um eine Einführung ausschließlich in die Technik der Rechnerkommunikation handelt. Nicht besprochen wird nämlich, wer lt. Telekommunikationsgesetz Netze einrichten und betreiben darf, welche Aufgaben das Netzmanagement hat und welche Alternativen für den konkreten Einsatz in Wirtschaftsunternehmen (z. B. Handel, Banken) bestehen. Aber dafür gibt es genügend andere Literatur.

Peter Stahlknecht (Osnabrück)

Eckert, C.

IT-Sicherheit

Konzepte – Verfahren – Protokolle
ISBN 3-486-57851-0, Oldenbourg-Verlag,
4. Aufl., München 2006, 918 Seiten,
€ 59,80

Das bereits in der 4. Auflage vorliegende und sehr umfangreiche Werk zum Thema IT-Sicherheit lässt sich ohne weiteres als Standardwerk zu diesem aktuellen und äußerst wichtigen Forschungsbereich der Informatik bezeichnen. Der Autorin, Professorin für Informatik an der TU Darmstadt und Leiterin des Fraunhofer Instituts für Sichere Telekooperation, ist es gelungen, eine aktualisierte und verbesserte Auflage ihres Werkes zu erstellen, dass sich hervorragend für die Lehre eignet und eine ausgezeichnete Basis für weitere Forschungsarbeiten bietet.

Das sehr umfangreiche Buch gliedert sich in 13 Kapitel. Nach einer Einführung (Kapitel 1), in der u. a. grundlegende Begriffe, Schutzziele, Schwachstellen und Sicherheitsstrategien erläutert werden, werden spezielle Bedrohungen wie z. B. Viren, Würmer und Trojanische Pferde behandelt (Kapitel 2). Kapitel 3 widmet sich in ausführlicher Form der Internet-(Un)Sicherheit, erklärt die Internet-Protokollfamilie und ihre Sicherheitsprobleme. Organisatorische Themen werden in den folgenden drei Kapiteln diskutiert. In Kapitel 4 wird zunächst ein Security Engineering-Ansatz als Vorgehensmodell vorgestellt, der sich grob in die vier Phasen Planung, Ausführung, Prüfung und Anpassung einteilen lässt. Die Bewertungskriterien werden in Kapitel 5 und die Sicherheitsmodelle in Kapitel 6 behandelt.

In sehr gut nachvollziehbarer Form werden in Kapitel 7 die Kryptografischen Verfahren und in Kapitel 8 die Hashfunktionen und elektronischen Signaturen erläutert. Das Schlüsselmanagement in Kapitel 9 setzt sich mit der sicheren Erzeugung, Verteilung, Zertifizierung, Speicherung bzw. Archivierung sowie Vernichtung von Schlüsseln auseinander. Die sehr wichtigen und anspruchsvollen Themen Authentifikation und Zugriffskon-

trolle sind Gegenstand der Kapitel 10 und 11. Hier werden in anschaulicher Form u. a. die Smartcard, die Biometrie, Speicherschutz, Objektschutz und Trusted Computing behandelt. Abschließend erklärt die Autorin die Sicherheit in Netzen (Kapitel 12) und die sichere Kommunikation bei mobiler und drahtloser Übertragung (Kapitel 13).

Das Buch ist logisch gut strukturiert und gegliedert. Marginalien und zahlreiche gut aufbereitete Abbildungen tragen zum besseren Verständnis bei. Beispiele zeigen die Wichtigkeit und Notwendigkeit der IT-Sicherheit auf. Das gegebene Glossar ist leider nur ein Abkürzungsverzeichnis. Ein Glossar mit den Kurzerklärungen der wichtigsten Begriffe wäre wünschenswert. Hilfreich sind das Inhaltsverzeichnis und die umfangreiche Literaturliste. Insgesamt ist das Buch ohne Bedenken zu empfehlen, und zwar als didaktisch gut aufbereitetes Lehrbuch für die Studierenden der Informatik und der Wirtschaftsinformatik, aber auch für alle Forscher und Praktiker als nützliches Nachschlagewerk.

Roland Gabriel, Bochum

Mörke, M.; Teufel, St. (Hrsg.)

Kosten und Nutzen von IT-Sicherheit

Praxis der Wirtschaftsinformatik (HMD),
Heft 248, April 2006
ISBN 3-89864-380-8, dpunkt,
Heidelberg 2006, 128 Seiten, € 23,50

IT-Sicherheit ist ein aktuelles Schwerpunktthema der Informatik, wobei hier vor allem die technischen und kryptografischen Bereiche im Mittelpunkt stehen. Die Wirtschaftsinformatik setzt sich in letzter Zeit immer stärker mit den organisatorischen und wirtschaftlichen Fragestellungen auseinander, so dass auch die Kosten und der Nutzen von IT-Sicherheit relevante Themen darstellen, die vor allem für den IT-Einsatz in der Praxis wichtig sind.

Das vorliegende Heft 248 der Praxis der Wirtschaftsinformatik (HMD) widmet sich mit zehn Beiträgen diesem hoch aktuellen und interessanten Informatikbereich. Bereits im Vorwort erklären die beiden Herausgeber, „dass die Untersuchung der Kosten-Nutzen-Relation von IT-Sicherheit nach wie vor erst an ihrem Anfang steht“ und „dass es außerordentlich schwierig war, eine ausgewogene Darstellung aller involvierten Themen in diesem Heft zu erreichen, ...“.

Die Auswahl der Themen ist jedoch gelungen, und die Beiträge sind insgesamt sehr interessant und inhaltlich gut aufbereitet. Nach einer allgemeinen kurzen Einführung von H. Federrath gibt H. P. Lubich eine

übersichtliche Darstellung der Systematik und erörtert aktuelle Probleme. Wichtig sind hier auch die unterschiedlichen Ansätze der Kostenermittlung für IT-Sicherheit und die Maßnahmen zur „Kostenoptimierung“. Einen sehr interessanten Beitrag liefert D. Schadt über die Ökonomie der IT-Sicherheit, der sich u. a. mit der Organisation und mit brauchbaren Alternativen bei der Risikoanalyse auseinandersetzt. N. Pohlmann diskutiert die Methode Return on Security Investment (ROSI) und gibt hierzu anschauliche Beispiele. Aktuelle Ansätze zum Messen von Sicherheit liefert S. Müßig in seinem Beitrag, in dem die Rendite von Sicherheitsinvestitionen untersucht wird. A. Gadatsch und H. Uebelacker betrachten die Wirtschaftlichkeit für IT-Security-Projekte an ausgewählten Beispielen. Weitere Beiträge widmen sich der Messung der Informationssicherheit (P. Windemann, Th. Schlienger, St. Teufel) und dem Open-Source-Sicherheits-Management (A. Wiesmann). J. Altmeier stellt den ROSI-Ansatz speziell am Beispiel der Business-Applikation SAP dar, und die Wirtschaftlichkeit von E-Mail-Verschlüsselung wird von M. Jerger und M. Mitev untersucht. Abschließend werden Kosten und Nutzen von Penetrationstests von S. Schreiber erörtert. Das Heft enthält weiterhin ein nützliches Glossar, das man noch um einige wichtige Begriffe erweitern könnte.

Alle Beiträge sind praxisorientiert verfasst, ergänzt um zahlreiche Anwendungsbeispiele. I. d. R. werden brauchbare Begriffserklärungen und Klassifikationen gegeben, die das komplexe Thema gut strukturieren und verständlicher machen. Das Heft bietet eine gute Hilfe an für alle, die sich in der Praxis mit dem Thema IT-Sicherheit auseinandersetzen und dabei vor allem die Wirtschaftlichkeitsaspekte betrachten.

Roland Gabriel, Bochum

Müller, K.-R.

IT-Sicherheit mit System

ISBN 3-528-15838-7, 2. Aufl., Vieweg,
Wiesbaden 2005, 327 Seiten, € 59,90

Die Bedrohungen aus dem Internet werden immer umfangreicher und sind noch lange nicht gebannt. Gerade für Unternehmen mit einem hohen Schutzbedarf stellen solche Gefahren natürlich ein enormes Risiko dar. Um dem entgegenzuwirken, stellt der Autor mit seiner dreidimensionalen Sicherheitspyramide ein strukturiertes Konzept vor, mit dem Schritt für Schritt ein unternehmerisches Sicherheitssystem nicht nur aufbauen (Top Down), sondern später auch