Klaus **SCHMIDT**

2. Auflage

IT SECURITY MANAGEN

HANSER

Schmidt

IT Security managen

Klaus Schmidt

IT Security managen

2., überarbeitete Auflage

HANSER

Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Lektorat: Brigitte Bauer-Schiewek
Copy editing: Jürgen Dubau, Freiburg/Elbe
Umschlagdesign: Marc Müller-Bremer, München, www.rebranding.de
Umschlagrealisation: Max Kostopoulos
Titelmotiv: © stock.adobe.com/dnd_project
Satz: Eberl & Koesel Studio, Kempten
Druck und Bindung: Hubert & Co. GmbH & Co. KG BuchPartner, Göttingen
Printed in Germany

Print-ISBN: 978-3-446-47759-9
E-Book-ISBN: 978-3-446-47822-0
E-Pub-ISBN: 978-3-446-48168-8

Inhalt

Vorwort

Die Zeiten sind längst vergangen, in denen Unternehmen von der Notwendigkeit der Informationssicherheit überzeugt werden mussten. Spektakuläre Sicherheitsvorfälle wie Nutzerdatendiebstähle im großen Stil oder empfindliche Betriebsunterbrechungen durch IT-Angriffe haben in den Unternehmen ein Bewusstsein für die Verletzlichkeit der Informationsverarbeitung und damit letztendlich auch der Geschäftstätigkeit geschaffen.

Die Erfahrung zeigt, dass die auf Informationen und die Informationstechnik bezogenen Bedrohungen vielfältig sind. Neben den Angriffen von außen, verübt von Hackern, Cyberkriminellen oder gar Geheimdiensten, sind es vor allem die Angriffe von innen, die, ausgestattet mit einem umfangreichen Wissen über das Unternehmen, durch Ausspähung und Diebstahl von unternehmenswichtigen Daten oder Sabotage dem Unternehmen schaden können. Solche Schadensfälle werden aufgrund der Imageschädigung in der Regel nicht publik gemacht.

Aber auch ohne Vorsatz existieren Informationsrisiken, zum Beispiel durch menschliche Schwächen wie Naivität oder Fehlbedienungen oder durch Elementargefahren wie Brände, Überflutungen oder Blitzschlag.

Die Unternehmen haben die Notwendigkeit und Wichtigkeit der IT-Sicherheit erkannt und mitunter umfangreiche IT-Sicherheitslösungen im Einsatz. Doch mit technischen Maßnahmen allein ist es nicht getan. Für die Planung, die Koordinierung, den Einsatz und die Kontrolle solcher Lösungen und für das weite Feld der organisatorischen Maßnahmen ist das Sicherheitsmanagement von großer Bedeutung.

Das vorliegende Buch soll Personen, die in das Thema Informationssicherheit einsteigen, das notwendige Wissen vermitteln, um im Management dieses Themas erfolgreich zu sein. Aber auch „alte Hasen“ und Personen aus anderen Sicherheitsbereichen werden nützliche Dinge in diesem Buch finden. Bewusst konzentriert sich das Buch auf die organisatorischen und methodischen Aspekte der IT-Sicherheit und

nicht auf die technische Behandlung des Themas. Hierfür wird die Perspektive der für das IT-Sicherheitsmanagement verantwortlichen Person eingenommen. Alle Geschlechter sind dabei gleichberechtigt angesprochen, auch wenn zur Erhaltung der Lesbarkeit an einigen Stellen (z. B. bei Rollenbezeichnungen) das generische Maskulin verwendet wurde.

Ich wünsche allen, die dieses Buch lesen, viele Denkanstöße bei der Lektüre und hoffe, dass Sie von dem Inhalt in Ihrem Verantwortungsbereich profitieren.

Vielen Personen ist zu danken, dass dieses Buch in dieser Form entstehen konnte. Der Zertifikatslehrgang „Information Security Manager“ der Akademie der Technologie gab ursprünglich den Anstoß für das Buch, daher sei hier Herr Klaus Häbel als damaliger Veranstalter erwähnt. Die vielen fachlichen Diskussionen mit Geschäftspartnern und Freunden waren konstruktiv und hilfreich – allen dafür ein herzliches Dankeschön. Mein Dank geht auch an das Lektorat vom Carl Hanser Verlag.

Ein besonderer Dank gilt meiner Frau Susanne Slater-Schmidt, die viel Geduld bewiesen und mich immer unterstützt hat. Ihr widme ich dieses Buch.

Klaus Schmidt

Flensburg, im Sommer 2023

Der Autor

Klaus Schmidt begann seine berufliche Laufbahn als Informationselektroniker in einer Entwicklungsabteilung der Siemens AG. Es folgten ein Hochschulstudium der Angewandten Informatik und Mathematik und der Einstieg in das IT-Consulting mit dem Schwerpunkt der Beratung deutscher Großunternehmen in den Themen IT-Infrastruktur und IT-Sicherheitsmanagement.

Seit 2001 unterstützt er mit seiner Marke Innomenta Unternehmen hinsichtlich des Managements der Informations- und IT-Sicherheit. Er erlangte die Zertifizierung zum Information Security Manager (CISM, ISACA), war Ausbilder für verantwortliche Personen im IT-Sicherheitsmanagement, Referent auf Sicherheitskonferenzen, regelmäßiger Seminarleiter bei Veranstaltungen des Management Circle und publiziert in diesem Themengebiet.

Sie erreichen den Autor per E-Mail unter ***klaus.schmidt@innomenta.de***.

1 Stellenwert der Informationssicherheit

Das Zeitalter, in dem wir leben, bezeichnet man gerne als Informationszeitalter und unsere Gesellschaft als Informationsgesellschaft, in der sich die Zahl der verfügbaren Informationen durch die elektronische Kommunikation in immer kürzer werdenden Abständen verdoppelt.

Im Zusammenspiel mit der Informations- und Kommunikationstechnik hat sich dadurch nicht nur unser privates Leben, sondern auch die Geschäftswelt verändert. Zu den klassischen Produktionsfaktoren Arbeit, Boden und Kapital gesellt sich der Faktor Information und Wissen hinzu, dessen Bedeutung besonders bei innovativen, hochtechnologischen Produkten und Dienstleistungen immer mehr zunimmt.

Die Faktoren Information und Wissen gewinnen auch hinsichtlich der Bestimmung des Unternehmenswertes an Bedeutung. Der Unternehmenswert bemisst sich nicht mehr nur nach Substanz oder Ertrag, vielmehr spielen Informationen und Daten als „Währung des 21. Jahrhunderts“ eine immer entscheidendere Rolle[1]. Innovationskraft, Digitalisierung und das intelligente Management der Faktoren Information und Kommunikation sind wichtige Erfolgsfaktoren. Annähernd alle Geschäftsprozesse werden maßgeblich von den Faktoren Wissen, Information und Kommunikation beeinflusst. Sie sind daher auch ein entscheidender Wettbewerbsfaktor für das Unternehmen.

Anders herum kann die Kompromittierung oder der Verlust von Informationen und Wissen einen großen Schaden für das Unternehmen bedeuten, wie zahlreiche Beispiele in der Vergangenheit zeigen. Nach einer Selbsteinschätzung von Unternehmen dürfte allein durch Erpressung mit gestohlenen oder verschlüsselten Daten 2022 ein Schaden von 10,7 Mrd. Euro entstanden sein[2].

---

[1] Ein Beispiel sind hochgenaue Geo-Daten, die wesentlich sind für das autonome Autofahren und damit auch die Zukunftsfähigkeit, die Wettbewerbsfähigkeit und den Unternehmenswert von Automobilherstellern beeinflussen.

[2] Quelle: *Statista.com*

Dies beweist, dass Information ein wichtiges, schützenswertes Gut ist, das als Erfolgsfaktor zu betrachten und entsprechend zu behandeln ist. Die Erfolgschancen von Unternehmen werden in Zukunft zunehmend davon abhängen, wie schnell und sicher Informationen beschafft, genutzt und verarbeitet werden können und ob mit Informationen als Geschäftswert sicher umgegangen wird. Den Schutz der Informationen zu organisieren und zu verantworten, ist primär Aufgabe der Unternehmensführung, die diese Aufgabe weiter delegiert. Je nach Struktur des Unternehmens landet das Thema im IT-Bereich, im GRC[3]-Bereich oder in einer eigenen Stabsstelle für Informationssicherheit. Oft findet sich die Rolle des „Chief Information Security Officer“ (CISO) für die personelle Verantwortung. Im Titel dieses Buches wird der Begriff IT-Sicherheit verwendet, denn das Management der Informationssicherheit soll in diesem Buch in Verbindung mit der Informationstechnik behandelt werden. Aus diesem Grund wird im Folgenden für die verantwortliche Person im IT-Sicherheitsmanagement die Abkürzung ITSM verwendet, die für „IT-Sicherheitsmanagerin“ bzw. „IT-Sicherheitsmanager“ steht.

1.1 Das Wesen einer Information

Eine Information besteht im Wesentlichen aus zwei Komponenten:

1. **Aussage (Datum).** Der eigentliche Informationsinhalt. Beispiel: „Um 13:00 Uhr waren 8 Personen am System angemeldet.“ Es gibt Informationsaussagen, die nur in einem bestimmten Zusammenhang eine Aussage darstellen oder zu einem bestimmten Zeitpunkt gültig sind, zum Beispiel wie viele externe Mitarbeitende zur Zeit unter Vertrag stehen.
2. **Neuigkeitswert.** Eine echte Information ist nur dann gegeben, wenn das Datum vorher noch nicht bekannt ist. Ein bekanntes Datum informiert den Empfänger nicht (mehr).

Eine Information kann nach verschiedenen Merkmalen charakterisiert werden:

- **Form.** Informationen können die unterschiedlichsten Formen besitzen. Die meisten Informationen im Geschäftsbereich sind visuell (Texte, Symbole, Grafiken, Bilder usw.) und auditiv (Sprache, Töne, Musik) bzw. eine Kombination aus beidem (z. B. Video). Informationen betreffen aber auch alle anderen Sinne. Ein Geruch, eine Gestalt, ein Geschmack oder ein Gefühl – alles kann Information sein.
- **Physischer Träger.** Eine Information ist an keinen physischen Träger gebunden. So kann auch ein Gedanke oder ein Traum eine Information sein. Die Informationssicherheit konzentriert sich aber auf Informationen mit einem physischen Träger.

[3] Governance, Risk Management and Compliance

Das kann bei manuell erfassten Informationen ein Blatt Papier oder eine Karteikarte sein, bei elektronischen Informationen eine Datei auf einer Festplatte oder einem anderen Datenträger. Je nach Form der Information können auch Videobänder, Mikrofilme oder andere Medien angemessene Träger sein. Durch den Träger werden die Informationen speicherbar. Nicht speicherbare Informationen nennt man auch flüchtige Informationen.

Gerade elektronische Informationen können sehr schnell und beliebig oft kopiert und verbreitet werden. Traditionelle Schutzverfahren, die den physischen Träger schützen, sind daher nicht mehr ausreichend.

- **Zeitlicher Verlauf.** Auch Informationen besitzen einen Lebenszyklus (Informationskreislauf) von der Entstehung bis zur „Entsorgung". „Neue" Informationen können einen erheblichen Wert darstellen, verlieren diesen Wert aber mehr oder weniger schnell. Eine Information sollte im Unternehmen nicht „einfach da" sein, sondern aktiv über den gesamten Informationskreislauf hinweg gemanagt werden.

  Das bedeutet, die Beschaffung, Speicherung, Wiederauffindung, Nutzung und Verarbeitung, Archivierung und Ausmusterung von Informationen zu organisieren. Es ist die Aufgabe des Informationsmanagements, hierfür Wege und Verfahren zu entwickeln.

- **Wahrheitsgehalt.** Die Aussage einer Information kann wahr oder falsch und mehr oder weniger präzise sein. Dabei ergibt sich das Problem, dass Wahrheit oft ein vom jeweiligen Umfeld abhängiger relativer Begriff ist. Die Aussage „Die Erde ist eine Scheibe" galt lange Zeit als wahr, bis sie widerlegt wurde. Zudem kann ohne Verifikation oft nicht sofort entschieden werden, ob eine Information wahr oder falsch ist. Dieses Problem stellt sich beispielsweise in den Nachrichtenmedien, wenn es darum geht, wie zuverlässig die Quelle einer Meldung ist.

  In Bezug auf die Informationssicherheit ist es wichtig, dass der Wahrheitsgehalt einer Information nicht unerkannt veränder- bzw. manipulierbar ist, weil die Verbreitung oder Nutzung falscher Informationen für das Unternehmen einen großen Schaden nach sich ziehen kann.

- **Bedeutung für das Unternehmen.** Informationen im Geschäftsumfeld sind von unterschiedlicher Bedeutung für das Unternehmen. Eine grobe Einteilung in vier Stufen ist möglich:
  - *Information ist Geschäftsinhalt.* Die größte Bedeutung ist gegeben, wenn die Information selbst den Geschäftszweck darstellt. Dies ist beispielsweise bei Nachrichtenmedien, Preisagenturen usw. der Fall. Die Information ist die Ware, die ich kaufe.
  - *Information ist geschäftstragend.* Eine geringere, aber dennoch recht große Bedeutung kommt Informationen zu, die für die Geschäftstätigkeit eine tragende Rolle spielen, beispielsweise eine Rezeptur für die Produktion einer Ware.

- *Information ist geschäftsunterstützend.* Unter geschäftsunterstützenden Informationen versteht man Informationen, die nicht direkt die Wertschöpfungskette betreffen, für den geordneten Ablauf aber dennoch benötigt werden. Wartungsinformationen von Maschinen oder Auslastungsquoten von Unternehmensnetzwerken sind Beispiele dafür.
- *Information ist nebensächlich.* In einem Unternehmen gibt es eine Fülle von Informationen, die für die Geschäftstätigkeit des Unternehmens nicht relevant, für die Belegschaft aber recht nützlich sind. Speisepläne der Werkskantine oder die Öffnungszeiten der Werksbibliothek gehören dazu.

Eine Ansammlung von Informationen zu einem bestimmten Thema wird mit dem Begriff Wissen beschrieben. Das Wissensmanagement (es findet sich auch oft die englische Bezeichnung Knowledge Management) nimmt in der Bedeutung für die Unternehmen zu. Es geht um die Fragen „Wie funktioniert etwas?“ (Methodenwissen), „Wie ist etwas?“ (Faktenwissen) und „Wie lässt sich das Wissen im Unternehmen sammeln, dokumentieren und verteilen?“.

Sie als ITSM müssen das Wesen der Informationen kennen, die Sie schützen wollen bzw. müssen. Es ist leicht nachvollziehbar, dass Informationen mit einem hohen Wert (z. B. Entwicklungsdaten mit einem hohen Neuigkeitswert) einen höheren Schutzbedarf besitzen als bereits bekannte Daten.

Die Informationssicherheit darf den Informationsfluss nicht unnötig behindern, soll aber unberechtigte Informationsflüsse verhindern. Je besser Sie die Informationsstrukturen in Ihrem Unternehmen kennen, desto passgenauer können Sie die Informationssicherheit gestalten.

Dabei müssen Sie nicht nur die Informationen selbst, sondern auch deren Austausch berücksichtigen. Die Kommunikation in einem Unternehmen ist ein wichtiger Erfolgsfaktor, wobei die elektronische Kommunikation die größte Rolle spielt, aber auch vielfältige Risiken mit sich bringt.

1.2 Informationstechnik als Informationsinfrastruktur

Der Großteil der Unternehmensinformationen wie Rechnungen, Briefe, Präsentationen oder Termine liegt heutzutage in elektronischer Form vor und wird in dieser Form verarbeitet und gespeichert. Damit kommt der Informationstechnik (IT) eine Schlüsselrolle sowohl für das Informationsmanagement als auch für die Informationssicherheit zu. Zu den oben genannten Unternehmensinformationen kommen noch aus sich selbst heraus produzierte Daten der IT hinzu – wie Protokollierungsdaten, Laufzeitinformationen oder Konfigurationsdaten.

Doch hier ergibt sich eine Reihe von Problemen. Die Informationstechnik wurde ursprünglich nicht als Infrastrukturmaßnahme, sondern als Arbeitshilfe (bezeichnet als EDV) eingeführt und entwickelt sich nun zum echten Business-Partner. Aus diesem Grund existieren in der Regel viele Insellösungen, die den Blick auf das Gesamte verstellen. Hinzu kommen viele Schnittstellen- und Formatprobleme.

Der Bereich IT arbeitet oft trotz enger Bindungen zu den Geschäftsprozessen rein technisch und isoliert, sodass aus der IT heraus nicht immer entschieden werden kann, welche Bedeutung IT-Komponenten für das Geschäft haben. Andererseits ist es aber auch für die Fachbereiche oft nicht möglich zu bestimmen, welche IT-Komponenten für die Unterstützung einzelner Geschäftsprozesse zum Einsatz kommen.

Der IT-Bereich ist aufgrund der technischen Ausrichtung und des hohen erforderlichen Know-how für Außenstehende schwer zu durchschauen. Der eigene Jargon und eine eigene Denkwelt tun ein Übriges und sind der Grund dafür, dass die IT besonders für das Management schwer zu fassen ist.

In Bezug auf die IT-Sicherheit gibt es einerseits die Situation, dass die IT selbst für den Technikbereich aufgrund der zahlreichen und hochdynamischen Bedrohungen nicht beherrschbar zu sein scheint. Auf der anderen Seite kann die IT-Sicherheit jedoch auch schnell zum Selbstzweck werden, besonders wenn die IT-Abteilung sehr technikverliebt ist. Man verliert sich dann in ggf. teuren und unbegründeten Sicherheitsmaßnahmen.

1.3 Sicherheit als Erfolgsfaktor

Das Ziel jeglicher Unternehmenstätigkeit liegt im Geschäftserfolg. Wie man Bild 1.1 entnehmen kann, hängt der Geschäftserfolg von mehreren Faktoren ab, wobei die Aufzählung keinen Anspruch auf Vollständigkeit erhebt.

Der für dieses Buch wichtige Faktor ist „Stabilität und Sicherheit“. Nur wenn es gelingt, alle Unternehmensbereiche – wie Produktion, Entwicklung usw. – gegen bestehende Risiken zu sichern bzw. mit ihnen umzugehen, ist ein planmäßiger Geschäftserfolg möglich. Das bedeutet nicht, dass man ohne Sicherheit nicht auch erfolgreich sein kann, doch beruht dieser Erfolg dann auf Zufall und dem Glück, dass sich Risiken nicht realisiert haben. Eine solche Einstellung ist für eine strategisch orientierte Geschäftsführung nicht vertretbar und verstößt auch gegen gesetzliche Sicherheitsbestimmungen.

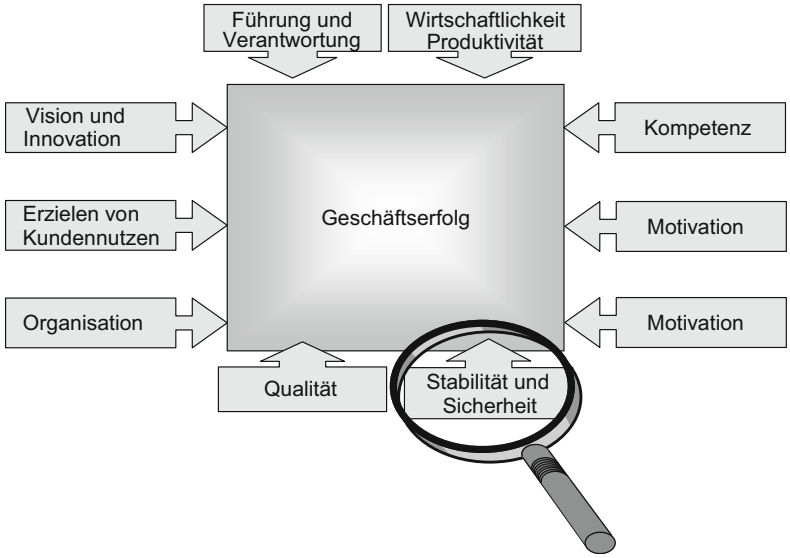

Bild 1.1 Erfolgsfaktoren für den Geschäftserfolg

Die Palette der Risiken, denen sich ein Unternehmen gegenübersieht, ist umfangreich. Bild 1.2 zeigt einige in der Praxis relevante Risikoarten.

Die für die Informationssicherheit relevanten Risikobereiche sind in Bild 1.2 dunkler schattiert. Man sieht, dass neben den eigentlichen Informationsrisiken, die noch näher zu betrachten sein werden, auch Technologie-, Prozess- und rechtliche Risiken für die Informationssicherheit eine Rolle spielen.

Bild 1.2 Einige Risikoarten im Unternehmen

1.4 Sicherheitsfunktionen im Unternehmen

Die in Bild 1.2 dargestellten Risiken werden von verschiedenen Sicherheitsbereichen im Unternehmen behandelt. Einige dieser Bereiche sind in Bild 1.3 aufgeführt.

Bild 1.3 Beispiele von Sicherheitsbereichen im Unternehmen

Die Sicherheitsbereiche, ihre Aufgaben und auch Probleme werden in Kapitel 4, in dem es um die Sicherheitsorganisation geht, eingehender betrachtet. Wichtig für die Informationssicherheit ist die Tatsache, dass sie nur gewährleistet werden kann, wenn die Sicherheit ganzheitlich gesehen wird, d. h. die Sicherheit in allen relevanten Ebenen gegeben ist. Kapitel 8 geht näher darauf ein, wie eine solche ganzheitliche Sicherheit strukturiert werden kann.

Ein wichtiger Grundsatz für die Informationssicherheit sollte immer sein, dass **der Schutz der Geschäftstätigkeit im Zentrum der Bemühungen steht und nicht, wie oft beobachtet, der Schutz der IT**. Der zu schützende Wert liegt bei einem Unix-Server weniger beim Server selbst als vielmehr bei den durch ihn unterstützten Geschäftsprozessen. Dies gilt auch monetär: Der Wiederbeschaffungswert des Servers ist erfahrungsgemäß geringer als die Kosten, die durch eine Serverausfall-bedingte Betriebsunterbrechung verursacht werden.

1.5 Risikomanagement vs. IT-Sicherheit

Die im Sinne der Informationssicherheit zu bewältigenden Aufgaben lassen sich in zwei großen Gruppen anordnen:

Zunächst muss festgestellt werden, welcher Grad an Sicherheit benötigt wird. Dazu wird innerhalb einer Risikobetrachtung die Schadenshöhe herangezogen, die im Zu-

sammenhang mit der Übertragung, der Verarbeitung und der Speicherung von Informationen zu erwarten ist. Diese Aufgabe fällt in den Bereich des *Risikomanagements*. In der Risikobehandlung werden sicherheitsbezogene Maßnahmen in Bezug auf die IT umgesetzt, die damit in den Bereich der *IT-Sicherheit* fallen. Bild 1.4 verdeutlicht diesen Zusammenhang.

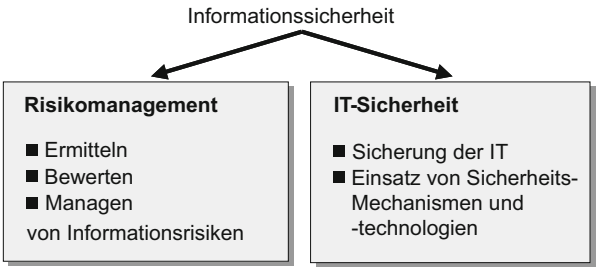

Bild 1.4 Aufteilung der Aufgaben in der Informationssicherheit

Diese Aufteilung sagt jedoch noch nichts darüber aus, wie diese Aufgaben in der Aufbauorganisation des Unternehmens verankert werden. Hierzu gibt es mehrere Möglichkeiten, wie in Kapitel 4 gezeigt wird. Im nächsten Kapitel werden diese beiden Begriffe Risiko und Sicherheit näher beleuchtet.

2 Risiko und Sicherheit

Die Kernaufgabe des IT-Sicherheitsmanagements besteht darin, die Risiko- bzw. Sicherheitssituation des Unternehmens so zu gestalten bzw. zu beeinflussen, dass sicherheitsrelevante Ereignisse und deren Auswirkungen innerhalb eines Rahmens bleiben, der vom Unternehmen als erträglich empfunden wird (siehe dazu auch Abschnitt 7.8, *Der Risikokorridor*).

Risiko und Sicherheit sind daher die zentralen Begriffe für die Arbeit im IT-Sicherheitsmanagement, die für die weitere Verwendung in diesem Buch nun näher beleuchtet werden sollen.

2.1 Risiko

Der Begriff *Risiko* entstand im 16. Jahrhundert mit dem Aufkommen des Überseehandels, als sich die Handelsunternehmen der damaligen Zeit gegen den eventuellen Verlust ihrer Schiffe schützen mussten, die zahlreichen Gefahren ausgesetzt waren.

Sprachlich lassen sich zwei Wurzeln finden: Das lateinische „risicare“ (eine Klippe umschiffen) und das arabische „rizq“ (Schicksal).

Diese sprachlichen Wurzeln sind wichtig, weil sie die Einstellung gegenüber einem Risiko widerspiegeln. Während die lateinische Wurzel ein Risiko als beeinflussbare Größe innerhalb eines aktiven Prozesses begreift, deutet die arabische Wurzel Risiken als gottgegeben. Die beiden Einstellungen und ihre Auswirkungen werden im Folgenden noch zu untersuchen sein.

2.1.1 Begriffsbedeutung

Der Begriff „Risiko“ findet sich in allen Bereichen des menschlichen Lebens, er wird in den diversen Bereichen jedoch unterschiedlich definiert.

Grundsätzliches

Mit dem Begriff Risiko sind drei Aspekte untrennbar verbunden:

1. **Auf die Zukunft gerichtete Betrachtung.** Weil ein Risiko eine Gefahr darstellt, die sich in der Zukunft manifestieren kann, steht im Zentrum der Risikobetrachtung die Frage: „Wie wird sich die Situation aus der Gegenwart heraus in der Zukunft entwickeln?“ Aus der Beschäftigung mit dem Risiko möchte man eine Orientierung ableiten, welche Entscheidungen und Handlungen angesichts dieser Zukunftsabschätzung in der Gegenwart ratsam sind.

2. **Unsicherheit.** Risiko bedeutet immer, dass niemand weiß, wie etwas ausgehen, wie sich die Situation entwickeln wird. Bei der Risikobetrachtung arbeitet man daher mit Wahrscheinlichkeiten, die man aus Erfahrungswerten, Intuition oder dem Auswerten von Hinweisen und Anzeichen ableitet.

   Daher sind auch Risiken der Vergangenheit allenfalls als Erfahrungswerte interessant. Zwar ist die Entwicklung in der Vergangenheit bekannt, sie wird sich aber nicht exakt wiederholen und ist daher keine zuverlässige Grundlage für die Beurteilung der Zukunft. Wenn eine Entwicklung zuverlässig voraussagbar ist, existieren keine Risiken, sondern nur Wirkungen.

3. **Möglichkeit einer negativen Entwicklung.** Es kann gut, aber auch „schief gehen“ – und genau auf diese negative oder schädliche Entwicklung konzentriert sich der Blick bei der Risikobetrachtung. Würde man den Blick auf die positive Entwicklung richten, würde man nicht den Begriff „Risiko“, sondern den Begriff „Chance“ verwenden.

Risiko kann also als „Maß für die Wahrscheinlichkeit, einen Schaden oder einen Verlust zu erleiden“ angesehen werden. Etwas anders formuliert, besteht das Risiko in der „Wahrscheinlichkeit des Eintretens eines unerwünschten Ereignisses (Schaden, Verlust) in einem bestimmten Zeitraum und den mit diesem Ereignis verbundenen Auswirkungen“.

Risiko im Alltagsleben

Im alltäglichen Leben sind wir ständig von Gefahren umgeben und gehen Risiken ein. Der Grund dafür, dass wir nicht fortwährend verängstigt sind, liegt darin, dass wir gelernt haben, die Risiken einzuschätzen und uns an sie zu gewöhnen. Dabei erleben wir Risiken und Gefahren sehr unterschiedlich:

- **als Schicksal.** Das gilt besonders für Naturkatastrophen wie Überschwemmungen, Erdbeben, Flutwellen, Tornados usw., also unabwendbare Ereignisse (höhere Gewalt).
- **als dumpfe Bedrohung.** Das betrifft sehr seltene Schadensereignisse (sehr geringe Wahrscheinlichkeit), deren Schäden aber enorm groß sind, z. B. schwere Reaktorunfälle. Man weiß, dass sich solche Unfälle trotz aller Sicherheitsvorkehrungen nicht verhindern lassen, geht aber aufgrund der sehr kleinen Wahrscheinlichkeit von einer – vermeintlichen – Sicherheit aus.
- **als Herausforderung oder Chance.** Viele Risiken gehen wir bewusst ein, um ein Ziel zu erreichen, einen Gewinn zu erzielen oder um die eigenen Fähigkeiten zu testen. Wir nehmen an Lotterien teil, spekulieren an der Börse oder begeben uns beim Free-Climbing in Lebensgefahr.

Risiko in Technik und Wissenschaft

In Technik und Wissenschaft wird der Begriff Risiko oft gebraucht, um künftige unsichere und negative Zustände einzuschätzen. Eingebürgert hat sich hierfür die sogenannte Risikoformel, nach der das Risiko ein mathematisches Produkt aus der Schadensgröße und der Eintrittswahrscheinlichkeit ist (siehe auch Kapitel 7).

Risiko in Betriebs- und Volkswirtschaft

Wirtschaftliches Handeln orientiert sich an Zielen. Daher wird in wirtschaftlichen Zusammenhängen der Begriff „Risiko“ meist in Verbindung mit den definierten Zielsetzungen gesehen. Risiko ist damit „die Gefahr einer Fehlabweichung “, die materielle, ideelle und monetäre Schäden bzw. Verluste nach sich zieht.

Daneben gibt es einen vor allem in der Versicherungswirtschaft gebräuchlichen, auf das Schadensereignis konzentrierten Risikobegriff. Die dort behandelten Risiken basieren nicht auf subjektiven (geschätzten) Wahrscheinlichkeiten, sondern auf beobachteten und statistisch gesicherten Häufigkeiten. Dazu werden viele Schadensereignisse zusammengefasst ausgewertet und auf diese Weise eine Unabhängigkeit von den einzelnen Ereignissen erreicht.

2.1.2 Risiko und Gefahr

Die Begriffe „Risiko“ und „Gefahr“ werden oft synonym verwendet, denn sie beschreiben beide ein Maß für das Eintreten eines negativen Ereignisses in einer bestimmten Situation. Der Unterschied zwischen Risiko und Gefahr liegt in den Entscheidungsmöglichkeiten über die Situation.

Eine Gefahr ist die Möglichkeit, dass ein negatives Ereignis in einer bestimmten Situation eintreten kann. Wird die Situation innerhalb eines zielgerichteten Handelns

aufgrund einer bewussten Entscheidung herbeigeführt, werden die Gefahren zu Risiken, die man im Zusammenhang mit dem zielgerichteten Handeln eingeht. Wichtig ist, dass man auch dann Risiken eingeht, wenn man sich für eine andere, alternative Situation entscheidet. Entscheidet man überhaupt nicht, sieht man sich wiederum den Gefahren gegenüber, die in der sich daraus ergebenden Situation vorhanden sind.

Gefahren sind im Gegensatz zu Risiken von bewussten Handlungen unabhängig. Bei Gefahren gibt es keine Wahlmöglichkeit, man ist ihnen in bestimmten Situationen ausgesetzt. Für die Beschreibung der Gefahrengröße verwendet man den Begriff der „Gefährlichkeit".

Für die Unterscheidung der beiden Begriffe kommt es also darauf an, welche Rolle man selbst gegenüber der Situation spielt, in der man sich befindet. Was für jemanden, der entscheidet, ein Risiko ist, ist für die von der Entscheidung Betroffenen eine Gefahr. Wichtig ist diese Tatsache im Hinblick auf die Zurechenbarkeit und Verantwortbarkeit eines Schadens bzw. negativen Ereignisses. Gefahren sind eher schicksalhaft, während Risiken von Menschen erzeugt werden, indem sie bewusst Wagnisse eingehen. Damit sind Risiken demjenigen zurechenbar, der die jeweilige Entscheidung trifft.

2.1.3 Deutungen des Risikobegriffs

Es fällt auf, dass im deutschen Sprachraum dem Begriff „Risiko" eine überwiegend negative Bedeutung zukommt. Risiken gilt es zu vermeiden. Jeder von uns weiß aber, dass es keine risikolosen Handlungen geben kann. Eine ganze Industrie, die Versicherungswirtschaft, lebt davon.

Mit jedem Vorhaben – also bewusstem, zielgerichtetem Verhalten – sind automatisch Risiken verbunden (z. B. bei einem Termin zu spät zu kommen). Dabei ist es unerheblich, worin die Handlung inhaltlich besteht.

Jede Tätigkeit beinhaltet ein Risiko. (Sylvius Hartwig)

Im englischen Sprachraum ist der Risikobegriff eng mit dem Begriff „Chance" verbunden. Damit bringt man zum Ausdruck, dass in einem zielgerichteten, risikobehafteten Handeln gleichzeitig auch Chancen stecken. Schon seit jeher ist der Begriff „Risiko" eng mit dem menschlichen Handeln und seinen Folgen (positiv wie negativ) verknüpft.

Risiko ist die Bugwelle des Erfolgs. (Carl Amery)

Daraus ergeben sich zwei wichtige Schlussfolgerungen:

1. In jeder Situation existieren Gefahren (wenn man sich in der konkreten Situation befindet) bzw. Risiken (wenn man sich bewusst für diese Situation entscheidet und sie herbeiführt).

2. Jedes menschliche Handeln ist mit Risiken verbunden.

Die Verknüpfung mit einem zielgerichteten Handeln und die vorhandene Motivation für das Ziel sind entscheidend für die Frage, ob ein Risiko akzeptabel ist oder nicht. Überwiegt die Motivation für das Ziel, kann auch ein Schaden bewusst in Kauf genommen werden.

2.1.4 Erkenntnisse über Risiken

Das Thema „Risiken" beschäftigt die Menschheit, wie bereits erwähnt, schon seit Langem. Im Zeitalter der Aufklärung begann man, sich dem Thema wissenschaftlich zu nähern, wozu insbesondere die Untersuchungen von Glücksspielen beitrugen. Sie führten zur Definition und Berechnungsmethodik von Wahrscheinlichkeiten und legten damit den Grundstein für die Risikoberechnung.

Das Risiko ist keine objektive Messgröße wie etwa das Gewicht. Bei der Beurteilung der Risiken spielen vielmehr psychologische Faktoren eine wichtige Rolle. Was für Laien ein großes Risiko darstellt, kann für Fachleute ein vernachlässigbares Risiko sein. Dies hat Anatol Rapoport schon 1989 aufgezeigt.[1)] Fachleute und Studierende beurteilten verschiedene Risiken und ordneten sie in eine Rangliste[2)] ein:

	Experten	Studenten
Autofahren	1	5
Schwimmen	10	20
Kernkraft	20	1

Wo liegen die Gründe für solche krassen Abweichungen in der Einschätzung von Risiken? Wie wir Risiken einschätzen, hängt von unseren Erfahrungen, Vorurteilen, Meinungen, von Moden und Moralvorstellungen ab. Von entscheidender Bedeutung ist es, wie wir Risiken wahrnehmen (Risikowahrnehmung) und inwieweit wir sie akzeptieren (Risikoakzeptanz).

Risikowahrnehmung

Hat man die Möglichkeit, ein Risiko aktiv zu beeinflussen, so schätzt man es geringer, als wenn man ihm passiv ausgesetzt ist. Ein bekanntes Phänomen besteht darin, dass man als Mitfahrender eine Verkehrssituation gefährlicher einschätzt als der Fahrende selbst, da man keine Kontrolle über das Fahrzeug hat. Auch unter Zeitdruck

[1] Quelle: Rapoport, Anatol (1989), „Risiko und Sicherheit in der heutigen Gesellschaft: Die subjektiven Aspekte des Risikobegriffs". In: Leviathan, Jg. 16, p. 133

[2] Rang 1 bedeutet das größte Risiko.

werden Risiken und Gefahren höher eingeschätzt. Dies bezeichnet man als Panikeffekt.

Bewusst eingegangene Risiken erscheinen leichter kontrollierbar als allgemeine Risiken, weil das Handeln zielgerichtet ist und daher auch entsprechende Alternativen gegeben sind. Ein Beispiel dafür ist der berühmte „Plan B“, mit dem bestimmte Risiken beherrschbar werden, indem man eine andere Alternative wählt.

Charaktereigenschaften beeinflussen die Risikoeinschätzung. So beurteilen optimistisch eingestellte Menschen ein Risiko anders als pessimistische Menschen. Gefühle, Überzeugungen, Gruppenzugehörigkeit, Glaubwürdigkeit der Informanten und gegenseitiges Vertrauen bzw. Misstrauen sind weitere Einflussfaktoren für die Risikowahrnehmung.

Die Erfahrung eines eingetretenen Risikos führt in der Regel zu einem vorsichtigeren Verhalten gegenüber dem Risiko. Der Volksmund sagt: „Ein gebranntes Kind scheut das Feuer.“

Die Risikowahrnehmung variiert stark unter Fachleuten und Laien. Die Diskussion um Elektrosmog bei Mobilfunkmasten löst bei Laien eine diffuse Angst aus, während Fachleute aufgrund tieferer Kenntnis und fundierterer Analyse der Datenbasis diese Angst nicht nachvollziehen können.

Von der Natur verursachte Gefahren erscheinen unwirklicher als vom Menschen verursachte Risiken, weil sich die Ursachen für Elementargefahren (Blitzschlag, Hochwasser) meist nicht vom Einzelnen beeinflussen lassen.

Risikoakzeptanz

Um sich Risiken nicht stellen zu müssen, werden sie gerne heruntergespielt oder als unwahrscheinlich angenommen. Je komplexer bzw. unüberschaubarer eine Risikosituation ist, desto stärker greift dieser Mechanismus der Risikoverdrängung. Dies ist ein psychologischer Schutzmechanismus.

Selbstgewählte Risiken werden eher akzeptiert als solche, denen man ohne Wahl ausgesetzt ist. Hier kommt der bereits angesprochene Umstand zum Tragen, dass mit einem Risiko auch eine Chance verbunden sein kann. Dementsprechend findet eine Risikoabwägung statt. „Es kann ja auch gut gehen“ – und dann hat man die Chance genutzt. Eine starke Motivation für ein Ziel lässt die Risikobereitschaft steigen.

Ein prinzipiell kontrollierbares Risiko wird auch bei Verzicht auf seine Kontrollierbarkeit eher ertragen als ein prinzipiell nicht kontrollierbares Risiko („Man könnte ja etwas tun, wenn es sein muss“). Die Schadenshöhe wird im ersten Fall geringer eingeschätzt. Einem unkontrollierbaren Risiko ist man hilflos ausgesetzt, sodass man das Schlimmste befürchtet, während im anderen Fall zumindest die Illusion besteht, man hätte es mit einem beherrschbaren, einschätzbaren, kalkulierbaren Risiko zu tun.

Je weniger transparent ein Risikobereich erscheint, desto mehr wird er gefürchtet. Viele würden sich fürchten, eine Nacht im Dschungel zu verbringen, selbst wenn es

objektiv gesehen gar nicht so risikoreich wäre. Die Intransparenz der potenziellen Risiken reicht aus.

Risiken, die sich allmählich akkumulieren, werden weniger gefürchtet als plötzliche, seltene Ereignisse. Dies liegt daran, dass man sich mit den Risiken vertraut gemacht, sich an sie gewöhnt hat und über Erfahrungen bzgl. der Auswirkungen verfügt.

Hohe Wahrscheinlichkeiten eines Risikos werden häufig von den Betroffenen dadurch erträglich gemacht, dass sie sich selbst einen Ausnahmestatus zuerkennen, der oft mit der Illusion einhergeht, man könne das Risiko besser als andere beherrschen.

2.2 Sicherheit

Der Begriff „Sicherheit“ beschreibt einen Zustand, der frei von Gefahren bzw. Risiken ist. Im Englischen unterscheidet man die Sicherheit des Lebens und der Gesundheit von Lebewesen (Safety) im Sinne der Verhütung von Unfällen bzw. technischem oder menschlichem Versagen einerseits sowie der Sicherheit vor Angriffen (Security) andererseits, während im Deutschen beides mit dem Begriff „Sicherheit“ umschrieben wird (siehe auch Abschnitt 6.11, IT-/OT-Sicherheit).

Einen absolut risiko- bzw. gefahrenfreien Zustand gibt es nicht. Daraus folgt, dass es auch eine hundertprozentige Sicherheit nicht geben kann. Sicherheit ist demnach immer nur als relativer Zustand der Gefahrenfreiheit anzusehen, d. h. bezogen auf eine bestimmte Situation, einen bestimmten Zeitraum und bestimmte Rahmenbedingungen.

2.2.1 Sicherheitskriterien

Ziel des Managements der Informationssicherheit ist eine passgenaue Sicherheit. Dies bedeutet, dass überall dort, wo man Sicherheit benötigt, der entsprechende Schutz gegeben ist, und dort, wo er nicht benötigt wird, kein Aufwand für einen Schutz betrieben wird.

Die Definition von Sicherheit als gefahrenfreier Zustand ist zu global, um eine passgenaue Sicherheit erzielen zu können. In der Praxis muss die Frage beantwortet werden, in welcher Hinsicht die für die Informationsverarbeitung relevanten Objekte[3)] geschützt werden müssen, um die Sicherheit des Unternehmens zu gewährleisten. Nur so lässt sich entscheiden, welche Sicherheitsmaßnahmen zu ergreifen sind.

Die Antwort auf diese Frage bilden Sicherheitskriterien. Sie brechen die globale Definition des gefahrenfreien Zustands auf einzelne Aspekte herunter. Einen Standard

[3] Computer, Netzwerke, Personen, Räume usw.

dafür, wie viele Kriterien zu betrachten sind, gibt es nicht, dafür aber diverse Kriterienmodelle mit unterschiedlich vielen Kriterien. Auch können einige Sicherheitskriterien aus anderen abgeleitet werden.

Im Folgenden beschreiben wir zunächst drei grundlegende Sicherheitskriterien und anschließend einige erweiterte, die sich aus den drei grundlegenden Kriterien ableiten lassen.

Verfügbarkeit

Die Informationstechnik stellt IT-Dienste zur Verfügung, die in Form von Software-Anwendungen innerhalb der unternehmerischen Tätigkeit genutzt werden. In vielen Fällen sind die Geschäftsprozesse von diesen IT-Diensten abhängig, und ohne sie ist die unternehmerische Tätigkeit nicht mehr zu erbringen.

Die Sicherheit der Prozesse erfordert es demnach, dass die IT-Dienste verfügbar und nutzbar sind. Ein Maß dafür ist das Sicherheitskriterium „Verfügbarkeit“. Die Verfügbarkeit ist die Wahrscheinlichkeit, das jeweils betrachtete System zu einem bestimmten Zeitpunkt in einem funktionstüchtigen Zustand anzutreffen.

Die Verfügbarkeit wird als Prozentwert angegeben. 0 % bedeutet: das System funktioniert nie; bei 50 % ist das System während der Hälfte der betrachteten Zeit ausgefallen; bei 100 % würde das System nie ausfallen und wäre jederzeit nutzbar. In der Informationssicherheit besitzen geforderte Verfügbarkeiten oft hoch anmutende Werte, die meist über 99 % liegen. Die nachfolgende Tabelle zeigt aber, dass selbst eine Verfügbarkeit von 99 % für einen IT-Dienst eine relativ große Ausfallzeit bedeutet.

Verfügbarkeit	Ausfall pro Jahr
90 %	36,5 Tage
95 %	18,25 Tage
99 %	3,65 Tage
99,9 %	8,76 Stunden
99,99 %	52,56 Minuten
99,999 %	5,26 Minuten

Für die in der Tabelle gezeigten Werte wurde ein kontinuierlich arbeitender[4)] IT-Dienst zugrunde gelegt und die Werte gerundet. Die Verfügbarkeit von 99,999 % wird in der Informationstechnik auch als „Five Nines“ bezeichnet.

Es kommt immer wieder zu Diskussionen, ob das IT-Sicherheitsmanagement oder der IT-Betrieb für die Verfügbarkeit zuständig ist. Das IT-Sicherheitsmanagement folgt

[4] Dauerbetrieb „24×7“, also 24 Stunden pro Tag, 7 Tage die Woche.

der oben dargestellten Argumentation, dass die Verfügbarkeit für die Sicherheit der Geschäftsprozesse notwendig ist, während der IT-Betrieb die Verfügbarkeit als Qualitätskriterium des laufenden Betriebs ansieht. In der Praxis ist es daher oft so, dass das IT-Sicherheitsmanagement bei den Vorgaben für die Verfügbarkeit aktiv wird und eine kontrollierende Funktion ausübt, während der IT-Betrieb die Verfügbarkeit verwaltet und im laufenden Betrieb überwacht.

Vertraulichkeit

In einem Unternehmen existieren viele Informationen, die als vertraulich einzustufen sind und nur einem bestimmten Personenkreis zugänglich sein dürfen. Geraten solche Informationen in die falschen Hände (z. B. Entwicklungs- oder Angebotsinformationen), kann für das Unternehmen daraus ein großer Schaden entstehen. Daher ist die Wahrung der Vertraulichkeit solcher Informationen für die Sicherheit des Unternehmens ein wichtiges Kriterium.

Die Vertraulichkeit ist also ein Maß dafür, inwieweit gewährleistet wird, dass eine vertrauliche Information nur denjenigen Personen zugänglich gemacht wird, für die sie vorgesehen ist.

Wenn vertrauliche und nicht-vertrauliche Informationen gemischt sind oder vertrauliche Informationen in größeren Informationseinheiten eingebettet sind, ist es mitunter eine technische Herausforderung, nur die vertraulichen Informationen zu schützen und die Gesamtinformation trotzdem als Ganzes nutzen zu können. In diesem Fall müssen Maßnahmen getroffen werden, dass die vertrauliche Information nicht unbefugt aus der Gesamtinformation entnommen werden kann, z. B. mittels Verschlüsselung.

Es gibt keine standardisierte Metrik für die Vertraulichkeit; oft findet man Vertraulichkeitsstufen wie die Einstufungen „gering – mittel – hoch – sehr hoch“ oder „öffentlich – intern – vertraulich – streng vertraulich“.

Integrität

Für die Informationssicherheit ist es wichtig, dass Informationen nicht unbefugt und unbemerkt verändert werden können, da sonst mitunter ein großer Schaden droht. Man stelle sich eine Bank vor, bei der die Kurswerte des Online-Wertpapierhandels manipuliert werden, oder einen Bahnverkehr, bei dem Lichtsignale unbemerkt verändert werden.

Die Integrität ist also ein Maß dafür, inwieweit eine Information ihren ursprünglichen Inhalt über die Zeit behält. Sie wird mit einem logischen Wahrheitswert angegeben. Entweder die Information wurde verändert oder nicht. „Ein bisschen integer“ gibt es nicht.

Im Hinblick auf die IT-Sicherheit wird oft dargestellt, dass die digitale Signatur eine Methode wäre, um die Integrität sicherzustellen. Das ist aber nicht richtig. Auch ein

digital signiertes Datum kann natürlich verändert werden, somit besteht kein Integritätsschutz. Das Datum lässt sich lediglich dahingehend überprüfen, ob eine Veränderung stattfand oder nicht. Das ursprüngliche Datum lässt sich mit einer digitalen Signatur nicht rekonstruieren.

Authentizität

Ähnlich wie bei der Manipulation von Daten kann es auch verheerend sein, wenn es gelingt, eine Information „unterzuschieben" – z. B. bei einer E-Mail-Nachricht einen bestimmten Absender vorzutäuschen.

Die Authentizität gibt an, ob etwas tatsächlich so ist, wie es scheint. Beispielsweise ob eine E-Mail tatsächlich von demjenigen stammt, der als Absender angegeben ist, oder ob eine Person tatsächlich diejenige ist, die sie vorgibt zu sein.

Technisch lässt sich die Authentizität mit einer digitalen Signatur überprüfen. Aus Fragmenten der Information, E-Mail etc. wird ein Datenabbild (Hash) erstellt und mit dem geheimen Schlüssel eines asymmetrischen Verschlüsselungsverfahrens verschlüsselt („unterschrieben" bzw. „signiert"). Weil dazu der geheime Schlüssel benutzt wird, den nur die signierende Person kennt, kann die Information nur von ihr stammen[5)].

Auch die Authentizität wird mit einem logischen Wahrheitswert angegeben. Entweder stammt eine Information vom angegebenen Urheber oder eben nicht.

Nachvollziehbarkeit

Mit der Nachvollziehbarkeit kann man verfolgen, welche Aktionen mit einer Information oder Nachricht durchgeführt wurden und ggf. wer diese Aktionen durchgeführt hat. Dies ist besonders für die IT-Forensik und die IT-Revision von Bedeutung.

Auch für die Nachvollziehbarkeit gibt es keine festgelegte Metrik. Oft wird sie wie die Vertraulichkeit mit Stufen wie „gering – mittel – hoch – sehr hoch" angegeben.

Konformität

Die Konformität ist ein Maß für die Übereinstimmung mit einem definierten Vergleichsgegenstand. Beispiel: Ein Unternehmen kann konform zu einem Sicherheitsstandard arbeiten, ein Netzwerk kann konform zur strukturierten Verkabelung aufgebaut sein, ein Administrator kann konform zu den Anforderungen für technisches Personal tätig sein.

Im Hinblick auf die IT-Sicherheit spielt die Konformität zu IT-Sicherheitsstandards die größte Rolle. Die Konformität kann mittels einer Zertifizierung nachgewiesen werden, um den Grad der Qualität der IT-Sicherheit des Unternehmens zu dokumentieren bzw. nachzuweisen.

---

[5] Das gilt aber nur unter der Voraussetzung, dass der Schlüssel nicht kompromittiert ist.

Eine einzelne Konformitätsangabe ist strenggenommen ein Wahrheitswert. Ist die Konformität jedoch nicht vollständig erfüllt, wird oft angegeben, zu welchen Teilen die Konformität bereits gegeben ist, z. B. mit einer Prozentangabe oder mit Hilfe von Begriffen, z. B. „weitgehend“ oder „geringfügig“.

Verbindlichkeit

Die Verbindlichkeit bzw. Nicht-Abstreitbarkeit ist ein Beispiel für ein Sicherheitskriterium, das sich aus zwei anderen Sicherheitskriterien zusammensetzt. Ein solches Kriterium wird auch als kombiniertes Sicherheitskriterium bezeichnet.

Die Verbindlichkeit setzt sich aus den beiden Kriterien Authentizität und Integrität zusammen. Beispiel: Wenn feststeht (z. B. auf Grund einer digitalen Signatur), dass ich der Absender einer Bestellung per E-Mail bin, und wenn weiterhin feststeht, dass diese E-Mail auf ihrem Weg vom Absender zum Empfänger nicht verändert wurde (ebenfalls durch digitale Signatur), kann ich nicht bestreiten, die Bestellung in der Form aufgegeben zu haben, wie sie beim Empfänger eingetroffen ist.

Die Verbindlichkeitsangabe ist strenggenommen ein Wahrheitswert. Durch die unterschiedlich starke Sicherheit der eingesetzten Verfahren finden sich aber auch Metriken, mit denen sich beurteilen lässt, wie vertrauenswürdig die Verbindlichkeit ist.

2.2.2 Sicherheitsgrad

Um das Unternehmen, ein Projekt, eine Situation o. ä. hinsichtlich der Sicherheit einschätzen zu können, bedarf es einer Maßgröße, die die Höhe der Sicherheit angibt. Weil der Begriff „Sicherheit“ als „Abwesenheit von Gefahr bzw. Risiko“ definiert wurde, spannen sich zwei Extreme auf: „gefährlich“ bzw. „risikoreich“ einerseits, „gefahrenfrei“ bzw. „sicher“ andererseits.

Versieht man diese beiden Extreme mit einer Prozentangabe, wie in Bild 2.1 geschehen, bekommt man ein Maß für die Sicherheit: den Sicherheitsgrad. 0 % steht für „totale Unsicherheit“, 100 % für „absolute Sicherheit“. Sowohl 0 % als auch 100 % sind, wie bereits erwähnt, theoretische Werte, die in der Praxis nicht vorkommen.

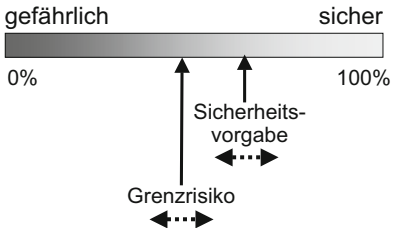

Bild 2.1 Sicherheitsgrad

Auf dieser Skala ist nun festzulegen, welcher Sicherheitsgrad erreicht werden soll. Dieser Zahlenwert zwischen 0 und 100 gibt Auskunft über das angestrebte Sicherheitsziel, das als Sicherheitsvorgabe die Grundlage für die Sicherheitsmaßnahmen bildet. Diese Zielsetzung wird durch die Sicherheitsvorgabe ausgedrückt, ein Zahlenwert zwischen 0 und 100. Für die Sicherheitsvorgabe wird auch der Begriff „Schutzziel“ verwendet. Denkt man umgekehrt von der Gefahrenseite aus, gibt es einen zweiten Punkt, der angibt, welcher Grad an Gefahr bzw. Risiko maximal akzeptiert werden kann. Er wird als Grenzrisiko bezeichnet. Zwischen Grenzrisiko und Sicherheitsvorgabe liegt der Bereich des akzeptablen Risikos. Kapitel 7 geht darauf näher ein.

2.2.3 Sicherheitsstufen

Mit dem reinen prozentualen Zahlenwert zu arbeiten, ist in der Praxis nicht sehr sinnvoll bzw. erfordert umfangreiche Erläuterungen. Daher wird diese recht feine Unterteilung oft in gröbere Stufen eingeteilt. Im Bereich zwischen 0 % und 100 % finden sich dann mehrere Sicherheitsstufen, wie in Bild 2.2 zu sehen ist. Anstelle des Begriffs „Sicherheitsstufen“ werden (seitens der Sicherheit) auch die Bezeichnungen „Sicherheitsklassen“ oder „Schutzklassen“ verwendet. Seitens des Risikos bzw. der Gefahr finden sich Begriffe wie „Alarmstufen“ oder „Gefahrenstufen“.

Wie hoch die Anzahl der Sicherheitsstufen ist, hängt davon ab, wie fein man den Bereich zwischen 0 % und 100 % einteilen möchte oder muss. Üblich sind zwischen 3 und 6 Stufen.

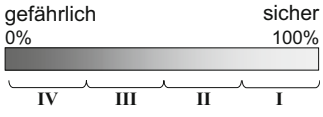

Bild 2.2 Sicherheitsstufen

Die Kennzeichnung der Sicherheitsstufen ist unterschiedlich, man findet Zahlen (1, 2, 3 oder I, II, III, IV wie in Bild 2.2), Buchstaben (A, B, C) oder auch Farben (Rot, Orange, Gelb, Grün). Auch die Namen für einzelne Sicherheitsstufen sind sehr unterschiedlich, aus dem Sprachgebrauch kennt man hierfür Begriffe wie „roter Alarm“, „Alarmstufe 1“ oder „DEFCON 2“[6]. Bild 2.3 zeigt ein Beispiel für ein solches Sicherheitsstufenmodell mit vier Stufen. Denkt man von der Sicherheit her, dann wird oft eine ansteigende Metrik verwendet. Ein Sicherheitslevel 4 ist also sicherer als ein Level 2. Denkt man vom Risiko her, wird oft eine abnehmende Metrik gewählt. DEFCON 2 ist also eine gefährlichere Situation als DEFCON 4.

Unabhängig davon, ob prozentual oder mit Sicherheitsstufen: Es muss klar definiert werden, was unter welcher Angabe zu verstehen ist, d. h. welche Sicherheit gefordert wird. Diese Einschätzung ist jedoch von Unternehmen zu Unternehmen unterschied-

[6] Defense Readiness Condition – Warnstufen der militärischen Verteidigungsbereitschaft der USA

lich, sodass es diesbezüglich einen allgemeingültigen Standard nicht geben kann. Eine Möglichkeit wird mit dem Security Capability Maturity Model in Abschnitt 8.3.2 gezeigt.

I	Hochsicherheit	sehr hohe Sicherheitsanforderungen
II	erhöhte Sicherheit	hohe Sicherheitsanforderungen
III	Grundschutz	mittlere Sicherheitsanforderungen
IV	geringe Sicherheit	keine bis geringe Sicherheitsanforderungen

Bild 2.3 Beispiel für ein Sicherheitsstufenmodell

2.2.4 Verhältnis zwischen Sicherheitsgrad und Aufwand

Es ist leicht einzusehen, dass mit steigendem Sicherheitsgrad auch die Kosten steigen, um diesen Grad zu erreichen. Der Verlauf der Kostensteigerung ist dabei aber nicht linear. Hier gilt in etwa die berühmte 80:20-Regel, d. h. mit 20 % der Kosten kann ich bis zu 80 % an Sicherheit erreichen. Benötige ich einen höheren Sicherheitsgrad, steigen die Kosten dafür von Prozent zu Prozent stark an. Dies bedeutet für den ITSM, dass sich die von ihm veranlassten Maßnahmen am jeweiligen Schutzbedarf orientieren müssen, was umso mehr gilt, je höher der Sicherheitsgrad festgelegt wird.

Den ungefähren Kostenverlauf zeigt Bild 2.4. In der Abbildung ist auch der Bereich des Grundschutzes zu sehen, d. h. der Bereich, der mit Standardmaßnahmen einen gewissen Schutz bietet, wenn keine höheren Schutzbedarfsanforderungen vorliegen.

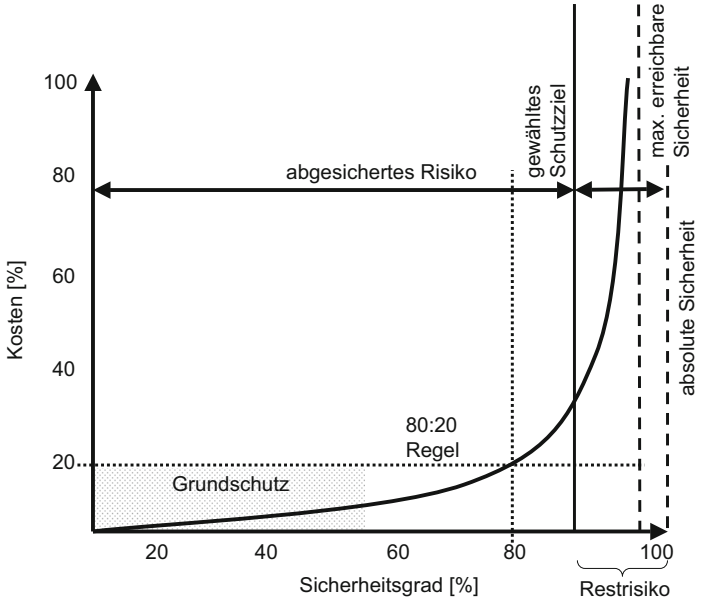

Bild 2.4 Sicherheitsgrad-Kosten-Diagramm