Xpert.press

Springer-Verlag Berlin Heidelberg GmbH

Die Reihe Xpert.press des Springer-Verlags vermittelt Professionals in den Bereichen Betriebs- und Informationssysteme, Software Engineering und Programmiersprachen aktuell und kompetent relevantes Fachwissen über Technologien und Produkte zur Entwicklung und Anwendung moderner Informationstechnologien.

Stephan Fischer
Christoph Rensing
Utz Rödig

Open Internet Security

Von den Grundlagen zu den Anwendungen

Mit 111 Abbildungen und 27 Tabellen

Springer

Dr. Stephan Fischer
Dipl. Wirtsch.-Inf. Christoph Rensing
Dipl.-Ing. Utz Rödig

Technische Universität Darmstadt
Industrielle Prozess- und Systemkommunikation KOM
Merckstraße 25, 64283 Darmstadt
{Stephan.Fischer, Christoph.Rensing, Utz.Roedig}@kom.tu-darmstadt.de
http://www.kom.e-technik.tu-darmstadt.de/

ISBN 978-3-540-66814-5

Die Deutsche Bibliothek - CIP-Einheitsaufnahme
Fischer, Stephan: Open Internet Security: von den Grundlagen zu den Anwendungen, Stephan Fischer; Christoph Rensing; Utz Rödig. - Berlin; Heidelberg; New York; Barcelona; Hongkong; London; Mailand; Paris; Singapur; Tokio: Springer, 2000
(Xpert.press)
ISBN 978-3-540-66814-5 ISBN 978-3-642-57003-2 (eBook)
DOI 10.1007/978-3-642-57003-2

Ursprünglich erschienen bei Springer-Verlag Berlin Heidelberg New York 2000

Umschlaggestaltung: Künkel + Lopka, Heidelberg
Satz: Belichtungsfertige Daten von den Autoren
Gedruckt auf säurefreiem Papier SPIN: 10753150 33/3142 GF 543210

Widmung

Für Ines.
Stephan Fischer

Für all diejenigen, die mir meinen Ausbildungs- und Lebensweg bis zur Erstellung dieses Buchs ermöglicht und mich auf diesem Weg begleitet haben.
Christoph Rensing

Für mich.
Utz Rödig

Vorwort

In den letzten Jahren ist die weltweite Vernetzung von Rechnern, getrieben durch das Internet und die schnelle Verbreitung des World Wide Web (WWW), stark angestiegen. Es existieren heute kaum noch Unternehmen, die nicht auf die Nutzung des Datenaustauschs über Netzwerke zurückgreifen. Die Welt stellt sich im Internet als eine Menge von miteinander verbundenen lokalen Netzen dar, auf die Endanwender auch per ISDN oder Modem extern zugreifen können.

Ziel dieses Buchs ist es, dem Leser zu erläutern, wie die Gefahren, die durch eine Kommunikation über das Internet entstehen können, beurteilt werden können. Der Leser sollte daher die Risiken kennenlernen, die bei der Internet-Kommunikation auftreten können, aber auch die Ansätze vermittelt bekommen, mit denen eine weitgehende Sicherheit bei der Internet-Kommunikation erreicht werden kann.

Um die verschiedenen Sicherheitskonzepte in einen formalen Rahmen einordnen zu können, orientiert sich die Struktur dieses Buchs am Schichtenmodell, das von der International Organization for Standardization im ISO-Open-Systems-Interconnection-Modell vorgeschlagen und standardisiert wurde. Nach der Erläuterung dieses Modells bzw. der auf den verschiedenen Schichten angesiedelten Sicherheitsmechanismen und Sicherheitsdienste wird der praktische Einsatz der dargestellten Konzepte anhand von ausgewählten Beispielen (bspw. der *IP-Telefonie* und dem *Internet-Banking*) demonstriert. Mit Hilfe der übergreifenden Anwendungen, aber auch mit Hilfe einer Vielzahl von Beispielen auf Ebene der einzelnen Schichten (bspw. *Secure Socket Layer*, *SSL* oder *IPsec*), soll der Leser in die Lage versetzt werden, das Zusammenspiel der verschiedenen Komponenten nachvollziehen zu können.

Für wen ist dieses Buch?

Betrachtet man die in letzter Zeit erschienene Literatur zum Thema *Sicherheit in Rechnernetzen*, so kann diese durch folgende Charakteristika beschrieben werden:

- Zielgruppen sind häufig Informatiker bzw. Systemadministratoren.
- Die Problematik wird in einem sehr großen Detailgrad beschrieben. Gerade für weniger erfahrene Anwender stellt sich hierbei das Problem, aus einer Vielzahl vorgestellter Alternativen die für ihn relevanten herauszufinden, da meist die notwendigen Grundkenntnisse nicht vermittelt werden.
- Einige Bücher beschreiben verschiedenste Varianten von Attacken auf Netzwerke. Es ist aber für den Anwender nur schwer erkennbar, welche Möglichkeiten existieren, um Netzwerke mit einem zufriedenstellenden Sicherheitsgrad zu betreiben.

Das vorliegende Buch setzt sich das Ziel, Sicherheitsstrategien für die Internet-Kommunikation für einen Zielkreis vorzugeben, der nicht zwingend nur aus Informatikern besteht. In diesem Umfeld sollen Sicherheitsstrategien sowie die Risiken ihrer Anwendung verständlich erklärt werden. Zu unserer Zielgruppe zählen wir daher neben Studenten (der Informatik und der Elektrotechnik/Informationstechnik) alle, die an Sicherheitskonzepten im Internet Interesse und Gefallen finden.

Das Buch soll auch bewusst als Grundlage verstanden werden, die dem Neuling einen verständlichen Einstieg ermöglicht, dem erfahrenen Anwender aber auch genügend Referenzen anbietet, um Spezialgebiete weiter zu vertiefen. Wir verstehen dieses Buch daher auch nicht als Referenzwerk für Sicherheit, das umfassend zu jedem Sicherheitsmechanismus jedes technische Detail darstellt.

Danksagung

Besonderen Dank schulden wir *Ralf Steinmetz*, dem Inhaber des Lehrstuhls für Industrielle Prozess- und Systemkommunikation an der Technischen Universität Darmstadt. Herr Steinmetz war uns nicht nur ein wertvoller Ratgeber, sondern ist durch sein außergewöhnliches Engagement auch maßgeblich dafür verantwortlich, dass wir Autoren überhaupt die Anstrengung unternommen haben, ein derartiges Buch zu verfassen.

Auch den Studenten des Lehrstuhls, die für uns als Hilfskräfte, als Diplom- und Studienarbeiter tätig sind, danken wir, da auch durch ihr Wirken das Wissen, das in diesem Buch steckt, entstehen konnte.

An dieser Stelle möchten wir uns auch bei Rolf Oppliger bedanken, aus dessen Werken wir bei der Konzeption dieses Buchs an mancher Stelle wertvolle Anregungen gewonnen haben.

Ebenfalls danken möchten wir Reinhard Bertram und Achim Steinacker, die als Mit-Autoren des Buchs *Open Security – Von den Grundlagen zu den Anwendungen* die Basis für dieses Werk gelegt haben.

Darmstadt, im Winter 1999/2000

Stephan Fischer, Christoph Rensing und Utz Rödig

Inhaltsverzeichnis