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-Grundschutzkompendium
- ✔ 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 Virenscanners 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 Virenscanners 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.

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

Tabellenverzeichnis

Kapitel 3

Kapitel 6

Kapitel 7

Kapitel 8

Kapitel 14

Kapitel 16

Kapitel 17

Kapitel 21

Illustrationsverzeichnis

Kapitel 2

Kapitel 3

Kapitel 5

Kapitel 6

Kapitel 7

Kapitel 9

Kapitel 10

Kapitel 11

Kapitel 12

Kapitel 13

Kapitel 15

Kapitel 17

Kapitel 18

Kapitel 19

Kapitel 20

Kapitel 21

Kapitel 22

Kapitel 23

Kapitel 24

Kapitel 25

Kapitel 27

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 mit 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 Querschnittthema 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 deutliche 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 diese 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.