

LERNEN EINFACH GEMACHT



IT-Sicherheit

für
dummies[®]



Technische Bausteine
kennen: Verschlüsselung,
Biometrie, Software, Hardware

Rechtliche Anforderungen
und Standards im Blick: DSGVO,
BDSG, ISO-Normen und mehr

IT-Sicherheit im Unternehmen
umsetzen

Rainer W. Gerling
Sebastian R. Gerling

IT-Sicherheit für Dummies

Schummelseite

DEUTSCHE GESETZE

In der Informationssicherheit sind die nachfolgenden Gesetze von besonderer Relevanz:

- ✓ BSI-Gesetz
- ✓ Telekommunikationsgesetz (TKG)
- ✓ Bundesdatenschutzgesetz (BDSG)
- ✓ Telemediengesetz (TMG)
- ✓ Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG)
- ✓ Geschäftsgeheimnisgesetz
- ✓ §§ 75b und 75c Sozialgesetzbuch V (SGB V)

WICHTIGE NORMEN

Die folgenden Normen sind Orientierungen bei der Gestaltung der Informationssicherheit:

- ✓ ISO-27000-Reihe
- ✓ BSI-Standards
- ✓ BSI-Grundsatzkompendium
- ✓ VdS-10000-Reihe
- ✓ TISAX
- ✓ CISIS 12
- ✓ DIN 66398 und 66399
- ✓ Common Criteria
- ✓ PCI-DSS
- ✓ ITIL

EUROPÄISCHE REGELUNGEN

Diese Verordnungen und Richtlinien spielen auf europäischer Ebene eine wichtige Rolle:

- ✓ Datenschutz-Grundverordnung
- ✓ Netzwerk- und Informationssicherheitsrichtlinie
- ✓ ePrivacy-Richtlinie
- ✓ Cybersecurity-Verordnung

SONSTIGE DOKUMENTE

Diese Standards und Dokumente machen spezifische Vorgaben, sind aber trotzdem von allgemeinem Interesse:

- ✓ Federal Information Processing Standards (FIPS)
- ✓ Branchenspezifische Sicherheitsstandards (B3S) nach § 8a Abs. 2 BSI-Gesetz
- ✓ Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung 2018
- ✓ VDA-ISA-Katalog
- ✓ Informationssicherheitsmanagement – Grundsatzpapier der Rechnungshöfe des Bundes und der Länder
- ✓ Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit

MERKBLÄTTER FÜR BESCHÄFTIGTE

Diese Merkblätter sollten den jeweiligen Beschäftigten übergeben werden:

- ✓ IT-Sicherheitsleitlinie des Unternehmens
- ✓ Passwortrichtlinie
- ✓ Nutzerordnung
- ✓ Merkblatt für Dienstreisen mit IT-Geräten
- ✓ Merkblatt zur Verschlüsselung von E-Mails

- ✓ Merkblatt zum Umgang mit Geschäftsgeheimnissen
- ✓ Datenschutzmerkblatt
- ✓ Meldung von Sicherheitsvorfällen

ROLLEN IN DER IT-SICHERHEIT

Die folgenden Rollen und Gremien sollten im Unternehmen beschrieben und besetzt werden:

- ✓ Informationssicherheitsbeauftragte/r
- ✓ Datenschutzbeauftragte/r
- ✓ Chief Information Officer
- ✓ Chief Digital Officer
- ✓ IT-Leiter
- ✓ Krisenstab

PC FÜR DAS HOME OFFICE

Diese Maßnahmen sollten für einen PC im Home Office konfiguriert werden:

- ✓ VPN konfigurieren
- ✓ Token für 2FA beim VPN übergeben
- ✓ Festplattenverschlüsselung mit Pre-Boot Authentication einrichten
- ✓ automatische Aktualisierung des Virenschanners aktivieren
- ✓ Bildschirmschoner nach 5 Minuten konfigurieren

NOTEBOOK FÜR DIENSTREISE

Diese Maßnahmen sollten für ein Notebook für Dienstreisen konfiguriert werden:

- ✓ VPN konfigurieren
- ✓ Token für 2FA beim VPN übergeben

- ✓ Festplattenverschlüsselung mit Pre-Boot Authentication einrichten
- ✓ automatische Aktualisierung des Virens scanners aktivieren
- ✓ Bildschirmschoner nach 5 Minuten konfigurieren
- ✓ Sichtschutzfolie am Bildschirm anbringen
- ✓ Desktop-Firewall konfigurieren
- ✓ Kabel mit Schloss bereitstellen



Rainer W. Gerling, Sebastian R. Gerling

IT-Sicherheit für **dummies**[®]

Fachkorrektur von Ronald Petrlic

WILEY
WILEY-VCH GmbH

IT-Sicherheit für Dummies

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.

© 2022 Wiley-VCH GmbH, Boschstraße 12, 69469 Weinheim, Germany

All rights reserved including the right of reproduction in whole or in part in any form. This book published by arrangement with John Wiley and Sons, Inc.

Alle Rechte vorbehalten inklusive des Rechtes auf Reproduktion im Ganzen oder in Teilen und in jeglicher Form. Dieses Buch wird mit Genehmigung von John Wiley and Sons, Inc. publiziert.

Wiley, the Wiley logo, Für Dummies, the Dummies Man logo, and related trademarks and trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries. Used by permission.

Wiley, die Bezeichnung »Für Dummies«, das Dummies-Mann-Logo und darauf bezogene Gestaltungen sind Marken oder eingetragene Marken von John Wiley & Sons, Inc., USA, Deutschland und in anderen Ländern.

Das vorliegende Werk wurde sorgfältig erarbeitet. Dennoch übernehmen Autoren und Verlag für die Richtigkeit von Angaben, Hinweisen und Ratschlägen sowie eventuelle Druckfehler keine Haftung.

Coverfoto: © Jonathan Schöps – stock.adobe.com

Korrektur: Matthias Delbrück, Dossenheim/Bergstraße

Print ISBN: 978-3-527-71852-8
ePub ISBN: 978-3-527-83357-3

Über die Autoren

Rainer W. Gerling beschäftigt sich seit über 40 Jahren beruflich mit Informationstechnologie und hat bereits 1986 einen der ersten Artikel in Deutschland über Computerviren veröffentlicht. Nach dem Studium der Physik an der Universität Dortmund von 1974 bis 1979 schloss er 1981 seine Promotion und 1986 seine Habilitation an der Universität Erlangen-Nürnberg ab. Von 1981 bis 1993 war er wissenschaftlicher Assistent und Privatdozent an der Universität Erlangen-Nürnberg.

Nach seiner Tätigkeit als Wissenschaftler war Rainer W. Gerling von 1993 bis 2013 Datenschutzbeauftragter und von 2006 bis 2020 IT-Sicherheitsbeauftragter der Max-Planck-Gesellschaft. Seit 1994 ist er Lehrbeauftragter an der Hochschule München und wurde 2006 zum Honorarprofessor für IT-Sicherheit an der Hochschule München ernannt. Er ist seit 2012 stellvertretender Vorsitzender des Vorstands der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD). Als Mitbegründer und von 2008 bis 2020 als Vorsitzender des Arbeitskreises Informationssicherheit der deutschen Forschungseinrichtungen (AKIF) hat er maßgeblich die Behandlung des Themas Informationssicherheit an deutschen Hochschulen und Forschungseinrichtungen mitgeprägt.

Darüber hinaus ist er seit 1996 freiberuflicher Trainer und Berater für Datenschutz und IT-Sicherheit.

Sebastian R. Gerling beschäftigt sich seit über 20 Jahren beruflich mit Informationstechnologie und ganzheitlicher Strategieentwicklung im Umfeld von Hochschulen und Forschungseinrichtungen. Erfahrungen sammelte er dabei seit 2000 insbesondere in der

Abteilung Informations- und Kommunikationstechnologie in der Generalverwaltung der Max-Planck-Gesellschaft, den Max-Planck-Instituten für Informatik und Softwaretechnik, der Universität des Saarlandes, dem »CISPA – Center for IT-Security, Privacy and Accountability« und dann am »CISPA – Helmholtz-Zentrum für Informationssicherheit« sowie der Universität Hamburg.

Nach dem Bachelor-und Masterstudium der Informatik an der Universität des Saarlandes zwischen 2004 und 2009, schloss er im Rahmen eines Promotionsstipendiums der International Max Planck Research School for Computer Science 2014 die Promotion an der Universität des Saarlandes ab. Nach seiner Tätigkeit als wissenschaftlicher Mitarbeiter an der Universität des Saarlandes 2012 bis 2014 war er von 2012 bis 2017 administrativer Leiter des »CISPA – Center for IT-Security, Privacy and Accountability«. Von 2018 bis 2019 war er Leiter der Stabsstelle Wissenschaftsstrategie und Technologietransfer erst am »CISPA – Center for IT-Security, Privacy and Accountability« und dann am »CISPA – Helmholtz-Zentrum für Informationssicherheit«, im Anschluss war er von 2019 bis 2020 Leiter Wissenschaftsstrategie am »CISPA – Helmholtz-Zentrum für Informationssicherheit«. Seit 2021 ist Sebastian Gerling der Chief Digital Officer (CDO) der Universität Hamburg. Darüber hinaus ist er seit 2011 freiberuflicher Berater für IT-Sicherheit und Digitalisierung sowie freiberuflicher Referent für IT-Sicherheitsschulungen und Vorträge. Darüber hinaus ist er Autor von zahlreichen Fachartikeln im Bereich der IT-Sicherheit.

Inhaltsverzeichnis

Cover

Titelblatt

Impressum

Über die Autoren

Einleitung

Über dieses Buch

Törichte Annahmen über den Leser

Was Sie nicht lesen müssen

Wie dieses Buch aufgebaut ist

Symbole, die in diesem Buch verwendet werden

Konventionen in diesem Buch

Wie es weitergeht

Teil I: Informationssicherheit, IT-Sicherheit und Datenschutz

Kapitel 1: Irrtümer und häufige Fehler

Internet-Sicherheit

Mobile und Cloud-Sicherheit

Endgerätesicherheit

E-Mail-Sicherheit

Kapitel 2: Grundlagen der Informationssicherheit

Was ist Informationssicherheit?

Was ist IT-Sicherheit?

Was ist Cybersicherheit?

Klassische Schutzziele der Informationssicherheit

Authentizität

Verantwortlichkeit

Benutzbarkeit

Weitere Schutzziele

Kapitel 3: Bausteine der Informationssicherheit

Risikomanagement

Meldepflichten bei Vorfällen

Einhaltung von Sicherheitsstandards

Nachweis der Einhaltung durch Audits

Kapitel 4: Datenschutz und technisch-organisatorische Maßnahmen

Teil II: Rechtliche Anforderungen

Kapitel 5: Die DS-GVO und das BDSG

Die acht Gebote des Datenschutzes (BDSG a. F.)

Stand der Technik

Implementierungskosten

Gewährleistungsziele des Datenschutzes

Kapitel 6: Gesetze zur IT-Sicherheit

NIS-Richtlinie (EU)

Rechtsakt zur Cybersicherheit (EU)

eIDAS-Verordnung (EU)

Single-Digital-Gateway-(SDG-)Verordnung (EU)

BSI-Gesetz (D)

BSI-Kritisverordnung (D)

Geschäftsgeheimnisgesetz (D)

Onlinezugangsgesetz (D)

Sozialgesetzbuch V (D)

TKG, TMG und TTDSG (D)

Kapitel 7: ISO-Normen

ISO/IEC 270xx Informationssicherheit

ISO/IEC 27701 Datenschutz

Kapitel 8: BSI und Grundschutz

IT-Grundschutz

Standard-Datenschutzmodell und IT-Grundschutz

Technische Richtlinien des BSI

Kapitel 9: Weitere Standards

Prozessorientierte Standards

Vorgaben für die öffentliche Verwaltung

Technikorientierte Standards

ITIL

Kapitel 10: Technisch-organisatorische Maßnahmen (TOM)

Vertraulichkeit

Integrität

Verfügbarkeit und Belastbarkeit

Auftragskontrolle, Lieferantenbeziehungen

Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM

Teil III: Organisation der Informationssicherheit

Kapitel 11: Organisation im Unternehmen

Verantwortung für die Informationssicherheit

Organisatorische Strukturen

Richtlinien und Regeln

Kapitel 12: Der Deming-Kreis (PDCA) und die ständige Verbesserung

Kapitel 13: Risikoanalyse und Kronjuwelen

Klassifizierung der Daten

Klassifizierung der Systeme

Bedrohungsanalyse

Metriken und Bewertung

Kapitel 14: Grundlegende Dokumentation

Asset- und Konfigurationsmanagement

Nutzermanagement und Zugriffskontrolle

Kapitel 15: Meldepflichten und Vorfallsmanagement

[Datenschutzvorfälle](#)

[IT-Sicherheitsvorfälle](#)

[Angriffserkennung](#)

[Security Information and Event Management \(SIEM\)](#)

Kapitel 16: Awareness und Beschäftigte

Teil IV: Bausteine der technischen IT-Sicherheit

Kapitel 17: Grundlagen der Verschlüsselung

[Symmetrische Verschlüsselung](#)

[Betriebsarten der Blockverschlüsselung](#)

[Asymmetrische Verschlüsselung](#)

[Hybride Verschlüsselung](#)

[Hashfunktionen](#)

[Digitale und elektronische Signaturen](#)

[Elliptische-Kurven-Kryptografie](#)

[DLIES und ECIES](#)

[Vertrauensmodelle](#)

[Kryptographische Forschung](#)

Kapitel 18: Biometrie

[Hautleisten](#)

[Venenmuster](#)

[Iris-Scan](#)

[Gesichtserkennung](#)

Kapitel 19: Chipkarten und Secure Hardware Token

[Einmalpasswort-Token](#)

Teil V: Lösungen und Umsetzungen

Kapitel 20: Backup & Co.

[Datensicherung](#)

[Aufbewahrungspflichten](#)

[Archivierung](#)

[Redundanz](#)

Kapitel 21: Netzwerksicherheit

[Grundlagen](#)

[Sicherheitserweiterungen von Netzwerkprotokollen](#)

[Netzwerkzugang](#)

[Netzwerksegmentierung](#)

[Denial-of-Service-Angriffe](#)

[Anonymisierung in Netzwerken](#)

[Funknetze](#)

[Das sichere Internet der Zukunft](#)

Kapitel 22: Firewalls

[Grundlagen von Firewalls](#)

[Packet Filter](#)

[Stateful Inspection Firewall](#)

[Network Address Translation \(NAT\)](#)

[Proxy-Server und Application Layer Firewall](#)

[NG Firewall und Deep Packet Inspection](#)

[Firewall in der Cloud](#)

Kapitel 23: Verschlüsselung im Einsatz

[Daten in Ruhe](#)

[Daten in Bewegung](#)

Kapitel 24: Monitoring

[Metriken der IT-Sicherheit](#)

[Angriffserkennungssysteme](#)

[Managed Security](#)

[Schadsoftware](#)

Kapitel 25: Patch Management

Kapitel 26: Zugangssicherung und Authentisierung

[Passwörter im Unternehmen](#)

[Zwei-Faktor-Authentisierung](#)

[Biometrie](#)

[Single Sign-on](#)

Kapitel 27: Anwendungssicherheit

[Chat](#)

[E-Mail](#)

[Videokonferenzen](#)

[Webanwendungen](#)

[Datenbanken](#)

[Cloud](#)

[Blockchain](#)

[Künstliche Intelligenz](#)

Teil VI: Der Top-Ten-Teil

Kapitel 28: Zehn Maßnahmen für den technischen Basisschutz

[Backup](#)

[Schutz vor Schadsoftware](#)

[Netzwerkschutz](#)

[Firewall](#)

[Patch-Management](#)

[Verschlüsselt speichern](#)

[Verschlüsselt kommunizieren](#)

[Passwort-Management](#)

[Biometrie und Zwei-Faktor-Authentifikation](#)

[Spam-Abwehr](#)

Kapitel 29: Zehn Maßnahmen für den organisatorischen Überbau

[Übernahme der Verantwortung](#)

[Leitlinie zur Informationssicherheit](#)

[Richtlinien zur Informationssicherheit](#)

[Definition und Besetzung der Rollen](#)

[Definition der fundamentalen Prozesse](#)

[Risikobetrachtung](#)

[Klassifizierung der Daten und Systeme](#)

[Awareness](#)

[Krisenmanagement](#)

[Regelmäßige Überprüfung](#)

[Literaturverzeichnis](#)

[Abbildungsverzeichnis](#)

[Stichwortverzeichnis](#)

[End User License Agreement](#)

Tabellenverzeichnis

Kapitel 3

[Tabelle 3.1: Die expliziten gesetzlichen Vorgaben für Unternehmen bezüglich der M...](#)

Kapitel 6

[Tabelle 6.1: Die Regelungen der §§ 165–169 TKG haben vier unterschiedliche Gruppe...](#)

Kapitel 7

[Tabelle 7.1: Änderungen und Ergänzungen der Abschnitte der ISO/IEC 27001/27002 du...](#)

Kapitel 8

[Tabelle 8.1: Die 47 elementaren Gefährdungen der IT-Sicherheit \(IT-Grundschutzkom...](#)

[Tabelle 8.2: Kreuztabelle für den Baustein »SYS.2.3: Clients unter Linux und Unix...](#)

[Tabelle 8.3: Zusammenfassung der wesentlichen empfohlenen Verfahren und Mindestsc...](#)

Kapitel 14

[Tabelle 14.1: Die Unterschiede zwischen einem Inventarverzeichnis und einer CMDB...](#)

Kapitel 16

[Tabelle 16.1: Die drei Phasen einer Awareness-Kampagne. \(nach SP 800-16\).](#)

Kapitel 17

[Tabelle 17.1: Die sechs Prinzipien \(Anforderungen\) des Auguste Kerckhoffs von Nie...](#)

[Tabelle 17.2: Bekannte Hashfunktionen mit Blocklänge, der Länge des Hashwerts und...](#)

[Tabelle 17.3: Vergleich der Schlüssellängen für verschiedene Verschlüsselungsverf...](#)

[Tabelle 17.4: Die wesentlichen Datenfelder der Datenstruktur zur Speicherung des ...](#)

Kapitel 21

[Tabelle 21.1: Übersicht über das OSI-Referenzmodell im Vergleich zum TCP/IP-Model...](#)

Illustrationsverzeichnis

Kapitel 2

[Abbildung 2.1: Anzahl der aktuellen \(2012, 2016 und 2019\) und veralteten \(2003, 2...](#)

Kapitel 3

[Abbildung 3.1: Das Risiko wird häufig als das Produkt aus Schadenshöhe und Eintri...](#)

[Abbildung 3.2: Durch die Risikostrategien Vermeiden, Reduzieren und Delegieren ka...](#)

Kapitel 5

[Abbildung 5.1: Die beispielhafte Auswertung der Fragebögen zur Bewertung des Stan...](#)

Kapitel 6

[Abbildung 6.1: Die gesetzlichen Vorgaben zur IT-Sicherheit in den unterschiedlich...](#)

[Abbildung 6.2: Das fünfstufige Reifegradmodell zur OZG-Umsetzung der Verwaltungsv...](#)

[Abbildung 6.3: Die Priorisierung P1 bis P4 sowie die Zahl der Maßnahmen für klein...](#)

[Abbildung 6.4: Je nach Größe einer ärztlichen beziehungsweise zahnärztlichen Prax...](#)

Kapitel 7

[Abbildung 7.1: Übersicht über die ISO-Normen der ISO/IEC 27000er Standard-Familie...](#)

Kapitel 9

[Abbildung 9.1: Grobe qualitative Darstellung des Aufwands und des typisch zu erre...](#)

[Abbildung 9.2: Tabellarische Übersicht über das Ergebnis einer Selbsteinschätzung...](#)

Kapitel 10

[Abbildung 10.1: Beispiele für Identifikatoren, Teil-Identifikatore...](#)

[Abbildung 10.2: Office-Dokumente können in den Desktopversionen von Microsoft Off...](#)

[Abbildung 10.3: Die Konfiguration der Verschlüsselung eines Webser...](#)

[Abbildung 10.4: Der Greenbone-Schwachstellenscanner bewertet die g...](#)

Kapitel 11

[Abbildung 11.1: Die Regelungspyramide, die die zeitlichen Änderungsskalen und die...](#)

Kapitel 12

[Abbildung 12.1: Der Deming- oder PDCA-Zyklus als vierstufiger Prozess der ständig...](#)

Kapitel 13

[Abbildung 13.1: Auszug aus der Log-Datei auth.log eines Servers. Hier sind die un...](#)

Kapitel 15

[Abbildung 15.1: Der Anfang eines TLP:WHITE-Dokuments des BSI mit einer Warnung vo...](#)

Kapitel 17

[Abbildung 17.1: Kommunikationsmodell eines symmetrischen Verschlüsselungssystem.](#)

[Abbildung 17.2: Symmetrische Verschlüsselung](#)

[Abbildung 17.3: Die Verschlüsselung zweier Blöcke im ECB- \(links\) und CBC-Modus \(...\)](#)

[Abbildung 17.4: Das Logo der Buchreihe \(oberes Bild\) wurde mit AES...](#)

[Abbildung 17.5: Das Verschlüsselungsschema ist beim CFB-, OFB- und CTR-Modus glei...](#)

[Abbildung 17.6: Bei einem Man-in-the-Middle-\(MITM-\)Angriff klinkt sich Mallory ak...](#)

[Abbildung 17.7: Die Verschlüsselung erfolgt mit dem öffentlichen Schlüssel des Em...](#)

[Abbildung 17.8: Zur Erzeugung von Schlüsselpaaren werden im Wesentliche...](#)

[Abbildung 17.9: Ein Briefkasten ist eine Analogie zur asymmetrischen Verschlüssel...](#)

[Abbildung 17.10: Bei der Hybridverschlüsselung wird der Schlüssel mittels asymmet...](#)

[Abbildung 17.11: Bei der Merkle-Damgård-Konstruktion besteht die Hashfunktion aus...](#)

[Abbildung 17.12: Wir können uns die Bildung eines Hashwerts wie die Faltung einer...](#)

[Abbildung 17.13: Beispiele für die verschiedenen Padding-Verfahren. Der...](#)

[Abbildung 17.14: Ein Schaukasten im Unternehmen hat eine Funktion, die der digita...](#)

[Abbildung 17.15: Schematische Darstellung einer digitalen Signatur und ihrer Über...](#)

[Abbildung 17.16: Darstellung der Addition zweier Punkt auf einer elliptischen Kur...](#)

[Abbildung 17.17: Beim ersten Verbindungsaufbau zu einem SSH-Server muss der Schlü...](#)

[Abbildung 17.18: Anforderungen an die Größe von Quantencomputern. Der graue Berei...](#)

Kapitel 18

[Abbildung 18.1: Die Abhängigkeit der False Acceptance Rate \(FAR\) und der False Re...](#)

Kapitel 19

[Abbildung 19.1: Die Chipkartenformate mit Kontaktfeld \(von links\): ID-1, ID-000, ...](#)

[Abbildung 19.2: Schematischer Aufbau einer Speicherchipkarte \(a\) und einer Prozes...](#)

[Abbildung 19.3: Aus einer Token-abhängigen individuellen Zufallszahl, die bei der...](#)

[Abbildung 19.4: Aus der Domain des Login-Servers, einer Zufallszahl \(Nonce\) und d...](#)

Kapitel 20

[Abbildung 20.1: Die Darstellung der Datensicherungsarten. a\) Vollsicherung; b\) Di...](#)

[Abbildung 20.2: Schematische Darstellung eines RAID-1- und eines RAID-5-System mi...](#)

Kapitel 21

[Abbildung 21.1: Der Ablauf der DNS-Auflösung mit normalen DNS \(a\) und DoT/DoH \(b\)...](#)

[Abbildung 21.2: Darstellung des Zusammenspiels von Supplicant, Authenticator und ...](#)

[Abbildung 21.3: Segmentierung eines Netzwerks.](#)

[Abbildung 21.4: VLAN-Beispiele.](#)

Kapitel 22

[Abbildung 22.1: Beispiel für eine Firewall mit vier Sicherheitszonen: Extern, Int...](#)

[Abbildung 22.2: Beispielhafte Übersetzung der IP-Adressen mit NAT ...](#)

Kapitel 23

[Abbildung 23.1: Es gibt vier Konzepte, wie Dateien auf einem Datenträger verschlü...](#)

[Abbildung 23.2: Dialog zum Einrichten der Datenträgerverschlüsselung Bitlocker un...](#)

[Abbildung 23.3: Schmatische Darstellung der Hardware-Verschlüsselung oder Device ...](#)

[Abbildung 23.4: Die unterschiedlichen verschlüsselten Datenströme bei einer Ende-...](#)

[Abbildung 23.5: Die Verbindung von einem Client zu einem Server \(Ziel\) über eine ...](#)

[Abbildung 23.6: Der gleichzeitige Aufruf einer Webseite zum Anzeigen der eigenen ...](#)

[Abbildung 23.7: OpenVPN läuft im User Space und transportiert Daten zwischen eine...](#)

Kapitel 24

[Abbildung 24.1: Ein Spinnennetzdiagramm erlaubt den quantitativen Vergleich mehrer...](#)

[Abbildung 24.2: Die fehlgeschlagenen SSH-Anmeldeversuche mit der Nutzerin pi auf ...](#)

Kapitel 25

[Abbildung 25.1: Die monatliche Zahl der Schwachstellenwarnungen und Updates der W...](#)

Kapitel 27

[Abbildung 27.1: Ein Verschlüsselungs-Proxy übernimmt die Ver- und Entschlüsselung...](#)

[Abbildung 27.2: Die Kommunikationsflüsse bei einer Videokonferenz ...](#)

[Abbildung 27.3: Die Kommunikationsflüsse bei einer Videokonferenz ...](#)

[Abbildung 27.4: Die Kommunikationsflüsse bei einer Videokonferenz ...](#)

[Abbildung 27.5: Die verkettete Listenstruktur einer Blockchain.](#)

[Abbildung 27.6: Die Verwendung von Algorithmen und Daten beim Maschinellen Lernen...](#)

Einleitung

Informationssicherheit stellt eine der elementaren Grundlagen für eine gesetzeskonforme und verlässliche Nutzung von Informationstechnologien und der digitalen Transformation dar.

Wer sich heute für Informationssicherheit interessiert, muss sich sowohl mit den organisatorischen als auch mit den technischen Grundlagen der Informationssicherheit befassen. Moderne Vorlesungen zur Informationssicherheit decken nicht nur den technischen Teil ab, sondern widmen sich genauso umfangreich den organisatorischen Strukturen. Leider fehlt es in der Informatikerausbildung aber häufig noch an der fachbereichsübergreifenden Darstellung und die IT-Sicherheit wird rein technisch gelehrt.

Das ist sicherlich ein Grund dafür, dass die Informationssicherheit noch lange nicht flächendeckend auf dem Niveau ist, auf dem sie sein sollte. Auch die regulatorischen Vorgaben durch den Gesetzgeber werden mehr. Die DS-GVO und die IT-Sicherheitsgesetzgebung fordern heute deutlich mehr IT-Sicherheit und technisch-organisatorische Maßnahmen als noch vor ein paar Jahren. Auch der IT-Planungsrat kümmert sich um einheitliche Informationssicherheitsvorgaben für Behörden. Tangiert wird das außerdem auch von den Rechnungshöfen des Bundes und der Länder, die im Rahmen ihrer Wirtschaftlichkeitsprüfungen auch die Informationssicherheit prüfen.

Das weltumspannende Internet sollten wir sicher nutzen können, deshalb benötigen wir eine einheitliche Regulierung der Informationssicherheit. Die Gültigkeit

nationalen Rechts endet an der Landesgrenze. Internationale Regelungen, wie sie die EU schafft, vereinheitlichen die Vorgaben. Hier bedarf es noch weiterer internationaler Anstrengungen.

Über dieses Buch

Wir stellen im Buch die organisatorischen und die technischen Grundlagen der Informationssicherheit gemeinsam dar. Das Buch gibt eine umfassende Orientierung zur Einordnung der Informationssicherheit in das regulatorische Umfeld (Deutschland, EU), die erforderlichen organisatorischen Strukturen im Unternehmen beziehungsweise in der Behörde und die technischen Grundlagen der Informationssicherheit.

Törichte Annahmen über den Leser

Sie wollen Informationssicherheit lernen. Das ist gut und Sie sind hier richtig.

Sie haben kein Vorwissen. Kein Problem! Die Inhalte werden so präsentiert, dass sie im Wesentlichen ohne Vorwissen verständlich sind.

Sie studieren Informatik, Mathematik oder Jura. Sie denken darüber nach, eine Berufslaufbahn in der Informationssicherheit einzuschlagen. Dann sollten Sie neben den technischen Grundlagen der Informationssicherheit (eher Informatik-Themen) auch die rechtlichen und organisatorischen Grundlagen (eher juristische, Wirtschafts- und Wirtschaftsinformatik-Themen) beherrschen. Das Buch führt das erforderliche Wissen aus den Schnittstellen zu den relevanten

Fachgebieten (Informatik, Rechtswissenschaften, Wirtschaftswissenschaften und Wirtschaftsinformatik) zusammen und stellt es einheitlich dar.

Was Sie nicht lesen müssen

Wenn Sie beginnen, ein Kapitel zu lesen, und Sie den Inhalt schon kennen, überspringen Sie das Kapitel. Bei einem Querschnittsthema mit juristischen, technischen und betrieblichen Inhalten ist es unvermeidbar, dass Sie, je nach Ausbildung, in dem einen oder anderen dieser Themen schon Vorkenntnisse haben. Die Juristen unter Ihnen kennen sich mit den Gesetzen aus und die Mathematiker oder Informatiker unter Ihnen wissen vermutlich schon einiges über Verschlüsselung.

Beispiele und Anekdoten können Sie überspringen, wenn Sie den Sachverhalt auch so verstehen oder der Hintergrund für Sie nicht so wichtig ist.

Wie dieses Buch aufgebaut ist

Wie jedes Buch der »... für Dummies«-Reihe ist auch dieses Buch in mehrere große Teile gegliedert. Die Einführung der grundlegenden Begriffe und Anforderungen geschieht in [Teil I](#). In [Teil II](#) lernen Sie die rechtlichen und regulatorischen Anforderungen kennen. Die Organisation im Unternehmen ist der Schwerpunkt von [Teil III](#). [Teil IV](#) soll Ihnen die technischen Grundlagen und Bausteine vermitteln. Aus den Bausteinen bauen wir dann im [Teil V](#) das IT-Sicherheitshaus auf.

Teil I: Informationssicherheit, IT-Sicherheit und Datenschutz

IT-Sicherheit und Informationssicherheit ist das nicht dasselbe? Und was hat Datenschutz damit zu tun? Sie lernen die Definitionen und Unterschiede der Begriffe der Informationssicherheit, nämlich die klassischen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit kennen. Wenn Sie sich mit der Umsetzung von Informationssicherheit beschäftigen wollen, müssen Sie zuerst lernen, was Informationssicherheit ist.

Erstaunlicherweise finden Sie diese Grundbegriffe nicht nur in Lehrbüchern und Standarddokumenten zur Informationssicherheit, sondern zunehmend auch in Gesetzen. Die immer weiter gehende Digitalisierung führt auch zu vermehrten Anforderungen an die Informationssicherheit. Von der Praxis Ihres Hausarztes bis zur Steuerung der Energieversorgung Ihrer Wohnung: überall werden Computer eingesetzt. Und wenn die Computer gestört sind, fällt die Dienstleistung oder Versorgungsleistung aus. Im Juli 2021 wurde in Deutschland erstmalig der Cyberkatastrophenfall ausgelöst, und zwar im Landkreis Anhalt-Bitterfeld. Störungen der Informationssicherheit können tatsächlich katastrophale Auswirkungen haben. Deshalb muss Informationssicherheit nicht nur Schutz vor Angriffen, sondern auch Vorsorge vor Katastrophen und Unfällen sein.

Die vier Begriffe Risikomanagement, Meldepflichten, Sicherheitsstandards und Audits ziehen sich wie ein roter Faden durch alle Regelungen zur IT-Sicherheit. Sie werden lernen, was es damit auf sich hat.

Und mit den technisch-organisatorischen Maßnahmen, kurz TOM, kommt dann auch der Datenschutz ins Spiel. Um den technischen Schutz der personenbezogenen

Daten zu gewährleisten, sind TOMs erforderlich. Datenschutz braucht unterstützend die IT-Sicherheit, auch wenn die Datenschutzziele nicht allein durch IT-Sicherheitsmaßnahmen erreicht werden können.

Teil II: Rechtliche Anforderungen

Da Computer und Digitalisierung immer weiter in unser Leben vordringen und deshalb die Informationssicherheit immer wichtiger wird, regelt der Gesetzgeber in immer mehr Gesetzen und Verordnungen die Anforderungen an die Informationssicherheit.

Viele Unternehmen müssen sich intensiv um Informationssicherheit kümmern. Dabei spielt es keine Rolle, ob ihnen das wichtig ist oder nicht: Es ist ihnen gesetzlich vorgeschrieben.

Sie erfahren, welche europäischen Vorschriften (Netzwerk- und Informationssicherheits-Richtlinie, Rechtsakt zur Cybersicherheit, Datenschutz-Grundverordnung) und welche deutschen Vorschriften (BSI-Gesetz, Geschäftsgeheimnisgesetz, Telekommunikationsgesetz und etliche andere) den Unternehmen Vorgaben zur IT-Sicherheit machen.

Neben den rechtlichen Vorgaben lernen Sie auch die Standards und Normen zur Informationssicherheit (ISO-Normen, BSI-Grundschutz und andere) kennen. Diese Standards sind wichtig, da sich die rechtlichen Vorgaben teilweise für die Umsetzung auf diese Standards beziehen. Gesetze haben eine deutlich längere Lebensdauer als IT-Systeme. Deshalb ist es für den Gesetzgeber schwer, IT in Gesetzen detailliert zu regeln. Der Bezug auf Standards, die sich schneller aktualisieren lassen, ist der Ausweg aus diesem Dilemma.

Und nochmal Datenschutz: Wie strukturieren Sie im Unternehmen die TOMs? Wir schauen uns gemeinsam

an, was bei den TOMs wichtig ist.

Teil III: Organisation der Informationssicherheit

Ein Unternehmen muss seine Prozesse durch interne Vorgaben und Regeln gestalten. Teilweise sind das relativ banale Dinge, wie eine Nutzerordnung oder eine Passwortrichtlinie. Welche Regeln und vor allem welche Inhalte der Regeln wollen Sie als zukünftige Expertin oder zukünftiger Experte für Informationssicherheit Ihrem Unternehmen empfehlen? Sie lernen in diesem Teil, was Sie regeln sollen und wie Sie es regeln sollen.

Wer hat im Unternehmen welche Aufgaben in der Informationssicherheit? Vom Chef über den Informationssicherheitsbeauftragten und den IT-Leiter bis zur Nutzerin, jede und jeder trägt seinen Teil zur Bewältigung der Aufgabe »Informationssicherheit« bei.

Wie machen Sie eine Risikoanalyse? Was sind die Kronjuwelen im Unternehmen? Was dürfen die Nutzerinnen? Wie gehen Sie mit Sicherheitsvorfällen um? Mit all diesen Fragen beschäftigen wir uns in diesem dritten Teil.

Eine der wichtigsten organisatorischen Fragen beschäftigt sich mit der alten Frage: »Wie sag ich es meinen Mitarbeitern?« Awareness und Schulung sind wichtige Maßnahmen, die Sie kennenlernen werden.

Teil IV: Bausteine der technischen IT-Sicherheit

Im vierten Teil, zugegeben ein ziemlich anspruchsvoller Abschnitt, spielen die technischen Grundlagen der IT-Sicherheit die Hauptrolle. Einen breiten Raum nehmen die Grundlagen der Verschlüsselung ein. Ganz ohne

Mathematik geht es nicht, aber die Anschaulichkeit steht im Vordergrund.

Ein weiteres wichtiges Thema ist die Biometrie. Eine Anmeldung am Smartphone mit Fingerabdruck oder Gesichtserkennung haben Sie bestimmt schon gemacht. Türöffnung im Sicherheitsbereich mit Iris-Scan ist in manchen Rechenzentren Pflicht. Sie lernen die Grundlagen der Biometrie kennen und wir schauen uns auch die damit verbundenen Risiken an.

Außerdem beschäftigen wir uns noch mit Chipkarten und Sicherheitstoken. Vom neuen Personalausweis über die Girocard bis zur SIM-Karte im Smartphone haben Sie sicher schon persönliche Erfahrungen gemacht im Umgang mit den kleinen Geräten. Wir schauen uns an, wie sie funktionieren und was sie können.

Teil V: Lösungen und Umsetzungen

Aufbauend auf den Bausteinen, die Sie im vierten Teil kennengelernt haben, schauen wir uns dann die Lösungen zur IT-Sicherheit an. Backup, Verschlüsselung von Daten auf Datenträgern und bei der Übertragung, Netzwerksicherheit, Firewalls und Zugangssicherung sind Lösungen, die Sie kennenlernen werden.

Wie überwachen und messen Sie die IT-Sicherheit im Unternehmen? Was sind geeignete Metriken, um die Qualität Ihrer IT-Sicherheit zu messen? Was ist ein Patch-Management? Sie wollten sicher immer schon mal wissen, wie eine Blockchain funktioniert und was es mit Künstlicher Intelligenz auf sich hat. Auch das werden Sie in diesem Teil lernen.

Alle diese Lösungen dienen zur technischen Unterstützung der organisatorischen Prozesse im Unternehmen.

Teil VI: Der Top-Ten-Teil

Im Top-Ten-Teil geht es nochmal um die wichtigsten Begriffe und die wichtigsten organisatorischen und technischen Maßnahmen. Quasi das Take-away in aller Kürze.

Symbole, die in diesem Buch verwendet werden



Neben dem Fernglas finden Sie Beispiele, die Ihnen helfen, das Gelernte an einer konkreten Situation besser zu verstehen.



Neben der Lupe finden Sie Definitionen von Begriffen. Häufig stammen diese aus offiziellen Normen, Standards oder Gesetzen.



Wenn Sie erst in das Thema einsteigen und noch nicht so viele Erfahrungen haben, hilft der eine oder andere Tipp.



Bevor Sie einen typischen Fehler machen oder einem gängigen Irrtum unterliegen, lesen Sie die mit diesem Symbol gekennzeichneten Warnungen.