

REZENSIONEN



Roland Hellmann:
**IT-Sicherheit.
 Methoden und
 Schutzmaßnahmen für sichere
 Cybersysteme.**

Berlin: De Gruyter 2022,
 Reihe De Gruyter Studium, 244 S.,
 ISBN 978-3110767087
 EUR 44,95.

Claudia Eckert:
**IT-Sicherheit.
 Konzepte – Verfahren –
 Protokolle.**

Berlin: De Gruyter 2023,
 Reihe De Gruyter Studium, 1.004 S.,
 ISBN 978-3110996890
 EUR 84,95.



Kenntnisse über Informationstechnologie (IT) werden für die Arbeit in Bibliotheken immer wichtiger. Die Einführung von Cloudsystemen und die Art und Weise der immer häufiger stattfindenden Cyberangriffe zeigen deutlich, dass die IT-Sicherheit nicht nur ein Thema der damit befassten Informatiker der jeweiligen IT-Abteilung ist, die die Bibliotheken betreut. Zu dieser Thematik liegen zwei ganz unterschiedliche Bücher aus dem De Gruyter Verlag vor.

Das Buch von Roland Hellmann, Dozent an der Fachhochschule Aalen, ist als Lehrbuch konzipiert und eignet sich speziell für Bibliothekarinnen und Bibliothekare, die nicht aus dem IT-Bereich kommen. Ein klug konzipierter Aufbau des Buches führt von den Grundbegriffen und der Methodik hin zur Vorstellung einzelner Bedrohungen für IT-Systeme: Kryptologie und ihre Anwendung: Verschlüsselung, Digitale Signatur, Steganographie – Verfügbarkeit – Internetsicherheit und Schadsoftware

– Firewalls – Sicherheit im Internet der Dinge.

Wie unterschiedlich die Vorkenntnisse auch sein mögen, die Leserinnen und Leser mitbringen und welche Erwartungen sie an die Thematik der IT-Sicherheit auch haben mögen, es werden möglichst wenige mathematisch-technische Vorkenntnisse vorausgesetzt, sodass auch Fachfremde den Einstieg in die Thematik finden. Gemäß der Intention des Autors soll dieses Werk Studierenden der Informatik und verwandter Disziplinen helfen, ein grundlegendes Verständnis für die IT-Sicherheit und deren Bedeutung zu bekommen. Am Ende jedes einzelnen Kapitels schließen sich Übungsaufgaben an, deren Lösungen im Anhang zu finden sind. Diese machen das Werk besonders geeignet für das Selbststudium und die Weiterbildung. Im Buch werden die Grundlagen der IT-Sicherheit erklärt, wobei auch die wichtigsten Methoden der Kryptographie allgemein verständlich dargestellt werden. Die Verfügbarkeit von Speichermedien und Daten, die Internet-Sicherheit und Firewalls werden ausführlich behandelt, und aktuelle Themen der Internet of Things (IoT)-Sicherheit wird abgedeckt. Besonders gut gelungen sind die Schritt-für-Schritt-Grafiken, anhand derer Verfahren wie z.B. die Public-Key-Verschlüsselung, Man in the middle (MITM)-Attacken, Digitale Signaturen, der Transport Layer Security (TLS)-Verbindungsaufbau und darüber hinaus viele Themen erklärt werden. Wer sich einen Überblick über die IT-Sicherheit verschaffen will, dem gelingt mit der Lektüre des Buches der Einstieg in diese Thematik mit Sicherheit.

Ganz anders konzipiert ist das Buch von Claudia Eckert, IT-Sicherheit: Konzepte – Verfahren – Protokolle, das in 11. Auflage

im gleichnamigen Verlag erschienen ist. Mit der Publikation dieses Buches hat die Autorin, Inhaberin des entsprechenden Lehrstuhls an der Technischen Universität München, sich als Zielsetzung vorgenommen, eine umfassende Information über wirksame Maßnahmen zu vermitteln, die erforderlich sind, um die vielfältigen Sicherheitsbedrohungen abzuwehren, denen heutige und zukünftige IT-Systeme ausgesetzt sind. Wie die Autorin erklärt, hängt die Qualität eines sicheren IT-Systems wesentlich davon ab, ob seine Konstruktion methodisch und systematisch erfolgt.

Wie bei der Publikation von Hellmann werden in einem ersten Kapitel die Grundbegriffe ausführlich erklärt. Die Autorin unterscheidet zwischen Risiko und Bedrohung. Dies ist aus Praktiker Sicht wenig sinnvoll. Als „Risiko einer Bedrohung“ bezeichnet die Autorin die Wahrscheinlichkeit des Eintritts eines Schadenereignisses und die Höhe des potenziellen Schadens, der dadurch hervorgerufen wird. Als „Bedrohung des Systems“ definiert die Autorin eine oder mehrere Schwachstellen, die zu einem Verlust der Datenintegrität, der Vertraulichkeit der gespeicherten Daten oder deren Verfügbarkeit führt. Dies ist für ein Bibliothekssystem irrelevant. Beide Herausforderungen beeinträchtigen das gute Funktionieren des Systems, ob sie jetzt potentiell oder real sind. Sicherheit ist kein originäres Ziel einer Bibliothek in Bezug auf ihr IT-System, dafür ist eine gewisse Risikobereitschaft notwendig. Risiken sind daher die aus der Unvorhersehbarkeit der Zukunft resultierenden Störungen des Betriebs, die „zufällig“ als Möglichkeiten auftreten können. Sicherheit sollte daher als Leitidee formuliert werden, die nicht in jedem Fall garantiert werden kann.

Das zweite Kapitel widmet sich der Vielzahl von Bedrohungen, die Ursache für die in heutigen Systemen am häufigsten auftretenden Sicherheitsprobleme sein können (so werden im Buch namentlich Buffer-Overflow, Viren, Würmer und Trojanische Pferde genannt und beschrieben). Die folgenden Kapitel 3 und 4 beschäftigen sich mit dem Internet und seinen Unsicherheiten, sowie dem Security Engineering. Das

fünfte Kapitel zeigt den Lesenden die Vielfalt der methodischen Bewertung der Sicherheit informationstechnischer Systeme auf. Auf Sicherheitsmodelle, kryptografische Verfahren, Hashfunktionen und elektronische Signaturen beschränken sich die Kapitel 6 bis 8. Die anschließenden Kapitel setzen sich mit den Themen „Schlüsselmanagement“, „Authentifikation“, „Digitale Identität“ und „Zugriffskontrolle“ auseinander. Das aktuelle Thema „Sichere mobile und drahtlose Kommunikation“ ist Schwerpunkt des Schlusskapitels 14.

Der Stil der Autorin ist nicht sehr eingängig. Um Vollständigkeit bemüht, geraten gewisse Kapitel geradezu zu epischer Länge. Als Praktiker hätte man sich einerseits mehr Beispiele aus anderen Fachgebieten gewünscht und nicht nur aus der Software-Entwicklung. Des Weiteren dürfte der Autorin bekannt sein, dass Windows 10 zwar immer noch weit verbreitet ist, das aktuelle Betriebssystem aber heute Windows 11 ist und Windows 12 sich in der Pipeline befindet. Da wäre eine entsprechende sprachliche Überarbeitung kein Luxus, auch wenn technisch gesehen keine große Änderung ins Haus steht.

Das für Praktiker sehr relevante Thema der Risikoanalyse (S. 187 f.) ist dermaßen wissenschaftlich ausgefallen, dass der Praktiker damit wenig anfangen kann. Für eine künftige Auflage wäre wünschenswert, wenn die Autorin ihr Buch an dieser Stelle um aktuelle Methoden des operationellen Risikomanagement erweitern würde. Ein Abschnitt mit einem Fazit am Ende fehlt leider.

Trotz dieser Einschränkungen ist das Buch als umfangreiches Nachschlagewerk (988 Seiten) für Praktiker zu empfehlen. Wer sich hingegen einen Überblick über das Thema IT-Sicherheit verschaffen möchte, sei es im Selbststudium oder zu Weiterbildungszwecken, dem sei das Buch von Roland Hellmann empfohlen.

Stephan Holländer, Basel

Thomas Böhm (Hg.):
**Die Wunderkammer
des Lesens.**

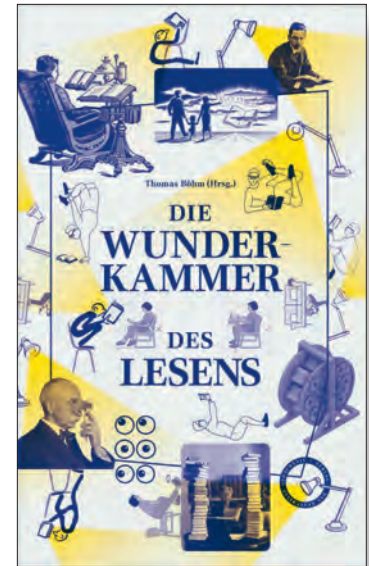
Berlin: Verlag Das Kulturelle Gedächtnis
2023; 318 S.: ill.,
ISBN 978-3-946990-76-5,
EUR 28,00.

Bekanntlich waren die frühneuzeitlichen Wunderkammern Vorläufer vieler heutiger Institutionen, beispielsweise von Kunst- und Naturkundemuseen, von Waffenkammern ebenso wie von Panoptiken und Kuriositätenkabinetten. Entsprechend fanden sich dort höchst unterschiedliche Gegenstände versammelt: Seltene Naturphänomene lagen neben Objekten des Kunsthandwerks, Bücher standen neben Automaten. Ein wenig verhält es sich so auch mit dem anzuzeigenden Buch. Es enthält eine Variation an sehr verschiedenen Texten rund um das Gene-

ralthema Lesen. Der Herausgeber möchte diese, wie er im Vorwort schreibt, als Einladung verstehen, um „das eigene Lesen zu bereichern – und sich von den kuriosen, erhellenden und poetischen Episoden aus der Kulturgeschichte des Lesens unterhalten zu lassen.“ (11) Dass ihm dies vortrefflich gelingt, liegt nicht nur an der durchdachten, klugen, oft überraschenden und überdies kurzweiligen Auswahl der hier zu findenden Abfassungen, sondern auch an der außerordentlich schönen Gestaltung des Buches. Man kann die an diesem wahren Kunstwerk Beteiligten zu diesem großen Wurf nur beglückwünschen!

Zielpublikum: Bibliothekarinnen und Bibliothekare, Germanistinnen und Germanisten

Konrad Stidl, Regensburg



Christoph Reske:
**Drucken in der
Handpressenzeit im deutschen
Sprachbereich (1450–1800).**

Technik und Handwerk in Druckereien
und bei der Herstellung von
Büchern (Beiträge zum Buch- und
Bibliothekswesen 69).
Wiesbaden: Harrassowitz Verlag 2023;
410 S.: ill., ISBN 978-3-447-12030-2,
EUR 98,00.

Christoph Reske, wissenschaftlicher Mitarbeiter am Lehrstuhl für Buchwissenschaft der Universität Mainz, ist buchgeschichtlich Interessierten durch ein stupendes Werk über die deutschen Buchdrucker des 16. Jahrhunderts bestens bekannt (Die Buchdrucker des 16. und 17. Jahrhunderts im deutschen Sprachgebiet. Auf der Grundlage des gleichnamigen Werkes von Josef Benzing [Beiträge zum Buch- und Bibliothekswesen 51] Wiesba-

den: Harrassowitz 2015). Nun hat er ein Werk über die praktischen Vorgänge und Abläufe des Druckens im Zeitalter der Handpressenzeit, also von Erfindung des Buchdrucks bis etwa zum Jahr 1800, vorgelegt. Und auch dieses Werk ist exzellent. Reskes Buch kann schon jetzt – unmittelbar nach dem Erscheinen – als Standardwerk gelten. Denn an keiner anderen Stelle findet man alle wesentlichen Elemente des Buchdrucks in der Vormoderne so konzise, gleichzeitig so fachkundig und auf dem aktuellen Stand der Forschung dargestellt. Ein herausragendes Buch, das man allen an buchhistorischen Themen Interessierten nur ausdrücklich ans Herz legen kann.

Zielpublikum: Bibliothekarinnen und Bibliothekare, Geisteswissenschaftlerinnen und Geisteswissenschaftler

Konrad Stidl, Regensburg

