



Thomas W.  
Harich

3. Auflage



# **IT-Sicherheitsmanagement**

## **Das umfassende Praxis-Handbuch**

für IT-Security und technischen Datenschutz nach ISO 27001

- **Aufgaben des IT-Security-Managers**
- **Informationssicherheit ausarbeiten**
- **IT-Sicherheitskonzepte einrichten**
- **Information Security Management System aufbauen**



## **Hinweis des Verlages zum Urheberrecht und Digitalen Rechtemanagement (DRM)**

Liebe Leserinnen und Leser,

dieses E-Book, einschließlich aller seiner Teile, ist urheberrechtlich geschützt. Mit dem Kauf räumen wir Ihnen das Recht ein, die Inhalte im Rahmen des geltenden Urheberrechts zu nutzen. Jede Verwertung außerhalb dieser Grenzen ist ohne unsere Zustimmung unzulässig und strafbar. Das gilt besonders für Vervielfältigungen, Übersetzungen sowie Einspeicherung und Verarbeitung in elektronischen Systemen.

Je nachdem wo Sie Ihr E-Book gekauft haben, kann dieser Shop das E-Book vor Missbrauch durch ein digitales Rechtemanagement schützen. Häufig erfolgt dies in Form eines nicht sichtbaren digitalen Wasserzeichens, das dann individuell pro Nutzer signiert ist. Angaben zu diesem DRM finden Sie auf den Seiten der jeweiligen Anbieter.

Beim Kauf des E-Books in unserem Verlagsshop ist Ihr E-Book DRM-frei.

Viele Grüße und viel Spaß beim Lesen,

*Ihr mitp-Verlagsteam*



Neuerscheinungen, Praxistipps, Gratiskapitel,  
Einblicke in den Verlagsalltag –  
gibt es alles bei uns auf Instagram und Facebook



[instagram.com/mitp\\_verlag](https://www.instagram.com/mitp_verlag)



[facebook.com/mitp.verlag](https://www.facebook.com/mitp.verlag)

# Inhaltsverzeichnis

## Impressum

## Einleitung

### **Kapitel 1: Umfang und Aufgabe des IT-Security-Managements**

- 1.1 Kapitelzusammenfassung
- 1.2 Einführung
- 1.3 Informationen und Daten
- 1.4 IT-Security-Management ist wichtig
- 1.5 Wie gefährdet sind die Unternehmensdaten
  - 1.5.1 Sicht des Verfassungsschutzes
  - 1.5.2 Öffentliche Wahrnehmung
  - 1.5.3 Die eigene Wahrnehmung
- 1.6 Begrifflichkeiten
- 1.7 Selbstverständnis der IT-Security-Organisation
- 1.8 Grundregeln
- 1.9 Umfang des IT-Security-Managements
  - 1.9.1 Pfeiler der IT-Security
  - 1.9.2 Aufgaben des IT-Security-Managements
- 1.10 IT-Security zwischen Nutzen und Kosten

### **Kapitel 2: Organisation der IT-Security**

- 2.1 Kapitelzusammenfassung
- 2.2 Einführung

## 2.3 Rollen innerhalb des IT-Security-Managements

### 2.3.1 Manager IT-Security

### 2.3.2 Unternehmensleitung

### 2.3.3 Weitere Rollen

## 2.4 Verankerung im Unternehmen

### 2.4.1 IT-Security im Organigramm

### 2.4.2 IT-Security und der Datenschutz

### 2.4.3 Zusammenspiel mit anderen Sicherheitsbereichen

## **Kapitel 3: IT-Compliance**

### 3.1 Kapitelzusammenfassung

### 3.2 Einführung

### 3.3 Standards

#### 3.3.1 ISO-2700x-Reihe

#### 3.3.2 Standards des Bundesamts für Sicherheit in der Informationstechnik

#### 3.3.3 Gegenüberstellung ISO 2700x und BSI-Grundschatz

#### 3.3.4 ITIL

#### 3.3.5 Weitere Standards

### 3.4 Gesetze

#### 3.4.1 EU-Datenschutz-Grundverordnung

#### 3.4.2 IT-Sicherheitsgesetz

#### 3.4.3 Weitere Gesetze

#### 3.4.4 Branchenstandards am Beispiel TISAX

#### 3.4.5 ISO 27001 und TISAX

#### 3.4.6 Vorbereitende Maßnahmen

#### 3.4.7 Fragenkatalog

## **Kapitel 4: Organisation von Richtlinien**

- 4.1 Kapitelzusammenfassung
- 4.2 Einführung
- 4.3 Strukturierung von Richtlinien
- 4.4 Beschreibung und Kategorisierung
- 4.5 Pflege und Lenkung von Richtlinien
- 4.6 Richtlinien und Audits
- 4.7 Verschiedene Richtlinien
  - 4.7.1 Sicherheitsrichtlinie
  - 4.7.2 Klassifizierungsrichtlinie
  - 4.7.3 ISMS-Handbuch
  - 4.7.4 Richtlinie zum IT-Risikomanagement
  - 4.7.5 IT-Sicherheitsrichtlinie
  - 4.7.6 IT-Systemrichtlinien
- 4.8 Von der Theorie in die Praxis

## **Kapitel 5: Betrieb der IT-Security**

- 5.1 Kapitelzusammenfassung
- 5.2 Einführung
- 5.3 IT-Security und der IT-Betrieb
- 5.4 Betriebliche Grundsätze
  - 5.4.1 Ableitung aus gesetzlichen Vorschriften
  - 5.4.2 Vertragswesen
  - 5.4.3 Administrative Tätigkeiten
  - 5.4.4 Trennung von Funktionen
  - 5.4.5 Prinzip der geringsten Rechte
- 5.5 IT-Security-Prozesse
  - 5.5.1 Zugangs- und Zugriffskontrolle

- 5.5.2 Sicherheit von Software
- 5.5.3 Sichere Softwareentwicklung
- 5.5.4 Identitätsmanagement
- 5.5.5 Genehmigungsprozesse
- 5.5.6 Standardisierung
- 5.5.7 Unterstützung des IT-Betriebs

## **Kapitel 6: IT Business Continuity Management**

- 6.1 Kapitelzusammenfassung
- 6.2 Einführung
- 6.3 Abgrenzung der Begriffe
- 6.4 IT-Notfallmanagement und Verfügbarkeitsmanagement
- 6.5 Gesetzliche Rahmenbedingungen des IT Business Continuity Managements
- 6.6 Business-Impact-Analyse
  - 6.6.1 Erfassung und Priorisierung der Geschäftsprozesse
  - 6.6.2 Business-Impact-Analyse in der Praxis
- 6.7 Weitere Einflussfaktoren

## **Kapitel 7: IT-Notfallmanagement**

- 7.1 Kapitelzusammenfassung
- 7.2 Einführung
- 7.3 IT-Notfallmanagement
- 7.4 Richtlinie zum IT-Notfallmanagement
- 7.5 Ableitung von Notfallstrategien
- 7.6 IT-Notfallkonzepte erstellen

- 7.6.1 Schweregrade
- 7.6.2 Notfallvorsorge
- 7.7 Notfallorganisation
  - 7.7.1 Organisationsstruktur
  - 7.7.2 Kompetenzen und Zuständigkeiten
  - 7.7.3 Notfallhandbuch
- 7.8 Notfallbewältigung
- 7.9 Notfallübungen
- 7.10 Überprüfung des IT-Notfallmanagements
- 7.11 Monitoring im Rahmen des IT Business Continuity Managements
- 7.12 Checklisten IT-Notfallmanagement
  - 7.12.1 Checkliste Business-Impact-Analyse
  - 7.12.2 Checkliste Notfallorganisation
  - 7.12.3 Checkliste Notfallpläne und Wiederanlaufpläne
  - 7.12.4 Checkliste Rechenzentrum

## **Kapitel 8: Verfügbarkeitsmanagement**

- 8.1 Kapitelzusammenfassung
- 8.2 Einführung
- 8.3 Richtlinie zum Verfügbarkeitsmanagement
- 8.4 Verfügbarkeit
  - 8.4.1 Klassifizierung von Verfügbarkeit
  - 8.4.2 Vorgehensweise
  - 8.4.3 Berechnung der Verfügbarkeit
- 8.5 Ausfallsicherheit
- 8.6 Ausprägungen von Redundanz

- 8.6.1 Strukturelle Redundanz
- 8.6.2 Funktionelle Redundanz oder unterstützende Redundanz
- 8.6.3 Informationsredundanz
- 8.7 Redundante Hard- und Software
- 8.8 Virtualisierung
- 8.9 Bauliche Maßnahmen zur Steigerung der Verfügbarkeit

## **Kapitel 9: Technische IT-Security**

- 9.1 Kapitelzusammenfassung
- 9.2 Einführung
- 9.3 Technisch-Organisatorische Maßnahmen
  - 9.3.1 Zugangskontrolle
  - 9.3.2 Zugriffskontrolle
  - 9.3.3 Übertragungskontrolle und Transportkontrolle
  - 9.3.4 Eingabekontrolle
  - 9.3.5 Verfügbarkeitskontrolle, Wiederherstellbarkeit und Zuverlässigkeit
  - 9.3.6 Datenintegrität
- 9.4 Verschlüsselung
  - 9.4.1 Begriffsbestimmungen
  - 9.4.2 Symmetrische Verschlüsselungssysteme
  - 9.4.3 Asymmetrische Verschlüsselungsverfahren
- 9.5 Cloud Computing
  - 9.5.1 Dienstleistungen in der Cloud
  - 9.5.2 Risikofaktoren
  - 9.5.3 Datenschutzrechtliche Aspekte
  - 9.5.4 Vertragliche Vereinbarungen

- 9.5.5 Sinnvolle Freigabeprozesse
- 9.6 Betrieb von Firewalls
  - 9.6.1 Paketfilter und Application-Gateways
  - 9.6.2 Firewall-Regelwerk
  - 9.6.3 Internet-Proxyserver
- 9.7 Internetzugang und Nutzung von E-Mail
  - 9.7.1 Risikofaktor E-Mail
  - 9.7.2 Verschlüsselung von E-Mails
  - 9.7.3 Risikofaktor Internetbrowser
- 9.8 Penetrationstests
- 9.9 Digitale Signatur
- 9.10 Intrusion-Detection-Systeme
- 9.11 Wireless LAN

## **Kapitel 10: IT-Risikomanagement**

- 10.1 Kapitelzusammenfassung
- 10.2 Einführung
- 10.3 IT-Risikomanagement im Unternehmenskontext
- 10.4 Akzeptanz des IT-Risikomanagements
- 10.5 Operatives IT-Risikomanagement
  - 10.5.1 Vorgehensweise
  - 10.5.2 IT-Risikomanagementprozess
  - 10.5.3 Übergeordnete Risikobetrachtung
  - 10.5.4 Schwachstellen
  - 10.5.5 Bedrohungen
  - 10.5.6 Zusammenspiel von Bedrohungen, Schwachstellen und Maßnahmen
  - 10.5.7 Verhältnismäßigkeit

## 10.6 Schutzbedarfsfeststellung

10.6.1 Schutzziele

10.6.2 Schutzstufen

10.6.3 Prinzipien

10.6.4 Feststellung des Schutzbedarfs

10.6.5 Veränderung des Schutzbedarfs

10.6.6 Widersprüchliche Schutzziele

10.6.7 Schadensklassen

10.6.8 Abbildung des Datenflusses

10.6.9 Entscheidungsfindung auf Basis des Schutzbedarfs

## 10.7 IT-Risikomanagement Prozess

10.7.1 Risiken identifizieren

10.7.2 Risikoermittlung

10.7.3 Risikobewertung

## 10.8 Quantitative Darstellung von Risiken

10.8.1 Grundlagen der Risikoberechnung

10.8.2 Risikoberechnung im Beispiel

10.8.3 Risikomatrix

10.8.4 Risikokatalog

## 10.9 Risikobehandlung

10.9.1 Risiko akzeptieren

10.9.2 Risiko reduzieren

10.9.3 Risiko vermeiden

10.9.4 Risiko auf Dritte verlagern

## 10.10 Maßnahmen definieren

10.10.1 Maßnahmentypen

10.10.2 Individuelle Maßnahmenkataloge

## **Kapitel 11: Sicherheitsmonitoring**

- 11.1 Kapitelzusammenfassung
- 11.2 Einführung
- 11.3 Ebenen des Monitorings
- 11.4 System-Monitoring
  - 11.4.1 Sicherheitsaspekte
  - 11.4.2 Auswahl zu überwachender Systeme
  - 11.4.3 Implementierung im Netzwerk
- 11.5 Protokoll-Monitoring
  - 11.5.1 Unterstützung von Audits
  - 11.5.2 Überwachung administrativer Tätigkeiten
  - 11.5.3 Schwachstellenmanagement

## **Kapitel 12: IT-Security-Audit**

- 12.1 Kapitelzusammenfassung
- 12.2 Einführung
- 12.3 Audits im Kontext des IT-Security-Managements
- 12.4 Audits im Unternehmenskontext
- 12.5 Audits nach Kategorien
- 12.6 Vor-Ort kontra Selbstauskunft
- 12.7 Anforderungen an den Auditor
- 12.8 Ein Audit Schritt für Schritt
  - 12.8.1 Vorbereitung
  - 12.8.2 Durchführung
  - 12.8.3 Nachbereitung
  - 12.8.4 Abschlussbericht

## **Kapitel 13: Management von Sicherheitsereignissen und IT-Forensik**

- 13.1 Kapitelzusammenfassung
- 13.2 Einführung
- 13.3 Angriffe auf Ihre Daten
  - 13.3.1 Durch eigene Mitarbeiter
  - 13.3.2 Durch Außenstehende
  - 13.3.3 Angriffe und Angriffsvektoren
  - 13.3.4 Angriffsarten
- 13.4 Management von Sicherheitsereignissen
- 13.5 IT-Forensik
  - 13.5.1 Arten der IT-Forensik-Analyse
  - 13.5.2 Einrichtung von Honeypots
- 13.6 Elemente der forensischen Untersuchung
  - 13.6.1 Zielsetzung
  - 13.6.2 Anforderungen an die Analyse
  - 13.6.3 Forensische Methoden
  - 13.6.4 Forensische Untersuchung

## **Kapitel 14: Kennzahlen**

- 14.1 Kapitelzusammenfassung
- 14.2 Einführung
- 14.3 Die Aufgabe von Kennzahlen
- 14.4 Quantifizierbare Kennzahlen
- 14.5 Steuerung mithilfe von Kennzahlen
- 14.6 Qualität von Kennzahlen
  - 14.6.1 Gute Kennzahlen
  - 14.6.2 Schlechte Kennzahlen

- 14.6.3 Vergleichbarkeit von Kennzahlen
- 14.7 Verschiedene Kennzahlen aus der IT-Security
- 14.8 Kennzahlen im laufenden Verbesserungsprozess
- 14.9 Laufende Auswertung von Kennzahlen
- 14.10 Annualized Loss Expectancy
- 14.11 IT-Security Balanced Scorecard
  - 14.11.1 Einführung der IT-Security Balanced Scorecard
  - 14.11.2 Maßnahmenziele für den Bereich IT-Security

## **Kapitel 15: Praxis: Aufbau eines ISMS**

- 15.1 Kapitelzusammenfassung
- 15.2 Einführung
- 15.3 ISMS in Kürze
- 15.4 Herangehensweise
- 15.5 Schritt für Schritt zum ISMS
  - 15.5.1 Plan-Do-Check-Act
  - 15.5.2 Vorarbeiten
  - 15.5.3 Plan: Gestaltung des ISMS
  - 15.5.4 Do: Umsetzung der Arbeitspakete
  - 15.5.5 Check: Überprüfung des ISMS
  - 15.5.6 Act: Umsetzung von erkannten Defiziten
  - 15.5.7 Dokumentation
- 15.6 Softwaregestützter Aufbau eines ISMS
  - 15.6.1 Auswahl einer ISMS-Lösung
  - 15.6.2 Darstellung der Risiken und der Unternehmenswerte
  - 15.6.3 Darstellung von Prozessen

- 15.6.4 IT-Risikomanagement
- 15.6.5 Richtlinienmanagement
- 15.6.6 Arbeitsabläufe abbilden
- 15.6.7 Berichte erstellen
- 15.7 Zertifizierung nach ISO 27001
  - 15.7.1 Ansprechpartner
  - 15.7.2 Prinzipien

## **Kapitel 16: Awareness und Schulung**

- 16.1 Kapitelzusammenfassung
- 16.2 Verbesserungsprozess
- 16.3 Voraussetzungen für eine Sicherheitskultur
- 16.4 Erfassung der Sicherheitskultur
- 16.5 Top-down-Ansatz
- 16.6 Awareness-Projekte

Thomas W. Harich

# **IT-Sicherheitsmanagement**

## **Das umfassende Praxis-Handbuch**

**für IT-Security und technischen Datenschutz  
nach ISO 27001**

**3. Auflage**



# Impressum

## **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.

ISBN 978-3-7475-0148-1

3. Auflage 2021

[www.mitp.de](http://www.mitp.de)

E-Mail: [mitp-verlag@sigloch.de](mailto:mitp-verlag@sigloch.de)

Telefon: +49 7953 / 7189 - 079

Telefax: +49 7953 / 7189 - 082

© 2021 mitp Verlags GmbH & Co. KG

Dieses Werk, einschließlich aller seiner Teile, ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Lektorat: Katja Völpel  
Korrektorat: Petra Heubach-Erdmann  
Covergestaltung: Christian Kalkert, Sandrina Dralle  
Coverbild: nightstranger1/[stock.adobe.com](https://stock.adobe.com)  
electronic **publication**: Ill-satz, Husby, [www.drei-satz.de](http://www.drei-satz.de)

Dieses Ebook verwendet das ePub-Format und ist optimiert für die Nutzung mit dem iBooks-reader auf dem iPad von Apple. Bei der Verwendung anderer Reader kann es zu Darstellungsproblemen kommen.

Der Verlag räumt Ihnen mit dem Kauf des ebooks das Recht ein, die Inhalte im Rahmen des geltenden Urheberrechts zu nutzen. Dieses Werk, einschließlich aller seiner Teile, ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und Einspeicherung und Verarbeitung in elektronischen Systemen.

Der Verlag schützt seine ebooks vor Missbrauch des Urheberrechts durch ein digitales Rechtemanagement. Bei Kauf im Webshop des Verlages werden die ebooks mit einem nicht sichtbaren digitalen Wasserzeichen individuell pro Nutzer signiert.

Bei Kauf in anderen ebook-Webshops erfolgt die Signatur durch die Shopbetreiber. Angaben zu diesem DRM finden Sie auf den Seiten der jeweiligen Anbieter.

# Einleitung

## Anmerkung zur dritten Auflage

Die grundlegenden Bestandteile eines IT-Sicherheitsmanagements ändern sich nicht in ähnlich kurzen Zeiträumen, wie sich die technische Seite der IT und der IT-Security ändert. Die Schwerpunkte, die fachliche Ausgestaltung und die Prozesse bleiben davon aber nicht unbeeindruckt. Werden Daten vermehrt in Public Clouds verarbeitet, auf Mobiltelefonen gespeichert, über Chat-Apps geteilt oder im Rahmen von Industrie 4.0 in einer Größenordnung erhoben, die bislang kaum denkbar war, dann müssen sich die entsprechenden Maßnahmen der IT-Security an diese Veränderungen anpassen. Der Gesetzgeber hat parallel dazu die Aufgabe, Regelungen zu erlassen, um frühzeitig die Rahmenbedingungen festzulegen und dabei zu helfen, dem Missbrauch entgegenzuwirken. In diesem Zusammenhang werden weltweit neue Gesetze erlassen und entsprechende Kontrollgremien eingesetzt. Völlig unterschiedlich gelagerte Beispiele dafür sind die EU-Datenschutz-Grundverordnung (EU-DSGVO), das IT-Sicherheitsgesetz oder das China Cybersecurity Law. Alle diese Regelungen haben immense Auswirkungen darauf, wie Unternehmen Daten erfassen, verarbeiten, speichern oder austauschen dürfen. In der Fülle und der Bandbreite der neuen Regelungen liegt aber immer auch die immanente Gefahr, etwas falsch zu machen, weil man eben den falschen Weg gewählt hat, mit diesen Anforderungen umzugehen. Der Weg aus dieser Problematik ist es, einem Lösungsansatz zu folgen, der zum einen international bekannt und anerkannt ist und zum anderen auf einem stringenten Prozess-Modell basiert, das so angelegt ist, dass alle oben genannten Punkte abgedeckt

werden können. Dieser Weg ist die Einführung eines IT-Sicherheitsmanagements auf Basis der ISO-27000-Normen-Familie unter Beachtung der datenschutzrechtlichen Bestimmungen der EU-DSGVO.

Auch wenn sich seit der 2. Auflage einiges auf dem Sektor der Informationssicherheit getan hat, so hat sich dennoch gezeigt, dass die Leitplanken, die durch die beherrschenden Normen der ISO-2700x-Reihe gelegt wurden, Bestand hatten und auch weiterhin Bestand haben werden. So richten sich an den Prozessmodellen dieser Normen in der Zwischenzeit nationale Gesetze genauso aus wie auch die Anforderungen von Unternehmen und dem öffentlichen Sektor. Diese Standardisierung und das damit einhergehende Ziehen am gleichen Seil ist auch bitter nötig. Die Zahl der täglich gemessenen gezielten Cyber-Angriffe steigt unaufhörlich weiter, während parallel deren Qualität im Durchschnitt immer weiter zunimmt.

Mit der Covid-19-Krise ändern sich die Angriffsvektoren und passen sich neuen Arbeitsprozessen an. Insbesondere Unternehmen, die kein umfassendes Sicherheitskonzept etabliert haben, bekommen dies zu spüren. Mitarbeiter arbeiten im weitgehend ungesicherten häuslichen Umfeld, Budgets werden eingefroren und personell ausgedünnte IT-Abteilungen werden der Masse an Makro- und Ransomware-Angriffen nicht mehr Herr. Jede Fehlkonfiguration an einem Server oder einer Sicherheitssoftware kann in einem solchen Umfeld schnell den Cyber-Supergau bedeuten. Für Unternehmen, die gleichzeitig in einem angespannten wirtschaftlichen Umfeld agieren, kann dies schnell auch das Aus bedeuten.

Niemals zuvor ist die Verflechtung von Lieferketten so offensichtlich zutage getreten wie nach den Lockdowns verschiedener Länder oder Regionen. Dies gilt auch für

Datenflüsse zwischen Lieferanten und Herstellern und damit verwundert es nicht, dass die großen Branchenverbände längst damit begonnen haben, nicht nur diejenigen Daten sicher zu verarbeiten, die sie im eigenen Zugriff haben, sondern auch Lieferanten anzuhalten, Sicherheitsstandards einzuhalten. Aus diesem Grund habe ich ein Kapitel zu dem viel beachteten Branchenstandard der deutschen Automobilindustrie, der unter der Abkürzung »TISAX« bekannt ist, im Kapitel »Compliance« hinzugefügt. Sehr ähnliche Standards entstehen in vielen Branchen und letzten Endes werden sie sich aufgrund der gleichen Wurzeln auch nicht wesentlich voneinander unterscheiden.

Neben dem eben erwähnten neu hinzugefügten Sicherheitsfeld wurden in der vorliegenden Auflage viele Kapitel aktualisiert.

Ich möchte all denjenigen danken, die mir Input bezüglich neuer Gesichtspunkte gegeben haben. Dies schließt sowohl die wohlmeinende Kritik an einzelnen Punkten durch Leser als auch das Feedback meiner Studierenden und der Professoren an der Hochschule oder von Kollegen im Unternehmen mit ein. Auch wenn man sich selbst als Generalisten im IT-Sicherheitsbereich sieht, ist man nicht ganz vom Tunneldenken befreit und übersieht doch das eine oder andere Mal neue Aspekte und neue Denkansätze – obwohl sie doch so offensichtlich vor einem liegen.

## **Über die Zielgruppe**

Nicht alle Wege, aber zumindest sehr viele, führen nach Rom, und wohl ebenso viele Wege führen zum Job des IT-Security-Managers. Einige Kandidaten haben schon ein paar Jahre Berufserfahrung in ähnlichen Bereichen gesammelt,

haben bereits einschlägige Erfahrungen gemacht oder kommen direkt aus dem Studium, in dem sie das Thema, zumindest theoretisch, schon behandelt haben.

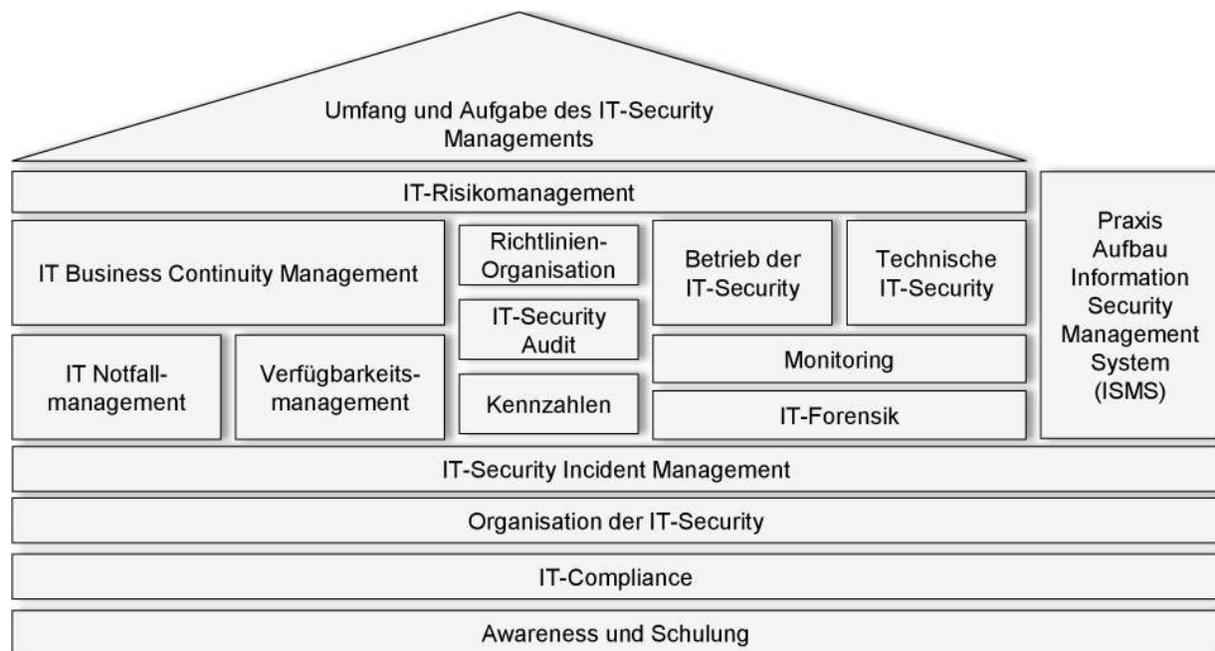
Andere, und damit sind wir wieder bei den vielen Wegen angekommen, die zum Ziel führen, sind Neueinsteiger oder Quereinsteiger. Vielleicht kommen sie aus der IT-Abteilung und haben zuvor Server administriert oder Softwareprojekte geleitet. In manchen Fällen waren sie davor aber auch im Controlling oder in der Unternehmensplanung tätig und haben sich mit Qualitätsaudits oder Risikomanagement beschäftigt. Diese Kollegen stehen dann häufig vor der Herausforderung, dass sie, selbst wenn sie angekommen sind (nicht in Rom selbstverständlich, sondern am Arbeitsplatz des IT-Security-Managers), die schiere Menge an Einzelthemen dann fast erschlägt.

Beiden Gruppen kann man aufrichtig versichern, dass es kaum eine Aufgabe gibt, die vielschichtiger und vielseitiger gestaltbar ist, als diese. Gerade der Umfang schafft die Chance, dem Arbeitsplatz den eigenen Stempel aufzudrücken, und wenn man die Grundlagen einmal verstanden hat, fällt es schwer, sich eine spannendere Aufgabe vorzustellen. Das Gebiet der IT-Security ist nicht so alt, als dass es bereits fest ausgetretene Pfade gäbe. Vielmehr gehen die Meinungen, was denn ein IT-Security-Manager zu tun hat, weit auseinander. Damit muss sich die IT-Security-Organisation dem Unternehmen flexibel anpassen. Stetige Veränderungen, hinzukommende Verknüpfungen mit anderen Abteilungen und die laufende Kommunikation mit denen, die Daten verarbeiten, und denen, die sie verwalten, bringen einerseits Abwechslung und andererseits den Druck, laufend hinzuzulernen.

Für alle, die frisch einsteigen, schon Erfahrungen haben oder gar aus einem ganz anderen Fachgebiet heraus

quereinsteigen und nun auf einfache, aber doch umfassende Art in die Thematik IT-Security eingeführt werden wollen, ist das vorliegende Buch gedacht.

## Aufbau des Buches



Für eine strukturierte Vorgehensweise beim Durcharbeiten des Buches ist es sinnvoll, mit dem ersten Kapitel »[Umfang und Aufgabe des IT-Security-Managements](#)« zu beginnen. Im Grunde umreißt es das Aufgabengebiet und bringt die verschiedenen Themen in einen Zusammenhang. Ein guter Einstieg, um danach zielgerichtet diejenigen Kapitel zu betrachten, die einem selbst am interessantesten erscheinen. Aus diesem Grund sind alle Kapitel so verfasst, dass ein direkter Einstieg erleichtert wird.

Ansonsten gilt: Für ein durchgängiges Verständnis und als eine Art roter Faden ist es empfehlenswert, sich erst um

Fundament und Dach zu kümmern, bevor die verschiedenen Säulen abgearbeitet werden.

Jedes Kapitel beschreibt einen zusammenhängenden Themenbereich der IT-Security. Der Aufbau bleibt dabei immer ähnlich. Obligatorische Theorie wechselt sich ab mit Tipps aus der Praxis für die Praxis, ein paar Beispielen und dazu Aufzählungen und Checklisten als Hilfestellung. Die einzelnen Themen umfassen dabei das notwendige Wissen, um den Arbeitsplatz IT-Security ausfüllen zu können, und häufig noch etwas mehr.

Die Aufgaben eines IT-Security-Managers sind vielfältig und abwechslungsreich, bauen aber immer wieder aufeinander auf. Es gibt Themen wie das IT-Risikomanagement, die in den verschiedensten Fragestellungen immer wieder auftauchen. So ist das Wissen notwendig, wie eine Risikobewertung durchgeführt wird, wenn es darum geht, Prioritäten in der Notfallvorsorge zu treffen, aber genauso auch im alltäglichen Betrieb, wenn es um die Berechtigungsvergabe oder die Entscheidung für und wider einer einzukaufenden Software geht. Aus diesem Grund wird dieses Aufgabenfeld als Teil der Dachkonstruktion in der Abbildung abgebildet.

Die weiteren Elemente des Hauses stellen die anderen Kapitel des Buches dar. Manche Themen bilden das Fundament für den gesamten Komplex, wieder andere bilden zusammen mit einem oder zwei Bereichen eine Einheit. So sind die Kapitel zum IT-Notfallmanagement und zum Verfügbarkeitsmanagement zwei Teile des übergeordneten Themas IT Business Continuity Management.

Die Wahl, die IT-Security-Organisation, die IT-Compliance, das IT-Security Incident Management und die Bildung von

Awareness als Fundament zu nutzen, fiel aufgrund der Tatsache, dass es nicht möglich ist, sie immer und immer wieder mitzubetrachten. Gleichgültig, welche Maßnahme implementiert oder welche Richtlinie durchgesetzt werden soll, immer stellt sich die Frage, wie diese zu kommunizieren und zu schulen ist, wie die inneren und äußeren Anforderungen aussehen und wie die IT-Security-Organisation aufgebaut sein muss, um dies auch bewältigen zu können.

Ein Kapitel sticht etwas hervor. Das reine Praxiskapitel über die Einführung eines Information Security Management Systems (ISMS) steht etwas abseits am rechten Rand des Hauses. Diese Zuordnung soll vergegenwärtigen, dass alle im Buch behandelten Themen in irgendeiner Art und Weise Teil des ISMS sind. Die Zusammenführung und die Annäherung an die Praxis werden an dieser Stelle vertieft angegangen.

# Kapitel 1

# Umfang und Aufgabe des IT-Security-Managements

## 1.1 Kapitelzusammenfassung

Im Rahmen des ersten Kapitels werden die einzelnen Themengebiete des IT-Security-Managements in einen Gesamtzusammenhang eingebettet. Es wird erläutert, warum man Informationen schützen muss und wie diese Aufgabe durch die IT-Security-Organisation wahrgenommen wird.

### Die Top-5-Fragen zum aktuellen Kapitel:

- Sind die Aufgabengebiete definiert, die dem IT-Security-Management zugeordnet werden?
- Sind die organisatorischen Einheiten, die sich um die Betreuung von sicherheitsrelevanten Systemen kümmern, darüber informiert und dahin gehend instruiert, dass sie sich im Einflussbereich des IT-Security-Managements befinden?
- Wurden Schutzziele zusammen mit der Unternehmensleitung definiert?
- Werden die Grundregeln (Prinzipien) im Umgang mit Informationen kommuniziert und in der Praxis umgesetzt?
- Werden die Grundpfeiler der IT-Security, das IT-Risikomanagement, die IT-Compliance und die IT-

Governance auch in Verbindung mit dem IT-Security-Management gebracht und damit auch als Aufgabe des Managers IT-Security gesehen?

## **1.2 Einführung**

Ransomware, Industrie 4.0, die EU-Datenschutz-Grundverordnung, Mobility, Heimarbeitsplätze, Public-Cloud-Services und viele andere Themen haben in letzter Zeit die Schlagzeilen beherrscht. Angesichts der Wucht dieser Themen und den häufig noch fehlenden, umfassenden Sicherheitsarchitekturen, die man benötigt, um diese zu beherrschen, geht immer häufiger das Gefühl dafür verloren, wie diese Sicherheits-Felder miteinander verwoben sind, und vor allem auch, wie diese mit den klassischen Sicherheitsanforderungen wie dem Assetmanagement oder auch einem Antivirenkonzept verknüpft werden müssen. Altes Wissen trifft dabei auf völlig neue Bedrohungen. In dieser Gemengelage ist es die Aufgabe des Managers IT-Security, den Überblick zu bewahren und auf die wichtigen Bedrohungen mit den erforderlichen Maßnahmen in angemessener Weise zu reagieren. Im Sprachgebrauch dieses Buches unterscheidet er sich damit von einem IT-Security-Experten, der Fachmann für ein dediziertes Feld der IT-Security ist und sich vorwiegend auch nur innerhalb dieses Arbeitsgebiets bewegt.

Der Manager IT-Security sieht sich in der Situation, das Know-how des Unternehmens zu schützen, indem er Bedrohungen erkennt, abschätzt und diesen dann geeignete Sicherheitskonzepte und Maßnahmen entgegensetzt. Zu diesem Zweck bedient er sich Werkzeugen, die in diesem Buch dargestellt werden. Diese Werkzeuge haben sich über

die Jahre bewährt und in der Zwischenzeit auch international durchgesetzt. Aus diesem Grund ist es nicht überraschend, dass sich eine recht junge EU-Datenschutz-Grundverordnung der gleichen Prozesse bedient wie eine »ältere« ISO-27001-Norm.

## **1.3 Informationen und Daten**

Der Schutz von Informationen, also dem Know-how des Unternehmens, ist die Aufgabe des IT-Security-Managements. Nur was sind Informationen und worin unterscheiden sie sich von Daten? Daten sind eine technische Darstellung von Informationen. Anders ausgedrückt: Informationen sind Daten, die einen Sinn ergeben. Auf niedrigster Ebene bestehen sie aus den physikalischen Zuständen »hohe Spannung« oder »niedrige Spannung« oder übersetzt null oder eins. Somit sind Daten zunächst einmal Bits und Bytes, deren Interpretation wiederum Informationen ergeben. Sicherheitsmaßnahmen wiederum kann man nicht direkt auf Informationen beziehen. Setzt man Verschlüsselung ein, dann werden die Daten verschlüsselt. Installiert man einen Virensch scanner, dann schützt man das Betriebssystem und indirekt wieder die Daten. Ganz anders, wenn man dies aus der Perspektive des Risikomanagements betrachtet, dann stehen die Informationen im Mittelpunkt und deren Wert für das Unternehmen. Wenn wir also von Informationsschutz sprechen, dann geht es im Grunde darum, alle Systeme inklusive der Daten technisch zu schützen, um die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen zu bewahren.

Die Gewinnung von Informationen aus einem Pool von Daten geschieht durch eine Fragestellung. So sind Daten mit der Ausprägung »4 Eier, 450 g Mehl, 400 ml Milch, Vanillezucker, 210 g Zucker und eine Prise Salz« nur im Zusammenhang mit der Frage »Was benötige ich, um vernünftige Pfannkuchen machen zu können?« als Information anzusehen. Ohne Fragestellung sind es nur beliebige, nicht zusammenhängende Daten. Daraus kann man ersehen, dass Daten zunächst einmal keinen Kontextbezug haben. Das wertvolle Gut, das es zu schützen gilt, ist also mehr als nur eine Menge von Bits und Bytes auf Festplatten.

Jede Form von Informationen, wie immer sie auch ausgestaltet sein mögen und deren Verlust einen Schaden für das Unternehmen bedeutete, gehört zu den Unternehmenswerten, die im Fokus des Managers IT-Security liegen.

### **Wichtig**

Auch wenn sich das IT-Security-Management auf Daten und Daten verarbeitende Systeme konzentriert, stehen noch eine ganze Reihe weiterer Unternehmenswerte im Fokus der IT-Security. Dazu zählen auch abstrakte Werte wie der Ruf des Unternehmens oder das Wissen in den Köpfen der Mitarbeiter.

Informationen können in vielfältiger Form vorliegen. Die Erfahrungen von Mitarbeitern gehören genauso zu den schützenswerten Informationen wie Informationen, die auf Datenträgern vorliegen und durch IT-Systeme verarbeitet