Hacking und IT-Security

Der leichte Weg zum IT-Security-Experten

Max Engelhardt

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

©2020 BMU Media GmbH
www.bmu-verlag.de
info@bmu-verlag.de

Lektorat: Matthias Kaiser
Einbandgestaltung: Pro ebookcovers Angie
Druck und Bindung: Wydawnictwo Poligraf sp. zo.o. (Polen)

Taschenbuch-ISBN: 978-3-96645-082-9
Hardcover-ISBN: 978-3-96645-083-6
E-Book-ISBN: 978-3-96645-081-2

Dieses Werk ist urheberrechtlich geschützt.
Alle Rechte (Übersetzung, Nachdruck und Vervielfältigung) vorbehalten. Kein Teil des Werks darf ohne schriftliche Genehmigung des Verlags in irgendeiner Form – auch nicht für Zwecke der Unterrichtsgestaltung- reproduziert, verarbeitet, vervielfältigt oder verbreitet werden.

Dieses Buch wurde mit größter Sorgfalt erstellt, ungeachtet dessen können weder Verlag noch Autor, Herausgeber oder Übersetzer für mögliche Fehler und deren Folgen eine juristische Verantwortung oder irgendeine Haftung übernehmen. 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.

Hacking und IT-Security

Inhaltsverzeichnis

1. IT-Security 8

1.1 Einführung ... 8
1.2 Begrifflichkeiten ... 10
1.3 Informationssicherheitsziele ... 14
1.3.1 Vertraulichkeit ... 15
1.3.2 Integrität ... 19
1.3.3 Verfügbarkeit ... 21
1.4 Informationssicherheitsmanagement ... 26
1.4.1 Grundlagen ... 26
1.4.2 ISMS ... 29
1.4.3 Sicherungsmaßnahmen ... 37
1.4.4 IT-Grundschutz mit Verinice ... 44
1.5 IT-Forensik ... 54
1.5.1 Grundlagen ... 54
1.5.2 Live-Response ... 57
1.5.3 Post-mortem-Analysen ... 59
1.5.4 Ablauf ... 60
1.6 IT-Notfallmanagement ... 65
1.6.1 Grundlagen ... 65
1.6.2 Elemente des IT-Notfallmanagements ... 69
1.6.3 BSI-Standard 100-4 ... 83
1.7 Kryptologie ... 90
1.7.1 Grundlagen ... 90
1.7.2 Verschlüsselung ... 96
1.7.3 Hash-Funktionen ... 106
1.7.4 Digitale Signatur ... 109

2. Hacking 114

2.1 Einleitung ... 114
2.2 Notizen ... 119
2.3 Netzwerkgrundlagen ... 125
2.3.1 ISO/OSI Schichtenmodell ... 125
2.3.2 Ethernet ... 131
2.3.3 Internet Protocol ... 134
2.3.4 TCP/UDP ... 138
2.3.5 DNS ... 142
2.3.6 Ports und Protokolle ... 145
2.3.7 Subnetze ... 147
2.3.8 Hypertext Markup Language ... 151
2.3.9 Hyper Text Transfer Protocol ... 155
2.4 Vorbereitungen für Kali Linux ... 166
2.4.1 Installation Virtual Box ... 166
2.4.2 Kali Linux VM unter VirtualBox ... 169

2.5 Kali Linux ... 180
2.5.1 Installation ... 180
2.5.2 Dateisystem und –befehle ... 190
2.5.3 Benutzer und Rechte ... 195
2.5.4 Netzwerkbefehle ... 197
2.5.5 Dienste ... 199
2.5.6 Installation und Updates von Tools ... 201
2.5.7 Skripte mit Bash ... 204
2.6 Python ... 210
2.6.1 Einführung ... 210
2.6.2 String ... 214
2.6.3 Mathematische Ausdrücke ... 219
2.6.4 Variablen ... 224
2.6.5 Listen ... 226
2.6.6 Verzweigungen ... 228
2.6.7 Schleifen ... 229
2.6.8 Bool'sche Ausdrücke ... 232
2.6.9 Module ... 236
2.6.10 Funktionen ... 238
2.6.11 Dictionaries ... 243
2.6.12 Sockets ... 246
2.6.13 Beispiel: Portscanner ... 247
2.7 Die fünf Phasen des Hacking ... 255
2.8 Sammeln von Informationen ... 263
2.8.1 Zielidentifikation ... 263
2.8.2 Passives Scannen ... 267
2.8.3 Hunter.io ... 273
2.8.4 Zugangsdaten mit breach-parse ... 276
2.8.5 theHarvester ... 281
2.8.6 Subdomains finden ... 283
2.8.7 Webseiten analysieren ... 291
2.8.8 Burp Suite ... 296
2.8.9 Google Dork ... 306
2.8.10 Soziale Medien ... 310
2.9 Aktives Scannen ... 315
2.9.1 Nmap ... 315
2.9.2 HTTP/HTTPS ... 323
2.9.3 SMB ... 326
2.9.4 SSH ... 329
2.9.5 Schwachstellendatenbanken ... 331
2.9.6 Weitere Werkzeuge ... 333
2.10 Zugang erhalten ... 343
2.10.1 Shells ... 344
2.10.2 Payload ... 349
2.10.3 Metasploit ... 351
2.10.4 Brute Force ... 357
2.10.5 Credential Stuffing & Password Spraying ... 363
2.10.6 Social Engineering ... 370
2.10.7 Physische Angriffe ... 372
2.11 Entwicklung von Exploits ... 377
2.11.1 Buffer Overflows ... 377
2.11.2 Spiking ... 380

2.11.3 Fuzzing 381
2.12 Active Directory 392
2.12.1 Einführung 392
2.12.2 Aufbau 393
2.12.3 Eigenes ‚Lab' 395
2.12.4 LLMNR Poisening 442
2.12.5 Hash Cracking 447
2.12.6 SMB Relay 449
2.12.7 Shell Access 455
2.13 Post-Exploitation 462
2.13.1 Scanning 462
2.13.2 Laterale Ausbreitung 469
2.13.3 Dateitransfer 470
2.13.4 Zugang behalten 473
2.14 Web-Applikationen 474
2.14.1 OWASP Juice Shop 476
2.14.2 Offenlegung sensibler Daten 483
2.14.3 Fehlkonfiguration 489
2.14.4 XSS 495
2.14.5 Injections 500
2.14.6 Broken Access Control 505
2.14.7 Broken Authentication 512
2.14.8 XXE 519

3. Schluss 527

4. Glossar 531

5. Index 535

Alle Programmcodes aus diesem Buch sind als PDF zum Download verfügbar. Dadurch müssen Sie sie nicht abtippen:
https://bmu-verlag.de/hacking-und-it-security/

Außerdem erhalten Sie die eBook Ausgabe zum Buch im PDF Format kostenlos auf unserer Website:

https://bmu-verlag.de/hacking-und-it-security/
Downloadcode: siehe Kapitel 3

Kapitel 1
IT-Security

1.1 Einführung

Informationen sind zu einem entscheidenden Produktionsfaktor für Unternehmen geworden. Da nahezu jeder Prozess von bestimmten Daten oder Wissen abhängt, werden das Überleben und der Erfolg von Unternehmen von den gespeicherten und verarbeiteten Informationen bestimmt. Damit wird jede Gefährdung dieser Informationen eine Gefährdung für das Unternehmen oder die Institution.

Gefährdungen für unternehmensinterne Informationen stellen zum Beispiel Datenverluste oder Datenabflüsse dar. Laut einer Studie von Ponemon und IBM verursacht der Abfluss eines sensiblen oder vertraulichen Datensatzes im Durchschnitt 148 $ Schaden. Vertrauliche oder sensible Datensätze sind zum Beispiel Kreditkartendaten oder Benutzeraccounts mit E-Mailadresse und Passwort. Ein aktueller Fall von abgeflossenen Daten ist der Hack der ROM-Website ‚Emuparadise' bei welchem private Daten von 1,1 Millionen Benutzern gestohlen wurden. Rein rechnerisch ist somit ein durchschnittlicher Schaden von 162,8 Millionen USD entstanden. Die Webseite haveibeenpwned.com listet mehrere solcher Fälle auf und kommt auf eine Gesamtsumme von fast 8 Milliarden kompromittierter Datensätze.

Andere Beispiele, die eine existenzbedrohende Gefahr für ein Unternehmen darstellen, ohne dass Daten gestohlen werden, sind Datenverluste, zum Beispiel durch Ransomware. Hier wird versucht alle Daten in einem Netzwerk zu verschlüsseln und nur nach Zahlung eines Lösegelds den Schlüssel freizugeben. Diese Art von Angriff traf 2019 zum Beispiel das norwegische Unternehmen Norsk Hydro. Der entstandene Schaden ist nicht genau beziffert, aber der Konzern musste mehrere Tage teilweise auf Papierprozesse umsteigen. Dies verdeutlicht, dass

die Bedeutung von Informationen im Unternehmen einhergeht mit der Abhängigkeit von Informationstechnologie (IT).

Allerdings müssen IT-Sicherheitsvorfälle nicht immer einen böswilligen Ursprung haben. Ein gutes Beispiel dafür ist der deutsche Bundestag im Jahr 2012. Hier wurde das E-Mail-System zweimal in Folge Opfer eines Ausfalls. Im Januar 2012 führte die versehentliche Adressierung der Mail einer Mitarbeiterin eines Abgeordneten an alle Adressaten im Bundestagsverzeichnis, zu hunderten Antworten an den gleichen Empfängerkreis. Dies führte zu einer Flut von E-Mails, welche letztendlich die Erreichbarkeit des E-Mail-Systems so stark beeinflusste, dass sich die IT-Abteilung genötigt sah eine Mitteilung an alle zu versenden, dass E-Mail ausschließlich zu dienstlichen Zwecken versendet werden dürfen.

Bereits 3 Monate später fiel das gleiche E-Mail-System komplett durch einen Hardwarefehler aus. Nach Aussage eines Bundestagssprechers funktionierte das entsprechende Notfallsystem nicht. Beide Szenarien sind Beispiele von Verfügbarkeitseinschränkungen ohne Einflussnahme einer böswilligen Partei.

Die Absicherung von Informationen wird dabei auf verschiedenen Ebene betrachtet: operativ und taktisch/strategisch. Die operative Ebene umfasst den tatsächlichen Schutz der IT vor Angriffen. Dabei geht es um klassische Maßnahmen, wie das Einspielen von Updates oder der Einsatz von Firewalls. Zu den operativen Maßnahmen der IT-Sicherheit gehören aber auch Intrusion Detection Systeme, eine Sicherheitsüberprüfung von Systemadministratoren oder die ständige Begleitung von Reinigungspersonal.

Die taktisch/strategisch Ebene umfasst grob gesagt das Management der Informationssicherheit. Hier liegt der Fokus auf Dokumentation, Analyse und Bewertung der Anforderungen an IT-Sicherheit und der umgesetzten Maßnahmen. Dabei liegt auch immer ein Fokus auf der kontinuierlichen Verbesserung. Wie nahezu alle Aspekte der IT, sind Anforderungen und Maßnahmen an IT-Sicherheit oft in sehr kurzer

Zeit nicht mehr aktuell und müssen aktualisiert werden, um wirksam zu bleiben.

Dieses Buch widmet sich im ersten Teil hauptsächlich der strategischen Ebene mit den Themenkomplexen Informationssicherheitsmanagements, IT-Forensik und IT-Notfallmanagement.

Der zweite Teil zielt auf die operative Ebene ab, wobei hier immer die Sicht des Angreifers und des Verteidigers gezeigt wird. Für ein hohes Informationssicherheitsniveau ist es unabdingbar, dass man die Denkweise des Angreifers versteht und die Sicherungsmaßnahmen darauf abstimmt.

1.2 Begrifflichkeiten

Bereits in der Einführung sind einige Begriffe genannt worden, die genauer erläutert werden müssen.

Als Erstes muss in diesem Zusammenhang der Begriff IT definiert werden, da dieser die Grundlage für die meisten weiteren Betrachtungen bildet. Als Abkürzung bedeutet IT nur Informationstechnologie. Damit ist jede Technologie gemeint, die Informationen aufnimmt, speichert, weiterleitet, anzeigt oder verarbeitet.

Allerdings hat sich der Begriff in der letzten Zeit stark weiterentwickelt und erstreckt sich über mehrere Ebene. Die unterste Ebene bildet die IT-Infrastruktur und stellt hauptsächlich Hardware dar, also die technische Ebene. Hier sind jegliche Endgeräte angesiedelt, welche von Menschen zur Anzeige von Informationen genutzt werden, aber auch Server und jegliche Netzwerkverbindungen.

Darüber liegt die Ebene der IT-Funktionen, welche hauptsächlich von Software bestimmt wird. Als Beispiele dienen hier Applikationen zur Verarbeitung von Daten, aber auch jede Art von Betriebssystem. Eine oder mehrere Applikationen stellen dann meist einen IT-Service dar, wie zum Beispiel der Betrieb einer Webseite.

Die dritte Ebene beinhaltet die Organisation an sich und stellt die Prozesse innerhalb dieser in den Vordergrund. Dabei werden aus den IT-Services der zweiten Ebene Geschäftsprozesse dargestellt, welche von der Organisationsstruktur betreut werden.

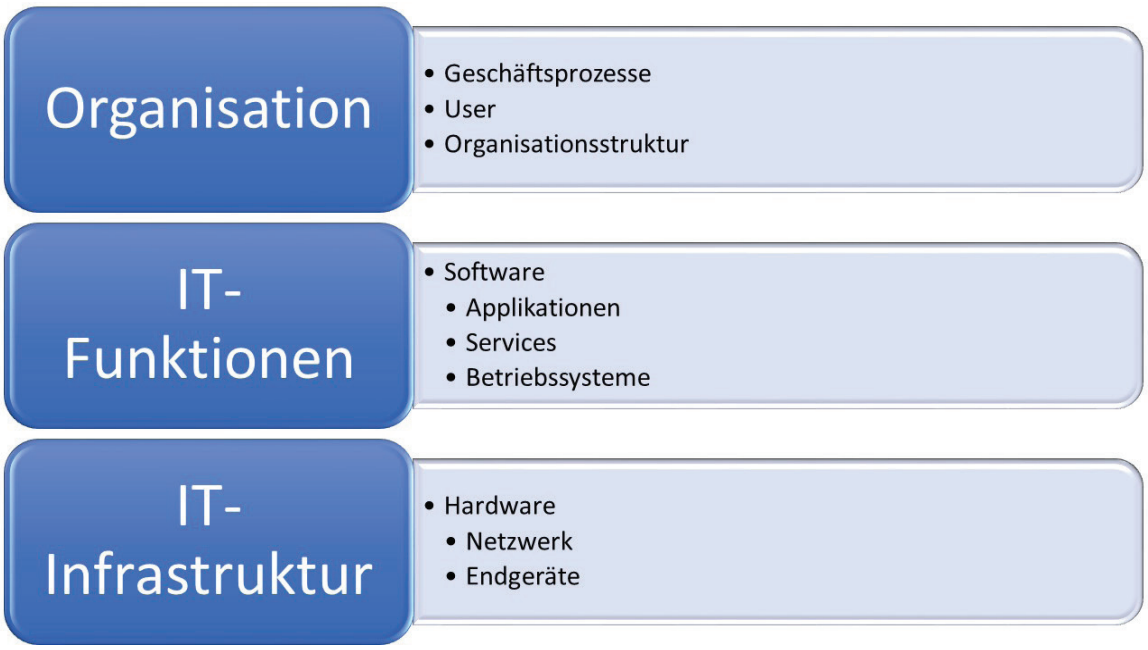

Abb. 1.1 Ebenen der IT

Diese Erweiterung des Begriffes IT ist extrem wichtig, um den Begriff IT-Sicherheit komplett zu definieren, denn IT-Sicherheit bezieht sich auf alle eben beschriebenen Aspekte und nicht nur auf die eigentliche Technologie. Die Technologie kann perfekt abgesichert sein, aber es existieren Angriffsszenarien, welche einzig und allein die Organisationsstrukturen ausnutzen. So wird bei der so genannten Chef-Masche (auch ‚CEO-Fraud') ein Mitarbeiter aus der Buchhaltung von einem Angreifer kontaktiert. Der Angreifer gibt vor der Chef des Unternehmens zu sein und es soll schnellstmöglich eine Überweisung auf ein bestimmtes Konto vorgenommen werden. Wenn keine Kontrollmechanismen für diesen Fall vordefiniert sind, dann wird der Mitarbeiter das Geld aus Gehorsam überweisen und der Angriff war erfolgreich.

Nachdem der Begriff IT beschrieben ist, kann IT-Sicherheit definiert werden. Der Begriff IT-Sicherheit besitzt ebenfalls verschiedene Definitionen, welche sich im Laufe der Zeit geändert haben. Zu Beginn wur-

de IT-Sicherheit als die Abwesenheit von Gefahren und Schwachstellen definiert. Diese Sichtweise ist nicht mehr zeitgemäß, denn es gibt kein System, welches keiner Gefahr ausgesetzt ist und welches keine Schwachstellen besitzt. Die Fülle der Angriffsvektoren und vernetzter Systeme ist zu groß.

Später wurde IT-Sicherheit, unter anderem vom Bundesamt für Sicherheit in der Informationstechnologie (BSI), als die Existenz angemessener Sicherungsmaßnahmen beschrieben. Dies rührt vor Allem von der Herangehensweise des BSI zum Informationssicherheitsmanagement her. Der IT-Grundschutz des BSI stellt Standard-Risiken der IT-Sicherheit Standard-Sicherungsmaßnahmen gegenüber. Mehr dazu in Abschnitt 1.4.

In neueren Publikationen wird IT-Sicherheit als individueller Begriff definiert, der von verschiedenen Faktoren abhängt. Zu diesen Faktoren gehören Anforderungen an die IT und die Bereitschaft zur Risikoübernahme. Außerdem wird davon ausgegangen, dass niemals 100% Sicherheit erreicht wird. Informationssicherheitsmanagement versucht somit eher die IT-Unsicherheit angemessen zu reduzieren.

Diese letzte Definition, welche vor Allem auf Angemessenheit von IT-Sicherheit beruht, baut Analogien zum Gesundheitsbegriff auf. Gesundheit wird in der Medizin weder als Abwesenheit von Krankheiten, noch als Existenz von medizinischen Maßnahmen gesehen, sondern als Zustand des physischen und psychischen Wohlbefindens.

Um die Definition der IT-Sicherheit zu vervollständigen, muss zusätzlich der Umfang beschrieben werden. Im Zuge der Definition von IT wurden bereits die drei Ebenen beschrieben, welche IT umfasst. IT-Sicherheit muss ebenfalls diese drei Ebenen umfassen. Wie das Beispiel CEO-Fraud zeigt, reicht es nicht allein die Technologie. abzusichern.

Weiterhin kann IT-Sicherheit in drei Teilbereiche ausgespaltet werden. Dies lässt sich am besten mit den drei englischen Begriffen für Sicherheit beschreiben. Im Englischen wird IT-Sicherheit in Safety, Security und Privacy zerlegt.

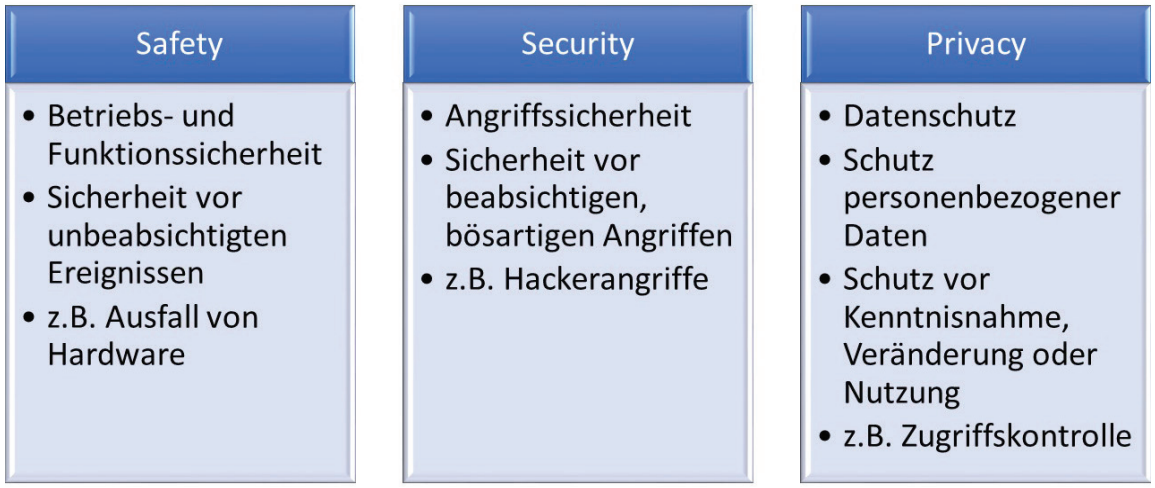

Abb. 1.2 IT-Sicherheitsbegriffe

Die Aspekte Safety und Security wurden bereits mit den Beispielen in der Einführung als Teil von IT-Sicherheit gezeigt. Privacy bildet einen weiteren, bisher nicht erwähnten, Teil der IT-Sicherheit. Die deutsche Übersetzung von Privacy ist Datenschutz. Eine Verletzung des Datenschutzes kann sowohl durch einen Hackerangriff verursacht werden, aber auch durch den Zugriff eines unberechtigten Mitarbeiters auf besonders schützenswerte, personenbezogene Daten. Vor allem im Zuge der DSGVO hat das Thema Datenschutz wesentlich an Bedeutung gewonnen und damit auch IT-Sicherheit.

Ein letzter Aspekt zum Begriff IT-Sicherheit betrifft die Verwandtschaft zur Informationssicherheit. Ursprünglich wurde Informationssicherheit der IT-Sicherheit übergeordnet und beinhaltete zusätzlich den Schutz der Daten, welche nicht digital gespeichert oder verarbeitet wurden. Die klassische Datenverarbeitung mit Stift Papier gehörte also nur zur Informationssicherheit, aber nicht zur IT-Sicherheit. Da diese Unterscheidung aber inzwischen obsolet ist, da sich digitale und analoge Prozesse zunehmend vermischen, werden in der aktuellen Forschung und Publikationen Informationssicherheit und IT-Sicherheit synonym verwendet. Dieser Vorgehensweise folgt auch dieses Buch.

Damit ist der grundlegende Begriff IT-Sicherheit ausreichend erläutert. Weitere Grundbegriffe folgen jetzt.

Eine Bedrohung ist ein Umstand oder Ereignis, durch den oder das die IT-Sicherheit beeinträchtigt werden kann und in dessen Folge ein Schaden entstehen kann. Bedrohungen sind also potentielle Ausgangspunkte für Gefährdungen.

Eine Gefährdung bzw. Gefahr entsteht, wenn beispielsweise eine Schwachstelle bei einem Angriff ausgenutzt wird. Die Bedrohung eines möglichen Hackerangriffs wird durch den tatsächlichen Angriff zur Gefahr. Es kommt zu einer Beeinträchtigung der IT und die Folge ist eine Verletzung eines der Informationssicherheitsziele (siehe Abschnitt 1.3).

Angriffe sind Aktionen, deren Ziel eine Verletzung der Sicherheit ist. Sie sind eine vorsätzliche Form der Gefährdung und nutzen in der Regel gezielt Schwachstellen der IT aus. Personen, die derartige Aktionen durchführen, werden als Angreifer bezeichnet. Angreifer verfolgen ein bestimmtes, meist illegales Ziel.

Sicherungsmaßnahmen sind Vorkehrungen und Methoden, die geeignet sind, die IT-Sicherheit zu erhöhen. Dies können sowohl organisatorische als auch technische Maßnahmen sein. Sicherungsmaßnahmen wirken zum Beispiel gegen identifizierte Schwachstellen.

Außerdem muss der Unterschied zwischen Daten und Informationen erläutert werden. Daten werden von Technologie übertragen, gespeichert oder verarbeitet. Wenn ein Mensch diese Daten interpretiert wird daraus eine Information.

1.3 Informationssicherheitsziele

Informationssicherheit hat mehrere Ziele. Diese Ziele beinhalten den Schutz von Informationen. Aus diesem Grund werden diese auch als Schutzziele bezeichnet. Jedes dieser Informationssicherheitsziele beschreibt eine Eigenschaft von Informationen, welche geschützt werden muss. Dabei muss teilweise zwischen Informationen und Daten unterschieden werden.

Die Informationssicherheitsziele sind Vertraulichkeit, Integrität und Verfügbarkeit. Eine Eselsbrücke, um sich diese drei Ziele zu merken, bilden die Anfangsbuchstaben der englischen Bezeichnungen - **CIA**:

- **C**onfidentiality
- **I**ntegrity
- **A**vailability

Abb. 1.3 Informationssicherheitsziele

Im Folgenden werden die Informationssicherheitsziele genauer erläutert und welche Ursachen für einen Verlust des Schutzziels verantwortlich sein können.

1.3.1 Vertraulichkeit

Vertraulichkeit beschreibt die Eigenschaft einer Information, nur dem vorgesehenen beziehungsweise autorisierten Personenkreis (den Befugten) bekannt zu sein. Es ist klar, dass die Vertraulichkeit eine Eigenschaft oder ein Attribut einer Information ist. Dabei ist die Unterscheidung zwischen Daten und Informationen ausschlaggebend. Liegt eine Information in Datenform vor, so kann sich die Forderung nach Vertraulichkeit natürlich auch auf die Daten (und Datenträger) übertragen. Das dies aber nicht zwingend ist zeigt folgendes Beispiel: Wird zum Beispiel eine Verschlüsselung genutzt um die Vertraulichkeit von Daten

zu schützen, müssen die verschlüsselten Daten nicht mehr vertraulich behandelt werden, sofern die Verschlüsselung ordnungsgemäß durchgeführt wurde.

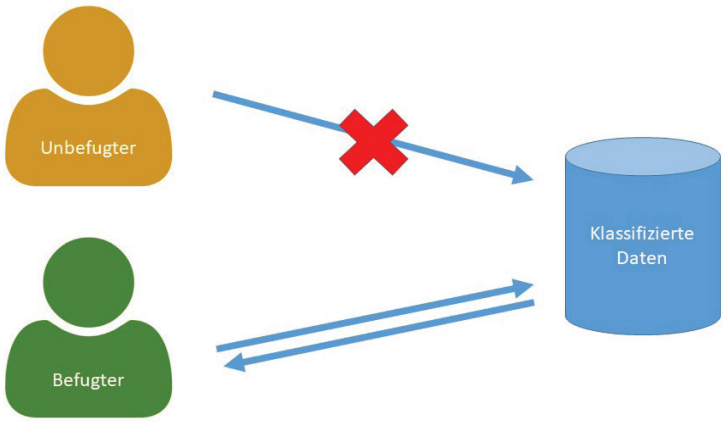

Abb. 1.4 Schematische Darstellung der Vertraulichkeit

Daraus folgt direkt, dass jemand den Kreis der Befugten festlegen und diesen autorisieren muss. Hierfür gibt es zwei Alternativen:

- der Urheber oder Eigentümer der Information (derjenige, bei dem die Information entsteht, der sie als Erster „besitzt“) oder
- eine zentrale Stelle, der die Informationen zur Festlegung der Befugten vor einer möglichen Verarbeitung oder Weitergabe vorgelegt werden.

Im ersten Fall spricht man von einer benutzerbestimmbaren Zugriffskontrolle, im zweiten Fall von einer vorgeschriebenen Zugriffskontrolle.

Bei Letzterem findet eine solche Festlegung oft in Form einer Einstufung statt: Informationen werden als offen oder vertraulich oder nur für Mitarbeiter bestimmter Abteilungen oder Projekte klassifiziert. In staatlichen Geheimdiensten sind dafür Klassen wie vertraulich, geheim und streng geheim festgelegt. Zugriff zu den Informationen mit einer solchen Einstufung haben nur Subjekte mit einer Freigabe für die entsprechende Stufe.

In der Praxis gibt es eine Reihe von Mischformen dieser beiden grundsätzlichen Formen der Zugriffskontrolle. Daraus ergibt sich dann das Berechtigungskonzept.

Entscheidend für die Zugriffskontrolle und damit für den Schutz der Vertraulichkeit ist die Authentizität der befugten Personen. Authentizität beschreibt die Echtheit von befugten Personen. Dies wird in der Praxis nahezu immer durch Benutzername und Passwort gelöst. Weitere Möglichkeiten zur Sicherstellung der Authentizität sind biometrische Verfahren (Fingerabdruck, Irisscan) oder der Einsatz von Einmalpasswörter (TAN, Hardwaretoken oder Ähnliches). Wenn die Authentizität verletzt ist, weil zum Beispiel die Kombination von Benutzername und Passwort einem Unbefugten zur Kenntnis gelangt ist, dann schützt die Zugriffskontrolle die Vertraulichkeit der Information ebenfalls nicht.

Einige Autoren nennen Authentizität jeglicher Elemente der IT sogar als weiteres Ziel der Informationssicherheit.

Kommen wir nun zum Verlust der Vertraulichkeit. Dieser Fall tritt ein, wenn vertrauliche Informationen Unbefugten zur Kenntnis gelangen. Einige Beispiel dafür sind:

- In einem Netzwerk werden Datenpakete auf dem Übertragungsweg von Unbefugten abgehört.
- Bei einem ansonsten vor Verlust der Vertraulichkeit geschützten IT-System wird täglich ein Backup der Daten ausgeführt. Die Backups liegen ohne Zugriffskontrolle auf einem unverschlüsselten Cloud-Server und Unbefugte können ungehindert zugreifen.
- Durch Schwachstellen in einem IT-System können Angreifer das IT-System penetrieren und vertrauliche Daten in großer Menge stehlen.

Ein Grundproblem der Vertraulichkeit ist, dass man Informationen und Daten einen Verlust der Vertraulichkeit nicht ansehen kann. Es kann also leicht passieren, dass die Vertraulichkeit längst nicht mehr gegeben ist, die Befugten dies jedoch nicht wissen. Das zweite der genann-

ten Beispiele für den Verlust der Vertraulichkeit ist so im Jahr 2020 bei der Autovermietung Buchbinder passiert. Ein Sicherheitsforscher hat das unverschlüsselte Backup auf einem öffentlich zugänglichen Server gefunden. Die Vertraulichkeit der Daten war zu diesem Zeitpunkt vermutlich schon lange verletzt, aber niemand hat dies bemerkt. Erst nach Bekanntwerden dieser Fehlkonfiguration wurden Zugriffskontrollen für dieses Backup eingeführt.

Als Nächstes kommen wir zu den Ursachen für den Verlust der Vertraulichkeit. Grundsätzlich müssen zwischen zwei Ursachentypen unterschieden werden:

- Schwachstellen in Systemen, aufgrund derer Unbefugte an vertrauliche Informationen gelangen,
- der Weitergabe von vertraulichen Informationen durch Befugte an Unbefugte.

Das Risiko des ersten Ursachentyps kann durch technische Sicherheitsmaßnahmen reduziert werden. Der zweite Ursachentyp gliedert sich auf in missbräuchliche Weitergabe und versehentliche Weitergabe. Wenn die Regeln für die Klassifikation von Informationen nicht klar definiert sind, können Informationen durch versehentliche Weitergabe an Unbefugte gelangen.

Missbräuchliche Weitergabe setzt einen internen Angreifer voraus. Gegen diese Art von Angriff kann man sich extrem schwer schützen, da ein interner Akteur immer gewisse Rechte hat, welcher er für seine tägliche Arbeit benötigt, sodass weder Authentizitätsprüfungen, noch Zugriffskontrolle Schutz bieten. Hier helfen nur stark gegliederte Berechtigungssysteme oder Systeme zur Erkennung untypischen Verhaltens.

Ein Beispiel dafür bildet der Steuerskandal um Uli Hoeneß. Als dieser öffentlich wurde stiegen die Zugriffe innerhalb der bayerischen Finanzverwaltung auf den Datensatz von Herrn Hoeneß stark an. Auf den Datensatz hatten viele Sachbearbeiter Zugriff, aber nur wenige waren für die Bearbeitung des Datensatzes zuständig. Alle anderen Zugriffe

waren lediglich der medialen Aufmerksamkeit geschuldet. Dies ist aber nicht zulässig.

In diesem Fall hätte sowohl eine Erkennung untypischen Verhaltens (extrem hohe Zugriffszahlen auf einen Datensatz) als auch ein stark gegliedertes Berechtigungssystem (nur die tatsächlichen Bearbeiter eines Datensatzes sind berechtigt diesen zu öffnen) die Verletzung der Vertraulichkeit verhindert.

1.3.2 Integrität

Die Integrität ist die Eigenschaft von Daten, nur in zulässiger Weise durch Befugte geändert worden zu sein.

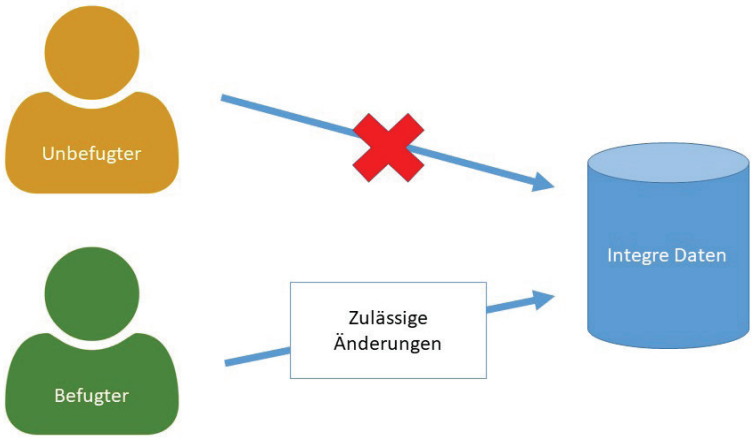

Abb. 1.5 Schematische Darstellung der Integrität

Unter Ändern versteht man das Abändern vorhandener Daten, das teilweise oder vollständige Löschen von Daten und das Hinzufügen neuer Daten. Die obige Definition von Integrität setzt voraus, dass die betrachteten Daten zu einem bestimmten Zeitpunkt

- als integer festgestellt,
- die zulässigen Änderungen als solche definiert wurden und
- der Kreis der Befugten festgelegt wurde.

Bezüglich des Löschens ist immer das Löschen von Daten in einer Datenstruktur (etwa einer Datei), ohne die Datenstruktur selbst zu löschen, gemeint. Integrität ist also genau genommen eine Eigenschaft des Inhalts einer Datenstruktur.

Für die Festlegung des Personenkreises der Befugten gibt es ähnliche Alternativen wie bei der Vertraulichkeit: Man überlässt sie dem Eigentümer der Daten oder einer zentralen Instanz. Auch diese Überlegungen finden ihren Niederschlag im Berechtigungskonzept.

In einem IT-System können Unbefugte zum Beispiel mit Mitteln der Zugriffskontrolle davon abgehalten werden, Daten zu ändern. Schwierig wird es, Befugte so zu überwachen, dass sie nur zulässige Änderungen vornehmen. Maßnahmen unter dieser Kategorie sind zum Beispiel Plausibilitätsprüfungen. Dies ist allerdings nicht immer möglich. Daten, die in einem bestimmten Format vorliegen, wie zum Beispiel IBAN-Nummern oder Steuernummern, können mit einer Plausibilitätsprüfung auf Fehler überprüft werden. Wird allerdings absichtlich eine valide, aber trotzdem falsche IBAN eingegeben, hat eine Plausibilitätsprüfung keine Wirkung.

Um hier in kritischen Fällen die Integrität zu wahren, hilft meistens nur das Vier-Augen-Prinzip.

Ein Verlust der Integrität liegt dann vor, wenn die Daten entweder

- durch Befugte in unzulässiger Weise oder
- durch andere Ursachen (unzulässig) geändert worden sind.

Bei der unzulässigen Änderung von Daten durch Befugte muss man wieder danach unterscheiden, ob dies unbeabsichtigt (durch Bedienungsfehler, auch vielleicht fahrlässig) oder beabsichtigt geschieht. Letzteres wollen wir als missbräuchliche Änderung von Daten bezeichnen.

Zu den anderen Ursachen zählen wir mehr zufällige Ursachen wie Fehlfunktionen der IT-Systeme oder Störungen bei der Datenübertragung sowie die Manipulation durch Unbefugte.

Eine Fehlfunktion der IT kann zum Beispiel zu einem Absturz eines Servers führen. Daraus resultiert meist ein Datenverlust, da einige Daten noch nicht vollständig in die Datenbank geschrieben wurde. So kann die Integrität einer Transaktion, zum Beispiel beim Onlinebanking verletzt werden. Ein anderes typisches Beispiel sind Computer-Viren und Computer-Würmer. Diese verletzten die Integrität von Software. Somit helfen Maßnahmen zum Virenschutz die Integrität von Software zu wahren.

Weitere wichtige Maßnahmen sind solche, die die Verletzung der Integrität von Daten nicht verhindern, aber erkennen lassen. Dazu werden hauptsächlich Hash-Funktionen als digitale Signaturen genutzt. Mehr dazu in Abschnitt 1.7.3.

Eine weitere Möglichkeit sind fehlerkorrigierende Codes. Dies sind Verfahren, um zum Beispiel störungsbedingte Änderungen an Daten auf dem Übertragungsweg oder am Speicherort erkennen und in beschränktem Maße automatisch beheben zu können.

Widmen wir uns noch der Frage, wann eine Verletzung der Integrität von Daten bemerkt wird. Frühestens dann, wenn man sie erneut verwenden will. Allerdings gibt es auch Techniken der Datenmanipulation, welche die Verletzung der Integrität nicht bemerken lassen. Hierzu zählt auch das Thema der Kollision von Hash-Funktionen.

1.3.3 Verfügbarkeit

Unter Verfügbarkeit wird die Eigenschaft von Daten verstanden, für Befugte bei Bedarf und dann in akzeptabler Zeit zur Verfügung zu stehen.

Ein Bedarf liegt immer dann vor, wenn ein Zugriff als Teil der zulässigen Verarbeitung erfolgen soll. In akzeptabler Zeit meint, dass die ge-

wünschten Daten mit einer noch als zulässig akzeptierten Verzögerung bereitstehen.

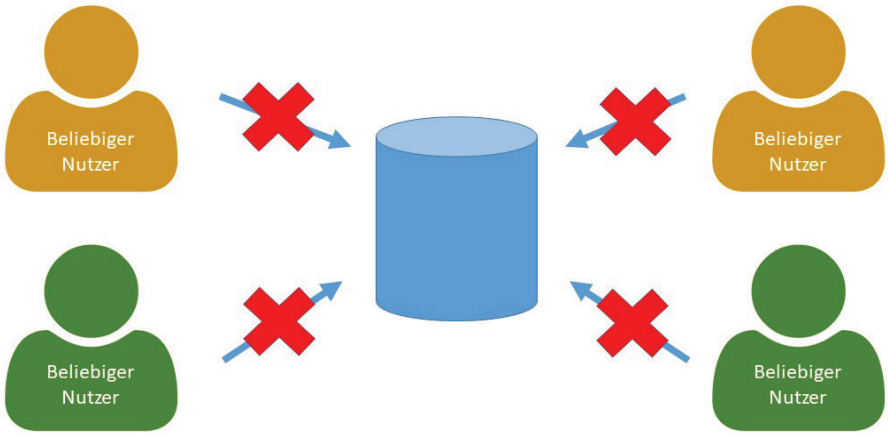

Abb. 1.6 Schematische Darstellung der Verfügbarkeit

Auch hier ist es möglich, dass die gerade noch akzeptierte Verzögerung durch den Eigentümer der Daten oder von einer zentralen Instanz festgelegt wird. Im internen Unternehmensumfeld liegt meistens der zweite Fall vor. Gegenüber Kunden legt meistens der Kunde fest, was für Ihn persönlich noch akzeptabel ist. Wenn diese Grenze unterschritten wird, sinkt der Wert für den Kunden. Dabei ist dies ein sehr individueller Wert.

Da Daten stets auf Datenträgern vorliegen, ist die Verfügbarkeit von Daten immer an die Verfügbarkeit von Datenträgern gebunden. Andererseits ist dies nicht hinreichend: Ein Datenträger kann im gewünschten Umfang verfügbar sein, aber die angeforderten Daten sind – zum Beispiel durch irrtümliche Löschung – nicht mehr verfügbar.

Typische Maßnahmen, um einen bestimmten Grad an Verfügbarkeit zu erreichen und aufrechtzuerhalten, sind

- Redundanzmaßnahmen (mehrfache Vorhaltung von Daten auf dem gleichen oder verschiedenen Datenträgern) und
- bestimmte Verfahren von Betriebssystemen zur Verwaltung konkurrierender Zugriffe, um Deadlocks beim Zugriff zu vermeiden.

Mehrfache Vorhaltung von Daten erreicht man im einfachsten Fall durch Erzeugen von Kopien auf dem gleichen Datenträger, regelmäßiges Backup der Daten auf separaten Datenträgern, parallele Speicherung auf mehreren Festplatten sowie Nutzung von Systemen für die Langzeitarchivierung. Praktische Beispiele für Redundanzmaßnahmen bei Datenträgern sind RAID-Systeme.

Der Verlust der Verfügbarkeit teilt sich in zwei Bereiche. Zum einen kann die Verfügbarkeit gar nicht mehr gegeben sein. Die Ursachen für den Verlust der Verfügbarkeit von Daten sind vielfältig:

- die Daten wurden gelöscht
- die Daten wurden versehentlich vernichtet
- der Nutzer hat kein Zugriffsrecht mehr auf die Daten
- unbeabsichtigte Handlungen von Personen (Befugte oder Unbefugte) wie zum Beispiel Bedienungsfehler, Fehler bei den Wartungsmaßnahmen, Fahrlässigkeit,
- technische Defekte und
- Manipulationen durch Unbefugte.

Eine andere Form des Verlustes der Verfügbarkeit von Daten liegt vor, wenn die Daten zwar vorhanden, aber nicht in akzeptabler Zeit zur Bearbeitung bereitgestellt werden können. Dies kann an nicht ausreichender Verfügbarkeit des IT-Systems oder anderer Prozesse liegen. Beispiele für einschränkende IT-Systeme sind zu langsame Verarbeitung von Daten (geringe Prozessorleistung) oder zu langsame Übertragung von Daten (geringe Bandbreite des Netzwerks). Ein Prozess, welcher die Verfügbarkeit einschränken kann, ist zum Beispiel das zu langsame Zurückspielen eines Backups.

Bitte beachten Sie, dass es bei der Verfügbarkeit nicht darauf ankommt, ob die bereitgestellten Daten unverändert sind – dies ist ein Integritätsaspekt, im Extremfall: Wird unzulässiger Weise der Inhalt einer Datei gelöscht (zum Beispiel durch Überschreiben mit Nullen), bleibt aber die

Datenstruktur als Datei erhalten, dann wurde die Integrität der Daten verletzt.

Der Verlust der Verfügbarkeit wird meist recht schnell entdeckt. Immer dann, wenn die Daten wieder bearbeitet werden, würde ein Verlust der Verfügbarkeit bemerkt werden.

Übungsaufgaben

1. Welche Sicherheitsziele sind durch den Ausfall eines Webserver in einem Unternehmen betroffen?
2. Der Befall eines Unternehmens mit Schadsoftware wird erst nach mehreren Wochen erkannt. Welche Sicherheitsziele sind potentiell gefährdet?

Musterlösung

1. Der Ausfall des Webservers führt unmittelbar zum Verlust der Verfügbarkeit. Dokumente und Dienste, die vorher durch den Webserver zur Verfügung gestellt werden, können nicht mehr genutzt werden.

   Für den Fall, dass andere Webdokumente auf Inhalte des ausgefallenen Webservers verweisen bzw. diese einbetten (zum Beispiel bei der Verwendung von Frames), verändert sich der Inhalt dieser Webdokumente (es fehlen ggf. einige Teile). Die Integrität der Dokumente wird verletzt.

   Außerdem kann es sein, dass unmittelbar durchgeführte Transaktionen (zum Beispiel Buchungen oder Überweisungen) nicht mehr gespeichert wurden, sodass die Integrität einer gewissen Menge an Transaktionen verletzt ist.

   Weitere Sicherheitsziele sind nicht unmittelbar gefährdet.

2. Die Verletzung von Integrität und Vertraulichkeit sieht man Daten nicht direkt an, sodass die Verletzung dieser beiden am wahrscheinlichsten ist.

   Die Verfügbarkeit wurde, wenn dann nur geringfügig beeinträchtigt, denn jede stärkere Einschränkung der Verfügbarkeit wäre sofort aufgefallen und nicht erst nach mehreren Wochen.

1.4 Informationssicherheitsmanagement

1.4.1 Grundlagen

Wie bereits beschrieben hängt die Funktions- und Leistungsfähigkeit von Unternehmen entscheidend von der Informationssicherheit ab. Um diese zu gewährleisten müssen die Verantwortlichen zunächst einige Dinge genau bestimmen:

- was in welchem Fall als sicher zu verstehen ist
- welche IT-Systeme in welchem Maße geschützt werden sollen
- wie hoch die Kosten und der Aufwand für die Einführung und den Betrieb von Sicherungsmaßnahmen sein dürfen
- welches Risiko sie bereit sind, trotz implementierter Maßnahmen weiter zu tragen (Restrisiko)

Die Bearbeitung dieser Punkte erfolgt unter sich ständig ändernden Gegebenheiten. Demzufolge ist das Erreichen von IT-Sicherheit kein einmaliges Projekt, sondern ein sich stets wiederholender Prozess. Die Planung, Steuerung und Kontrolle dieses Prozesses ist Aufgabe des Informationssicherheitsmanagements.

Zusammengefasst beinhaltet Informationssicherheitsmanagements oder IT-Sicherheitsmanagement alle

- Führungsaufgaben
- Führungstechniken
- Führungsmittel
- Aspekte der Organisation

die sich mit IT-Sicherheit beschäftigen.

Der Zweck des IT-Sicherheitsmanagements ist die Erreichung der Informationssicherheitsziele (siehe Abschnitt 1.3) und damit das Abwenden

von Schäden an der IT und auch Schäden, welche durch die IT verursacht werden. Wobei der Grad der Erreichung wesentlich von der Risikobereitschaft der Akteure abhängt. Dieser geforderte oder erreichte Grad an Sicherheit wird im Informationssicherheitsniveau beschrieben. Dieses Niveau ist natürlich keine Zahl, sondern wird in Schutzklassen oder Absicherungsvarianten umgesetzt. Dazu später mehr in Abschnitt 1.4.2.

Die Umsetzung des geforderten Informationssicherheitsniveaus wird über das IT-Sicherheitskonzept geplant. Ein IT-Sicherheitskonzept ist ein Entwurf der geplanten Vorgehensweise zur Erreichung und Erhaltung eines gewünschten oder geforderten Sicherheitsniveaus. Damit wird die IT-Sicherheitsstrategie eines Unternehmens erfüllt.

In einer IT-Sicherheitsstrategie verankert die Leitung einer Organisation grundlegende Aussagen zum Stellenwert der IT-Sicherheit und der Ziele, die damit erreicht werden sollen. Die wichtigsten Aussagen der IT-Sicherheitsstrategie werden in einer Leitlinie zur Informationssicherheit oder IT-Sicherheitsleitlinie dokumentiert. Dazu gehören zum Beispiel die grobe Definition der Informationssicherheitsziele für verschiedene Organisationsbereiche, die Festlegung der IT-Sicherheitsorganisation sowie die Beschreibung von allgemeinen Maßnahmen zur Planung, Entwicklung, Durchsetzung und Kontrolle der verschiedenen Aufgaben des Sicherheitsmanagements. Detaillierte Sicherungsmaßnahmen sind nur Bestandteil des Sicherheitskonzepts.

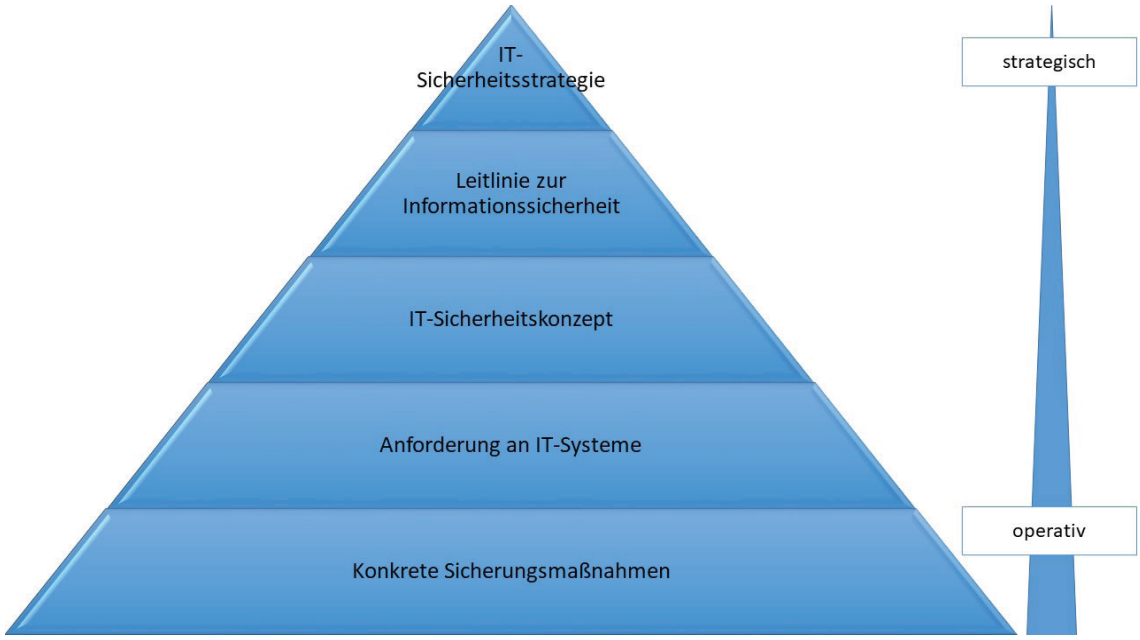

Abb. 1.7 Dokumente des Informationssicherheitsmanagements

Die Abb. 1.7 zeigt die wichtigsten Konzepte des Informationssicherheitsmanagements in einer Pyramide. Natürlich kann es je nach Organisation weitere Konzepte oder Dokumente geben, aber dies sind die Wichtigsten. Umso weiter oben ein Konzept angeordnet ist, umso strategischer ist dieses angelegt. Die Anforderungen an die IT-Systeme und die konkreten Sicherungsmaßnahmen hingegen sind eher für die operative Ebene.

Dies bedeutet, dass eine IT-Sicherheitsstrategie nur grobe Ziele vorgeben wird, wie zum Beispiel „Unsere extern erreichbaren Webapplikationen müssen besonders abgesichert sein“. Hier werden keine konkreten Maßnahmen oder Zielerreichungsgrade genannt.

Die Sicherungsmaßnahmen auf der untersten Ebene sind hingegen sehr konkret. Hier werden explizit Konfiguration von Betriebssystemen oder die Mindestlänge eines Passworts festgelegt.

Ein weiterer Aspekt ist die Langlebigkeit der jeweiligen Konzepte. Je strategischer ein Dokument ist, desto seltener wird es geändert. Dies liegt daran, dass eine Neuausrichtung der Strategie wesentliche Änderung in allen Bereichen nach sich ziehen würde, aber auch daran, dass

die Aussagen der Strategie sehr generisch sind und somit nicht so oft einer Änderung bedürfen.

Die konkreten Sicherungsmaßnahmen dagegen werden sich eventuell täglich ändern, wenn neue Schwachstellen oder Angriffsmöglichkeiten veröffentlich werden, muss ein IT-System anders konfiguriert oder eingesetzt werden als am Tag davor.

1.4.2 ISMS

Ein ISMS ist ein Informationssicherheitsmanagementsystem. Dieses umfasst alle Aufgaben die zur Implementierung des Informationssicherheitsmanagements notwendig sind. Dies bedeutet das ISMS entwirft unter anderem alle im vorherigen Abschnitt genannten Konzepte und Dokumente. Außerdem enthält das ISMS die notwendigen Verantwortungsbereiche und Organisationsstrukturen um die geforderte Informationssicherheit zu erreichen. Das ISMS dient also dazu alle Ziele der IT-Sicherheit zu erreichen.

Der Aufbau eines ISMS kann von einem Unternehmen oder einer Organisation natürlich alleine vorgenommen werde, allerdings ist dies extrem aufwendig und ressourcenintensiv. Aus diesem Grund existieren gleich mehrere Standards und Leitfäden, welche dabei helfen ein ISMS aufzubauen.

Die Nutzung solcher Standards hat mehrere Vorteile:

- Verringerung der Wahrscheinlichkeit, dass wichtige Punkte, zum Beispiel gesetzliche oder gesetzesähnliche Regelungen, vergessen werden
- Reduktion des Aufwands für die Konzeption des Managementsystems, durch Vorgabe von Aufgaben, Rollen sowie Strukturen
- Leitfäden und Standards bieten eine gemeinsame Sprachgrundlage über die Grenzen von Unternehmen und Organisationen hinweg
- Vorgaben für die Dokumentation des ISMS

- Option zur Zertifizierung und damit der Erhöhung der Nachvollziehbarkeit und Transparenz der Bemühungen um IT-Sicherheit auch für externe Interessengruppen
- Erleichterung der Zusammenarbeit von Unternehmen und Organisationen in der IT-Sicherheit

Einige der verbreitetsten Standards werden im Folgenden auch beschrieben. Grundsätzlich gibt es jedoch zwei Vorgehensweisen bei der Erarbeitung eines ISMS:

- Risikoanalyse oder
- Grundschutz

Eine Risikoanalyse ist ein systematischer Prozess zur Identifikation und Einschätzung des Umfangs von Risiken. Bei der Durchführung einer Risikoanalyse werden mögliche Bedrohungen und Gefahren ermittelt, analysiert und bewertet, um anschließend angemessene Sicherungsmaßnahmen zur Vermeidung, Verringerung bzw. Begrenzung von erkannten Risiken ergreifen zu können. Dabei folgt der Prozess der Risikoanalyse meist dem Schema aus Abb. 1.8.

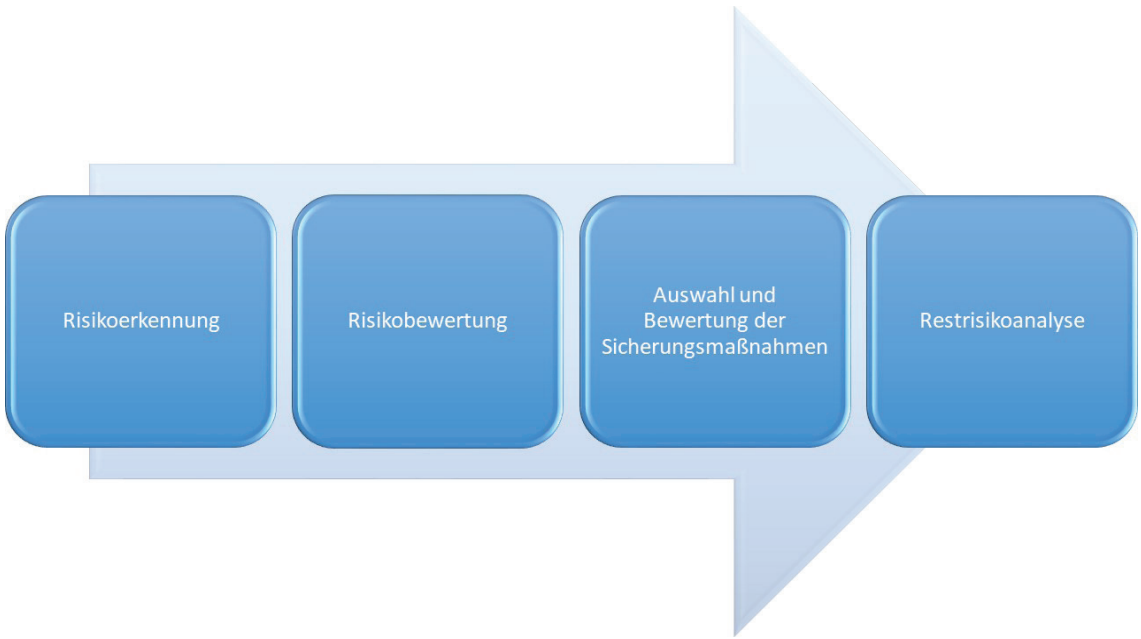

Abb. 1.8 Prozess der Risikoanalyse

Zuerst müssen die Risiken gefunden und erkannt werden, um diese anschießend zu bewerten. Für diese Risiken müssen dann entsprechende Sicherungsmaßnahmen ausgewählt werden. Die Restrisikoanalyse zeigt dann, ob die Maßnahmen bereits ausreichen.

Der Ansatz der Risikoanalyse wird in vielen Managementsystemen genutzt und ist weit verbreitet. Grundsätzlich werden spezifisch für die aktuellen Gegebenheiten die Risiken bestimmt, um darauf abgestimmt Maßnahmen zu finden, welche das Restrisiko so weit verringern, dass dies akzeptiert werden kann.

Die andere Art zur Entwicklung eines ISMS bietet die Vorgehensweise eines Grundschutzes. Beim Grundschutz handelt es sich um einen Best-Practice-Ansatz. Die Entwicklung eines IT-Sicherheitskonzepts erfolgt durch Auswahl von allgemein anerkannten und für notwendig erachteten Sicherungsmaßnahmen. Idealerweise gibt es Leitfäden bzw. Checklisten von anerkannten Autoritäten, die für typische IT-Systeme Standard-Sicherungsmaßnahmen vorschlagen, die ein Mindestmaß an IT-Sicherheit ermöglichen. Die Angemessenheit der Sicherungsmaßnahmen wird mit der „üblichen Praxis“ in vergleichbaren Organisationen begründet. Die Auswahl der Maßnahmen erfolgt, ohne die tatsächlich vorhandenen Risiken näher zu untersuchen.

Die Idee des Grundschutzes lautet kurz zusammengefasst: Mit vertretbarem Aufwand sollen Standard-Risiken mithilfe von Standard-Sicherungsmaßnahmen bekämpft werden, um damit ein Standard-Sicherheitsniveau zu erreichen. Damit ähnelt der Grundschutz einer ABC-Analyse (siehe Abb. 1.9).

Alle Programmcodes aus diesem Buch sind als PDF zum Download verfügbar. Dadurch müssen Sie sie nicht abtippen:
https://bmu-verlag.de/hacking-und-it-security/

Außerdem erhalten Sie die eBook Ausgabe zum Buch im PDF Format kostenlos auf unserer Website:

https://bmu-verlag.de/hacking-und-it-security/
Downloadcode: siehe Kapitel 3