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

Springer Vieweg

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.

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 Martin Kappes
im Juni 2022

Inhaltsverzeichnis