

LEHRBUCH

Martin Kappes

# Netzwerk- und Datensicherheit

Eine praktische Einführung

*3. Auflage*

 Springer Vieweg



# Netzwerk- und Datensicherheit

---

Martin Kappes

# Netzwerk- und Datensicherheit

Eine praktische Einführung

3., aktualisierte und erweiterte Auflage

Martin Kappes  
FB 2 Informatik und Ingenieurwissenschaften  
Frankfurt University of Applied Sciences  
Frankfurt am Main, Deutschland

ISBN 978-3-658-16126-2      ISBN 978-3-658-16127-9 (eBook)  
<https://doi.org/10.1007/978-3-658-16127-9>

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

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2007, 2013, 2022

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von allgemein beschreibenden Bezeichnungen, Marken, Unternehmensnamen etc. in diesem Werk bedeutet nicht, dass diese frei durch jedermann benutzt werden dürfen. Die Berechtigung zur Benutzung unterliegt, auch ohne gesonderten Hinweis hierzu, den Regeln des Markenrechts. Die Rechte des jeweiligen Zeicheninhabers sind zu beachten.

Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag, noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Planung/Lektorat: Leonardo Milla

Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.

Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

---

## Vorwort zur dritten Auflage

IT-Sicherheit ist ein sehr komplexes und umfangreiches Thema, das letztlich jeden Teilbereich der Informatik mehr oder weniger direkt betrifft. Entsprechend groß ist die Materialfülle, aus der die Inhalte für dieses Buch ausgewählt werden mussten. Seit der Erstauflage sind noch viele neue Technologien und Protokolle hinzugekommen.

Ziel dieses Buchs ist es, den Leserinnen und Lesern einen verständlichen, konsistenten und auf das Wesentliche beschränkten Text zum Thema IT-Sicherheit an die Hand zu geben. Das Buch legt ein solides Fundament, auf dem sich später Detailwissen aus anderen Quellen leichter aneignen und vor allem auch sinnvoll einordnen lässt. Der Fokus liegt also auf einem grundlegenden Verständnis für die prinzipiellen Probleme und deren Relevanz, genauso wie auf der Skizzierung möglicher Lösungen. Die wichtigsten Methoden und Prinzipien der Netzwerk- und Datensicherheit werden exemplarisch anhand von praktischen Beispielen illustriert. Die präsentierte Auswahl von Inhalten hat sich bei den vorangegangenen Auflagen hervorragend bewährt und wird daher auch in dieser dritten, vollständig überarbeiteten und erweiterten Auflage beibehalten. Neu hinzugekommen sind die Themen IPv6, Webanwendungen und Cloud Computing.

Die Leserinnen und Leser dieses Buches werden nicht mit möglichst umfassendem Detailwissen konfrontiert. Die Darstellung konzentriert sich auf die wichtigsten Details und ordnet sie in ihren Kontext ein. Oft werden Sachverhalte vereinfacht dargestellt, denn jedes einzelne Kapitel deckt ein Thema ab, das für sich alleine genommen schon genügend Stoff für ein ganzes Buch bieten würde. Aus Gründen der besseren Lesbarkeit verwenden wir in diesem Buch überwiegend das generische Maskulinum, beispielsweise bei Begriffen wie „Hacker“ und „Angreifer“. Dies impliziert alle Geschlechter und schließt selbstverständlich auch die weibliche Form mit ein.

Im Internet gibt es zahllose, auch sehr gute und umfassende Quellen, die minutiös alle Details zu bestimmten Technologien und Protokollen auflisten, nicht zuletzt viele der maßgeblichen Standards selbst. Mit dem Wissen aus diesem Buch können die

Leserinnen und Leser diese Quellen zielgerichtet verwenden, um sich tiefgehend über viele weitere spannende Details zu informieren.

Soviel Mühe sich ein Autor auch gibt, Lehrbücher werden oft nicht von der ersten bis zur letzten Seite gelesen. Ich habe versucht, dem Rechnung zu tragen, indem die einzelnen Kapitel, soweit als möglich, auch eigenständig gelesen werden können:

Das erste Kapitel bietet eine Einführung in die Thematik. Es werden grundlegende Begriffe eingeführt sowie Ziele von IT-Sicherheit und mögliche Angriffe auf sie dargestellt. Neben einigen organisatorischen Grundlagen werden auch die rechtlichen Rahmenbedingungen in Deutschland skizziert. In Kap. 2 werden fundamentale kryptographische Prinzipien und Methoden vorgestellt. Kap. 3 diskutiert die wichtigsten Authentifikationsmechanismen. Diese Kapitel sind grundlegend für nahezu alle weiteren Kapitel des Buchs und sollten deshalb von Ihnen speziell dann gelesen werden, wenn Sie hinsichtlich IT-Sicherheit, Kryptographie und Authentifikation keine Vorkenntnisse besitzen.

Hieran schließen sich drei Kapitel an, die eine logische Einheit bilden und sich mit Systemsicherheit beschäftigen. Kap. 4 befasst sich mit Sicherheit auf der Betriebssystemebene. Kap. 5 betrachtet die Sicherheit von Anwendungen. Hieran schließt sich in Kap. 6 eine Darstellung von Malware, also Viren, Würmern und anderem Ungeziefer, an.

Danach wenden wir uns der Netzwerksicherheit zu. In Kap. 7 wird eine knappe Darstellung der wichtigsten Grundlagen und Protokolle präsentiert, die sich speziell an Leser ohne Vorkenntnisse im Bereich Netzwerke richtet, oder an Leserinnen und Leser, die ihre Kenntnisse auffrischen möchten. Hieran schließt sich in Kap. 8 eine erste Betrachtung von Sicherheitsaspekten in Netzwerken an, in der wir speziell auf Schwachstellen in den im Internet verwendeten Protokollen eingehen. Die darauffolgenden Kap. 9 bis 17 beschäftigen sich mit Firewalls, Virtual Private Networks, Netzwerküberwachung, Verfügbarkeit, Netzwerkanwendungen, Webanwendungen, Cloud Computing, Realzeitkommunikation und Sicherheit auf der Datenverbindungsschicht und in lokalen Netzen. Diese Kapitel können auch einzeln oder in anderer Reihenfolge gelesen werden. Am Ende betrachten wir in Kap. 18 praktische Richtlinien für die IT-Sicherheit in Institutionen.

Unter <https://www.fg-itsec.de/> finden sich Zusatzmaterialien zum Buch wie etwa Demonstrationsvideos. Nicht zuletzt finden sich dort auch Informationen über die Aktivitäten meiner Forschungsgruppe für Netzwerksicherheit, Informationssicherheit und Datenschutz an der Frankfurt University of Applied Sciences. Dort entwickeln Wissenschaftler Sicherheitstechnologien der nächsten und übernächsten Generation und werden dabei durch zahlreiche Studierende der Hochschule unterstützt. Gemeinsam mit Kooperationspartnern aus Industrie, öffentlichen Einrichtungen und Verbänden führen wir Projekte in den Bereichen Netzwerk- und Systemsicherheit, Sicherheitsorganisation, -bewertung und -management, Zuverlässigkeit und Verfügbarkeit komplexer Systeme, Netzwerkmanagement und technischen Datenschutz durch.

Ganz am Ende möchte ich mich an Sie, liebe Leserinnen und Leser, wenden und Sie ermutigen, mir ebenfalls Ihr Feedback zu diesem Buch zukommen zu lassen. Ich bin gespannt darauf, wie Ihnen die Neuauflage des Buch gefällt, und welche Anmerkungen Sie haben.

Frankfurt am Main  
im Juni 2022

Martin Kappes

---

# Inhaltsverzeichnis

<b>1</b>	<b>Einführung</b> .....	1
1.1	Warum IT-Sicherheit .....	1
1.2	Ziele von IT-Sicherheit .....	3
1.3	Angriffe auf IT-Sicherheit .....	6
1.3.1	Angriffsarten .....	6
1.3.2	Schwachstellen .....	7
1.3.3	Ziele eines Angriffs .....	8
1.4	Risiken und Unsicherheit .....	9
1.5	IT-Sicherheit in der Praxis .....	11
1.6	Organisatorische Grundlagen der IT-Sicherheit .....	12
1.6.1	Rahmenbedingungen .....	12
1.6.2	IT-Sicherheit als Prozess .....	12
1.7	Rechtliche Grundlagen und Rahmenbedingungen in Deutschland .....	13
1.7.1	Strafgesetzbuch .....	14
1.7.2	Datenschutzgrundverordnung .....	14
1.7.3	Telekommunikation-Telemedien-Datenschutz-Gesetz .....	15
1.7.4	Handelsgesetzbuch .....	16
1.7.5	Bundesamt für Sicherheit in der Informationstechnik .....	16
1.7.6	Vorratsdatenspeicherung .....	19
1.8	Zusammenfassung .....	20
1.9	Übungsaufgaben .....	21
1.9.1	Wiederholungsaufgaben .....	21
1.9.2	Weiterführende Aufgaben .....	22
	Literatur .....	22
<b>2</b>	<b>Kryptographische Prinzipien und Methoden</b> .....	25
2.1	Grundlagen .....	25
2.1.1	Definition .....	25
2.1.2	Modell .....	26



2.2	Verschlüsselungsverfahren . . . . .	28
2.2.1	Vom Klartext zum Chiffretext . . . . .	28
2.2.2	Sicherheit von Verschlüsselungsverfahren . . . . .	30
2.2.2.1	Kryptanalyse . . . . .	30
2.2.2.2	Ein absolut sicheres Verfahren . . . . .	32
2.3	Symmetrische Verfahren und Public-Key-Verfahren . . . . .	34
2.3.1	Grundlagen . . . . .	34
2.3.2	Symmetrische Verfahren . . . . .	35
2.3.3	Public-Key-Verfahren . . . . .	36
2.3.4	Hybride Verfahren . . . . .	38
2.4	Betriebsarten . . . . .	40
2.4.1	Electronic Code Book . . . . .	40
2.4.2	Cipher Block Chaining . . . . .	41
2.4.3	Cipher Feedback Mode und Output Feedback Mode . . . . .	42
2.4.4	Counter Mode . . . . .	43
2.5	Zusammenfassung . . . . .	45
2.6	Übungsaufgaben . . . . .	47
2.6.1	Wiederholungsaufgaben . . . . .	47
2.6.2	Weiterführende Aufgaben . . . . .	48
	Literatur . . . . .	50
<b>3</b>	<b>Authentifikation . . . . .</b>	<b>51</b>
3.1	Grundlagen . . . . .	51
3.2	Mögliche Faktoren zur Authentifikation . . . . .	52
3.3	Passwörter . . . . .	53
3.3.1	Größe des Passwortraums . . . . .	54
3.3.2	Sicherheit der Passwortspeicherung beim Anwender und im System . . . . .	55
3.3.3	Sicherheit der Passworteingabe und Übertragung . . . . .	58
3.3.4	Passwörter – Eine Sicherheitslücke? . . . . .	59
3.4	Tokens und Smart-Cards . . . . .	60
3.5	Biometrie . . . . .	62
3.6	Kryptographische Methoden . . . . .	63
3.6.1	Authentifikation von Benutzern und Maschinen . . . . .	63
3.6.2	Digitale Signatur . . . . .	66
3.6.3	Infrastrukturen zur Authentifikation . . . . .	68
3.6.3.1	Zertifikate und Certificate Authorities . . . . .	68
3.6.3.2	Zertifikate in der Praxis: X.509 . . . . .	72
3.6.3.3	Beispiel: X.509 Zertifikate mit OpenSSL selbst erstellen . . . . .	74
3.6.3.4	Online Certificate Status Protocol und Extended Validation . . . . .	79
3.6.3.5	Web of Trust . . . . .	80

3.7	Zusammenfassung .....	81
3.8	Übungsaufgaben.....	81
3.8.1	Wiederholungsaufgaben.....	81
3.8.2	Weiterführende Aufgaben .....	83
	Literatur.....	84
<b>4</b>	<b>Betriebssysteme und ihre Sicherheitsaufgaben .....</b>	<b>85</b>
4.1	Aufgaben und Aufbau von Betriebssystemen .....	85
4.2	Systemadministratoren.....	87
4.3	Rechtevergabe und Zugriffskontrolle am Beispiel Dateisystem .....	88
4.4	Trusted Computing.....	95
4.5	Monitoring und Logging .....	95
4.6	Absichern des Systems gegen Angriffe .....	96
4.7	Zusammenfassung .....	97
4.8	Übungsaufgaben.....	98
4.8.1	Wiederholungsaufgaben.....	98
4.8.2	Weiterführende Aufgaben .....	98
	Literatur.....	99
<b>5</b>	<b>Anwendungen .....</b>	<b>101</b>
5.1	Einführung .....	101
5.2	Buffer Overflows .....	102
5.2.1	Das Problem.....	102
5.2.2	Beispiel.....	105
5.2.3	Schutzmaßnahmen .....	106
5.3	Race Conditions .....	107
5.4	Software aus dem Internet .....	109
5.4.1	Downloads .....	109
5.4.2	Aktive Inhalte.....	110
5.4.2.1	Einführung.....	110
5.4.2.2	Java .....	110
5.4.2.3	JavaScript .....	112
5.5	Zusammenfassung .....	113
5.6	Übungsaufgaben.....	114
5.6.1	Wiederholungsaufgaben.....	114
5.6.2	Weiterführende Aufgaben .....	114
	Literatur.....	114
<b>6</b>	<b>Malware .....</b>	<b>115</b>
6.1	Einführung .....	115
6.2	Schaden .....	116
6.3	Verbreitung und Funktionsweise .....	117
6.3.1	Verbreitung.....	117