Knoll, Matthias

Book Review — Published Version

Rezension „Cyber-Sicherheit“

HMD Praxis der Wirtschaftsinformatik

Provided in Cooperation with:
Springer Nature

Suggested Citation: Knoll, Matthias (2023) : Rezension „Cyber-Sicherheit“, HMD Praxis der Wirtschaftsinformatik, ISSN 2198-2775, Springer Fachmedien Wiesbaden GmbH, Wiesbaden, Vol. 60, Iss. 2, pp. 510-513, https://doi.org/10.1365/s40702-023-00956-2

This Version is available at:
https://hdl.handle.net/10419/307579

HMD Praxis der Wirtschaftsinformatik (2023) 60:510–513
https://doi.org/10.1365/s40702-023-00956-2

REZENSION

Rezension „Cyber-Sicherheit“

Matthias Knoll

Angenommen: 13. Februar 2023 / Online publiziert: 27. Februar 2023

Norbert Pohlmann **Cyber-Sicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung**

ISBN 978-3-658-36242-3, Springer Vieweg, Wiesbaden 2022, 2. Aufl., 775 S., 32,99 €

Nicht erst aktuelle, teilweise spektakuläre Sicherheitsvorfälle bestätigen die hohe Bedeutung guter Cyber-Sicherheitssysteme. Solche Systeme entstehen jedoch nicht von selbst. Es ist daher von zentraler Bedeutung, das Thema für Studierende und die berufliche Weiterbildung anwendungsorientiert, systematisch, thematisch breit und angemessen detailliert aufzubereiten.

Das 2022 in der 2. Auflage erschienene Lehrbuch erfüllt diese Anforderungen auf über 770 Seiten. Genug Raum, um alle relevanten Aspekte zu beleuchten, ohne dabei Anspruch auf eine angesichts der Thematik in einem einzigen Buch nicht erreichbare Vollständigkeit zu erheben. Vielmehr wird in allen Kapiteln des Buches anhand von Beispielen im Text und Verständnisfragen am Kapitelende aufgezeigt, wie die anspruchsvolle Theorie angewandt werden kann. Das Buch hilft dabei jedoch nicht nur, angehende Fachleute im Themengebiet auf ihre späteren Aufgaben vorzubereiten. Es eignet sich auch sehr gut als Informationsquelle für alle an der Cyber-Sicherheit Interessierten in Fachabteilungen ohne unmittelbaren IT-Bezug und für Prüfende in der Revision, die einschätzen müssen, wo und wie sie selbst prüfen können und wo externe Sachverständige hinzugezogen werden sollten.

Dazu wird das Themengebiet in insgesamt 20 Kapiteln ausgehend von wichtigen Grundlagen sowie einer gesellschaftlichen Einordnung erschlossen. So greift das

✉ Matthias Knoll
Hochschule Darmstadt, Darmstadt, Deutschland
E-Mail: matthias.knoll@h-da.de

Kapitel 1 zentrale Herausforderungen der Cyber-Sicherheit, Rahmenbedingungen, Paradigmen und grundlegende Begriffe, wie etwa die Wirksamkeit, auf. Aber auch Bedürfnisse, Ziele, Strategien, die Motivation von Angreifern und weitere Fragestellungen werden angesprochen. Das für die Schwerpunktausgabe April 2022 der „HMD – Praxis der Wirtschaftsinformatik“ zu Digitalen Identitäten besonders interessante Themenfeld „Identifikation und Authentifikation“ wird dabei in Kapitel 1.2.3 und später nochmals ausführlich in Kapitel 5 und 18 aufgegriffen.

Kapitel 2 widmet sich der mathematisch anspruchsvollen Kryptographie. Dabei wird nur so weit auf die teilweise sehr komplexe Theorie zurückgegriffen, dass Grundprinzipien sicher nachvollzogen und anhand einfacher Beispiele und Aufgaben das korrekte Verständnis für das angeeignete Wissen überprüft werden kann – nicht nur hier ein gelungener Weg, um die Motivation zur Erschließung der Themen zu erhöhen.

Logisch konsequent widmen sich Kapitel 3 den Hardware-Sicherheitsmodulen, Kapitel 4 den digitalen Signaturen, Zertifikaten und der Public-Key-Infrastruktur und Kapitel 5 der Identifikation und Authentifikation. Auch diese Kapitel enthalten alle Informationen, die für einen Überblick und ein grundlegendes Verständnis entscheidend sind. Besonders interessant ist die in Kapitel 5 vorgestellte risikobasierte und adaptive Authentifizierung, vielleicht auch, weil sie uns im Alltag bereits in unterschiedlicher Form und möglicherweise weitgehend unbemerkt begleitet. Hervorgehoben sei an dieser Stelle auch, dass sich Identifikation und Authentifikation nicht ausschließlich auf Personen, sondern auch auf IT-Systeme bezieht. Ein mit zunehmender Verbreitung von IoT-Devices im Smart-Home- und Industrie-4.0-Kontext zentraler Aspekt.

An Fragen der Identität und Authentifizierung schließt sich Kapitel 6 mit einer umfassenden Betrachtung der Identity- und Access-Problematik in Unternehmen an. Um die komplizierte und für Unternehmen kritische Thematik leichter erfassbar zu machen, enthalten die Unterabschnitte kleine, leicht nachvollziehbare, aber ein wenig zu knappe Beispiele. Sie könnten durchaus detaillierter und konkreter sein.

Die folgenden drei Kapitel orientieren sich an Anwendungs- und Einsatz-Szenarien zur Erhöhung der Cyber-Sicherheit. Sie diskutieren Trusted Computing, Cyber-Sicherheit-Frühwarn-/Lagebildsysteme und Firewall-Systeme. Wie anspruchsvoll diese Themen sind, zeigen beispielhaft herausgegriffen sehr anschaulich formulierte Beschreibungen zum Aufbau eines Cyber-Sicherheit-Frühwarnsystems oder der Funktionsweise einer Next-Generation-Firewall.

Warum sich in den beiden folgenden Kapiteln 11 und 12 die eher abstrakten Themen IPSec-Verschlüsselung und TLS/SSL anschließen, bleibt ein wenig unklar, man hätte sie bereits früher, näher an den Grundlagen-orientierten Inhalten erwartet. Vergleichbares gilt für Kapitel 18 (Self-Sovereign Identity), das näher an Kapitel 5 hätte gerückt werden können, und Kapitel 19 (Vertrauen und Vertrauenswürdigkeit), das durchaus auch direkt auf Kapitel 1 hätte folgen können. Da das Buch linear gelesen werden kann, aber nicht muss, ist das jedoch sicherlich Kritik auf hohem Niveau und schmälert den guten Gesamteindruck nicht.

Die anschließenden fünf Kapitel widmen sich erneut ganz praktischen Fragestellungen. Die Abwehr von (D)DoS-Angriffen wird dabei ebenso diskutiert wie das immerwährend aktuelle Thema E-Mail-Sicherheit. Aufgegriffen werden auch

Blockchain, KI und Cyber-Sicherheit sowie Sicherheit im Social-Web-Kontext. Eine Rezension kann gar nicht so umfassend sein, um alle beim Lesen als spannend empfundenen Details zu erwähnen. Doch ein Punkt verdient herausgegriffen zu werden: KI, Cyber-Sicherheit und Ethik. Es ist sehr gut und wichtig, dass diese Themen angesprochen werden. Denn aus den überaus spannenden und gesamtgesellschaftlich relevanten Fragen ließe sich problemlos ein eigenes Buch und eine eigene Lehrveranstaltung entwickeln.

Kapitel 17 greift einen heiklen Punkt auf: Die Frage der Wirtschaftlichkeit von Cyber-Sicherheits-Maßnahmen. Wie lässt sich die Angemessenheit sinnvoll ermitteln? Gelungen ist hier ein einfaches Rechenbeispiel, das zeigt, wie schwierig es sein kann, einen guten Weg zwischen zu viel und zu wenig Sicherheit zu finden.

Kapitel 20 schließlich rundet das Buch mit ausgewählten weiteren Fragen ab. Besonders hervorzuheben, weil nahe am Alltag nicht nur von Studierenden, ist hierin das Aufgreifen von Chancen und Risiken im Smart-Home-Kontext, ein Themengebiet, das oftmals vollkommen unterschätzt wird. Zugegeben, vorteilhaft ist der Einsatz durchaus, auch kann er die Sicherheit des eigenen Zuhauses erhöhen. Und: Wie elegant ist es doch, von überall her auf die IoT-Geräte im eigenen Haushalt zuzugreifen. Doch was man selbst kann, könnte theoretisch auch ein Angreifer. Und wer will den schon – wenn auch nur virtuell – im eigenen Zuhause haben?

Wie der Autor im Vorwort selbst erklärt, ist das Themengebiet unerschöpflich. Es ist daher immer eine Gratwanderung, was in eine neue Auflage Eingang finden kann. Für die 3. Auflage könnte beispielsweise interessant sein, die Hardware-Sicherheitsmodule noch etwas ausführlicher zu betrachten, ebenso anspruchsvolle Verfahren wie die Wiederherstellung einer zerstörten oder verlorenen Blockchain-Wallet oder das aktuell vieldiskutierte Zero-Trust-Modell. Mit zunehmender Verfügbarkeit rechtssicherer und akzeptierter Lösungen für digitale Identitäten könnten zudem die Kapitel 5 und 18 um entsprechende Aspekte ergänzt werden. Auch wäre es durchaus hilfreich, die in Kapitel 6.9 diskutierten Compliance- und Audit-Themen in anderen Kapiteln aufzugreifen (beispielsweise im Firewall-Kontext) oder gleich ein eigenes Kapitel hierfür vorzusehen.

Doch selbst wenn ein solches Buch eigentlich niemals „fertiggestellt“ sein kann, bietet die 2. Auflage ein übervolles Füllhorn an Wissen und ist damit nicht nur für Lehrveranstaltungen ein idealer und uneingeschränkt zu empfehlender Begleiter, sondern auch bei der alltäglichen Bewältigung der stetig zunehmenden Cyber-Sicherheits-Herausforderungen. Unterstützt wird das Buch durch zahlreiche zusätzliche Informationen und Materialien, wie etwa Lösungen zu den Verständnisfragen, die auf der Website des Autors bereitgestellt werden. Nicht nur damit wird einmal mehr deutlich, dass der Autor hier mit großer Begeisterung für das Themenfeld tätig ist – und hoffentlich auch künftig sein wird.

Funding Open Access funding enabled and organized by Projekt DEAL.