. Wiesbaden, 2008.
16. Königs, H.-P.: IT-Risikomanagement mit System. Wiesbaden, 2006.
17. Lassmann, W.: Wirtschaftsinformatik – Nachschlagewerk für Studium und Praxis. Wiesbaden, 2006.
18. Laudon, K.C., Laudon, J.P., Schoder, D.: Wirtschaftsinformatik – Eine Einführung. München, 2006.
19. Meyers Lexikon: Öffentlicher Raum. http://lexikon.meyers.de/wissen/öffentlicher+Raum, abgerufen am 30.09.2008.
20. Müller, K.-R.: IT-Sicherheit mit System – Sicherheitspyramide – Sicherheits-, Kontinuitäts- und Risikomanagement – Normen und Practices – SOA und Softwareentwicklung. Wiesbaden, 2008.
21. Oehler, A. / Unser, M.: Finanzwirtschaftliches Risikomanagement. Berlin, 2002.
22. Piaz, J.-M.: Operational Risk Management bei Banken. Zürich, 2002.
23. Pohlmann, N.: Wie wirtschaftlich sind IT-Sicherheitsmaßnahmen? In Kosten & Nutzen von IT-Sicherheit Heft 248, S. 26-34, 2006.
24. Pohlmann, N. / Blumberg, H.F.: Der IT-Sicherheitsleitfaden. Bonn, 2004.
25. Prokein, O.: IT-Risikomanagement – Identifikation, Quantifizierung und wirtschaftliche Steuerung. Wiesbaden, 2008.
26. Raepple, M.: Sicherheitskonzepte für das Internet – Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung. Heidelberg, 2001.
27. Rau-Medrow, H.: Value at Risk, Expected Shortfall, and Marginal Risk Contribution. 2002, http://www.bwl.uni-wuerzburg.de/fileadmin/12020000/_temp_/Value.pdf, abgerufen am 05.10.2008.
28. Romeike, F.: Risikoidentifikation und Risikokategorien. In: Romeike, F. / Finke, R. B.: Erfolgsfaktor Risiko-Management. Wiesbaden, S. 165-180, 2004.
29. Rommelfanger, H.: Stand der Wissenschaft bei der Aggregation von Risiken, in: Risikoaggregation in der Praxis, Heidelberg, S.15-47, 2008.
30. Rüdiger, K.: Internet-Gütesiegel in Spanien. In: Datenschutz und Datensicherheit, Volume 31 Nummer 6,. Wiesbaden, S.416-421, 2007.
31. Schadt, D.: Über die Ökonomie der IT-Sicherheit. In Kosten & Nutzen von IT-Sicherheit Heft 248, S. 16-25, 2006.
32. Schmid, F., Trede, M.: Finanzmarktstatistik. Heidelberg, 2006.
33. Schmidt, K.: Der IT-Security-Manager. München, 2006.
34. Schneier, B.: Secret & Lies: IT-Sicherheit in der vernetzten Welt. Heidelberg, 2001.
35. Seibold, H.: IT-Risikomanagement. München, 2006.
36. Trusted Shops: Anlage TS-QAL. http://www.trustedshops.de/shopbetreiber/pdf_download/TS-QAL.pdf , abgerufen am 05.12.2008.
37. Vaughan, E.J.: Risk Management. New York, 1997.
38. Wagner, K.W.: PQM – Prozessorientiertes Qualitätsmanagement: Leitfaden der ISO 9001:2000. München, 2003.
39. Wikipedia Enzyklopädie: FMEA. http://de.wikipedia.org/wiki/FMEA, abgerufen am 11.12.2008.
40. Witt, B.C.: IT-Sicherheit kompakt und verständlich: Eine praxisorientierte Einführung. Wiesbaden, 2006.

IWI Discussion Paper Series/Diskussionsbeiträge

ISSN 1612-3646

Michael H. Breitner, *Rufus Philip Isaacs and the Early Years of Differential Games,* 36 p., #1, January 22, 2003.

Gabriela Hoppe and Michael H. Breitner, *Classification and Sustainability Analysis of e-Learning Applications*, 26 p., #2, February 13, 2003.

Tobias Brüggemann und Michael H. Breitner, *Preisvergleichsdienste: Alternative Konzepte und Geschäftsmodelle*, 22 S., #3, 14. Februar, 2003.

Patrick Bartels and Michael H. Breitner, *Automatic Extraction of Derivative Prices from Webpages using a Software Agent,* 32 p., #4, May 20, 2003.

Michael H. Breitner and Oliver Kubertin, *WARRANT-PRO-2: A GUI-Software for Easy Evaluation, Design and Visualization of European Double-Barrier Options,* 35 p., #5, September 12, 2003.

Dorothée Bott, Gabriela Hoppe und Michael H. Breitner, *Nutzenanalyse im Rahmen der Evaluation von E-Learning Szenarien*, 14 S., #6, 21. Oktober, 2003.

Gabriela Hoppe and Michael H. Breitner, *Sustainable Business Models for E-Learning*, 20 p., #7, January 5, 2004.

Heiko Genath, Tobias Brüggemann und Michael H. Breitner, *Preisvergleichsdienste im internationalen Vergleich*, 40 S., #8, 21. Juni, 2004.

Dennis Bode und Michael H. Breitner, *Neues digitales BOS-Netz für Deutschland: Analyse der Probleme und mögliche Betriebskonzepte,* 21 S., #9, 5. Juli, 2004.

Caroline Neufert und Michael H. Breitner, *Mit Zertifizierungen in eine sicherere Informationsgesellschaft*, 19 S., #10, 5. Juli, 2004.

Marcel Heese, Günter Wohlers and Michael H. Breitner, *Privacy Protection against RFID Spying: Challenges and Countermeasures*, 22 p., #11, July 5, 2004.

Liina Stotz, Gabriela Hoppe und Michael H. Breitner, *Interaktives Mobile(M)-Learning auf kleinen End-geräten wie PDAs und Smartphones*, 31 S., #12, 18. August, 2004.

Frank Köller und Michael H. Breitner, *Optimierung von Warteschlangensystemen in Call Centern auf Basis von Kennzahlenapproximationen,* 24 S., #13, 10. Januar, 2005.

Phillip Maske, Patrick Bartels and Michael H. Breitner, *Interactive M(obile)-Learning with UbiLearn 0.2*, 21 p., #14, April 20, 2005.

Robert Pomes and Michael H. Breitner, *Strategic Management of Information Security in State-run Organizations,* 18 p., #15, May 5, 2005.

Simon König, Frank Köller and Michael H. Breitner, *FAUN 1.1 User Manual,* 134 p., #16, August 4, 2005.

Christian von Spreckelsen, Patrick Bartels und Michael H. Breitner, *Geschäftsprozessorientierte Analyse und Bewertung der Potentiale des Nomadic Computing,* 38 S., #17, 14. Dezember, 2006.

Stefan Hoyer, Robert Pomes, Günter Wohlers und Michael H. Breitner, *Kritische Erfolgsfaktoren für ein Computer Emergency Response Team (CERT) am Beispiel CERT-Niedersachsen,* 56 S., #18, 14. Dezember, 2006.

Christian Zietz, Karsten Sohns und Michael H. Breitner, Konvergenz von Lern-, Wissens- und Personalmanagementssystemen: Anforderungen an Instrumente für integrierte Systeme, 15 S., #19, 14. Dezember, 2006.

Christian Zietz und Michael H. Breitner, *Expertenbefragung „Portalbasiertes Wissensmanagement": Ausgewählte Ergebnisse*, 30 S., #20, 5. Februar, 2008.

IWI Discussion Paper Series/Diskussionsbeiträge

ISSN 1612-3646

Harald Schömburg und Michael H. Breitner, *Elektronische Rechnungsstellung: Prozesse, Einsparpotentiale und kritische Erfolgsfaktoren*, 36 S., #21, 5. Februar, 2008.

Halyna Zakhariya, Frank Köller und Michael H. Breitner, *Personaleinsatzplanung im Echtzeitbetrieb in Call Centern mit Künstlichen Neuronalen Netzen*, 35 S., #22, 5. Februar, 2008.

Jörg Uffen, Robert Pomes, Claudia M. König und Michael H. Breitner, *Entwicklung von Security Awareness Konzepten unter Berücksichtigung ausgewählter Menschenbilder*, 14 S., #23, 5. Mai, 2008.

Johanna Mählmann, Michael H. Breitner und Klaus-Werner Hartmann, *Konzept eines Centers der Informationslogistik im Kontext der Industrialisierung von Finanzdienstleistungen*, 19 S., #24, 5. Mai, 2008.

Jon Sprenger, Christian Zietz und Michael H. Breitner, *Kritische Erfolgsfaktoren für die Einführung und Nutzung von Portalen zum Wissensmanagement*, 44 S., #25, 20. August, 2008.

Finn Breuer und Michael H. Breitner, *„Aufzeichnung und Podcasting akademischer Veranstaltungen in der Region D-A-CH": Ausgewählte Ergebnisse und Benchmark einer Expertenbefragung*, 30 S. #26, 21. August, 2008.

Harald Schömburg, Gerrit Hoppen und Michael H. Breitner, *Expertenbefragung zur Rechnungseingangsbearbeitung: Status quo und Akzeptanz der elektronischen Rechnung*, 40 S., #27, 15. Oktober 2008

Hans-Jörg von Mettenheim, Matthias Paul und Michael H. Breitner, *Akzeptanz von Sicherheitsmaßnahmen: Modellierung, Numerische Simulation und Optimierung,* 30 S., #28, 16. Okotber 2008

Markus Neumann, Bernd Hohler und Michael H. Breitner, *Bestimmung der IT-Effektivität und IT-Effizienz serviceorientierten IT-Managements,* 20 S., #29, 30. November 2008

Matthias Kehlenbeck und Michael H. Breitner, *Strukturierte Literaturrecherche und -klassifizierung zu den Forschungsgebieten Business Intelligence und Data Warehousing,* 10 S. #30, 19. Dezember 2009

Michael H. Breitner, Matthias Kehlenbeck, Marc Klages, Harald Schömburg, Jon Sprenger, Jos Töller und Halyna Zakhariya, *Aspekte der Wirtschaftsinformatikforschung 2008,* 128 S., #31, 12. Februar 2009