

Mario Pufahl · Patrick Paulsen ·  
Paul Arndt

# Cybersecurity für Manager

Cybergefahren wirksam begegnen –  
das Kompetenzmodell für die Praxis



 Springer Gabler

---

# Cybersecurity für Manager

---

Mario Pufahl · Patrick Paulsen ·  
Paul Arndt

# Cybersecurity für Manager

Cybergefahren wirksam  
begegnen – das Kompetenzmodell  
für die Praxis

 Springer Gabler

Mario Pufahl  
Düsseldorf, Deutschland

Patrick Paulsen  
Norderstedt, Deutschland

Paul Arndt  
Darmstadt, Deutschland

ISBN 978-3-658-44891-2      ISBN 978-3-658-44892-9 (eBook)  
<https://doi.org/10.1007/978-3-658-44892-9>

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <https://portal.dnb.de> abrufbar.

© Der/die Herausgeber bzw. der/die Autor(en), exklusiv lizenziert an Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2024

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von allgemein beschreibenden Bezeichnungen, Marken, Unternehmensnamen etc. in diesem Werk bedeutet nicht, dass diese frei durch jede Person benutzt werden dürfen. Die Berechtigung zur Benutzung unterliegt, auch ohne gesonderten Hinweis hierzu, den Regeln des Markenrechts. Die Rechte des/der jeweiligen Zeicheninhaber\*in sind zu beachten.

Der Verlag, die Autor\*innen und die Herausgeber\*innen gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag noch die Autor\*innen oder die Herausgeber\*innen übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Planung/Lektorat: Maximilian David

Springer Gabler 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

Wenn Sie dieses Produkt entsorgen, geben Sie das Papier bitte zum Recycling.

---

## Vorwort

In einer zunehmend vernetzten Welt, in der digitale Technologien unser tägliches Leben bestimmen und die Anzahl der Hackerangriffe weiter steigt, ist der Schutz der sensiblen Daten und Systeme der Unternehmen von entscheidender Bedeutung.

Dieses Buch bietet Führungskräften, Geschäftsführern und Vorständen einen Überblick über die wichtigsten Bereiche der Cybersecurity. Im Gegensatz zu vielen technischen Leitfäden ist es das Ziel dieses Buches, einen praktischen Leitfaden und Handlungsempfehlungen für das Management zu geben. Es enthält konkrete Hilfestellungen und Erläuterungen aktueller Trends sowie ein Kompetenzmodell inklusive Detailerläuterungen der wichtigsten Bausteine für die operative Umsetzung. Darüber hinaus bieten Experteninterviews aus unterschiedlichen Blickwinkeln konkrete Einsichten rund um professionelle Cybersecurity in Unternehmen.

Warum ist dieses Buch relevant? Weil es nicht nur technische Details vermittelt, sondern auch das Bewusstsein für die Dringlichkeit von Sicherheitsmaßnahmen schärft. Wir leben in einer Zeit, in der Cyberangriffe nicht nur finanzielle Verluste verursachen, sondern auch das Vertrauen in unsere digitalen Systeme erschüttern können.

Dieses Buch soll komplexe Konzepte kompakt und verständlich erklären sowie praktische Ratschläge geben, die Sie im beruflichen Alltag umsetzen können. Wir hoffen, dass Sie dieses Vorworts neugierig auf die folgenden Kapitel macht und deren Lektüre Ihnen die Kompetenzen vermittelt, die nötig sind, um die digitale Welt sicherer zu machen – für Ihr Unternehmen und dessen Umfeld.

Unser Dank gilt vor allem unseren Experten, die sich Zeit für die Interviews genommen und wertvolle Einsichten gegeben haben, aber auch unseren Unterstützern für die grafische Umsetzung durch Sabine Kirchem und Delyana Dancheva. Besonderen Dank möchten wir auch an den Cyberexperten Nico Werner richten, der uns mit seiner Spezialexpertise rund um Cybersecurity im Hintergrund, bei der Qualitätssicherung und bei einem Interview sehr geholfen hat.

Frankfurt  
im Mai 2024

Mario Pufahl  
Patrick Paulsen  
Paul Arndt

---

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung: Warum Cybersecurity Heute Unverzichtbar Ist</b>	<b>1</b>
	Literatur	7
<b>2</b>	<b>Das Cybersecurity-Kompetenzmodell – Basis Einer Ganzheitlichen Ausrichtung auf Cybergefahren</b>	<b>9</b>
2.1	Cybersecurity aus der Sicht des Angreifers	9
2.2	Warum ist Cybersecurity wichtig?	14
2.2.1	Gesetze und Compliance	15
2.2.2	Organisationsinteressen	16
2.3	Was kann geschützt werden?	17
2.3.1	Technologien und Daten	17
2.3.2	Faktor Mensch	19
2.3.3	Physische Infrastruktur	20
2.4	Was sind die essenziellen Cybersecurity-Bereiche in Unternehmen?	21
2.4.1	Security Governance	21
2.4.2	Assessments	22
2.4.3	Integration	23
2.4.4	Security Operations	25
2.4.5	Digital Identity	27
2.4.6	Zero Trust	28
2.5	Wie kann eine Organisation das Thema Cybersecurity umsetzen?	29
2.5.1	Sicherheit planen	30

---

2.5.2	Implementieren .....	30
2.5.3	Validieren .....	31
2.5.4	Optimieren .....	31
Literatur	.....	31
<b>3</b>	<b>Umsetzung Des Cybersecurity-Kompetenzmodells .....</b>	<b>33</b>
3.1	Den organisatorischen Rahmen geben: Security Governance ....	33
3.1.1	Cybersecurity-Risikoanalyse .....	34
3.1.2	Risikobehandlung .....	37
3.1.3	Strategische Integration .....	38
3.1.4	Verbundene Disziplinen .....	38
3.1.5	Management Commitment .....	39
3.2	Den Status Quo feststellen: Security Assessments .....	39
3.2.1	Erfassung des aktuellen Status eines Unternehmens in Bezug auf Cybersecurity .....	40
3.2.2	Anpassung der Sicherheitsstrategie basierend auf Assessment-Ergebnissen .....	44
3.3	Technische Maßnahmen umsetzen: Integrationen .....	45
3.3.1	Konzepte zur Wahrung der Cybersecurity .....	45
3.3.2	Technische Umsetzung .....	47
3.4	Den Schutzraum bauen: Security Operations .....	53
3.4.1	Erweiterte Einblicke in die Kernkomponenten .....	54
3.4.2	Betriebsmodelle .....	58
3.4.3	Empfehlungen für den Einstieg .....	60
3.5	Zugriff steuern: Digital Identity .....	62
3.5.1	Identity Governance and Administration (IGA) .....	63
3.5.2	Access Management (AM) .....	68
3.5.3	Privileged Access Management (PAM) .....	70
3.5.4	Empfehlungen & Best Practices .....	71
3.6	Die Grenzen neu denken: Das „Zero Trust“-Konzept .....	72
3.6.1	Zero-Trust-Übersicht .....	73
3.6.2	Ausgewählte Einsatzgebiete von Zero Trust .....	77
3.6.3	Empfehlungen & Best Practices .....	78
Literatur	.....	79



---

<b>4 Managementperspektiven – Erfahrungen zu Cybersecurity aus der Managementpraxis</b> .....	83
4.1 Security Governance – Florian Jörgens, CISO .....	83
4.2 Cybersecurity bei Großveranstaltungen – Jorge Oliviera e Carmo, Head of Data Protection & Cybersecurity Risk .....	89
4.3 Digitale Identitäten – Wolfgang Schurr, Group Cyber Resilience Director Richemont .....	98
4.4 Rechtliche Aspekte – Olga Stepanova, Rechtsanwältin für Cybersecurity .....	100
4.5 Zero Trust – Max Imbiel, CISO .....	106
4.6 Künstliche Intelligenz – Lutz Jannausch, Microsoft .....	110

---

## Über die Autoren



**Mario Pufahl**, Diplomkaufmann, ist Group Chief Sales Officer und Mitglied des Leaderships der internationalen und auf Cybersecurity spezialisierten Beratungsfirma DIGITALL. Er ist Managementberater sowie Speaker, Dozent und langjähriger Springer-Autor. Sie können über LinkedIn Kontakt zu ihm aufnehmen: <https://www.linkedin.com/in/mariopufahl/>



**Patrick Paulsen**, Diplom-Wirtschaftsinformatiker, ist als führender Experte bei der DIGITALL für die Beratung und Betreuung von Kunden im Bereich Cybersecurity verantwortlich. Er entwickelt für diese maßgeschneiderte Cybersecurity-Lösungen und unterstützt Kunden dabei, die jeweils beste Option zu finden und umzusetzen. Zudem führt er Beratungen rund um die Themen Cybersecurity und AI durch.



**Paul Arndt**, Diplominformatiker, Certified Information System Security Professional (CISSP), beschäftigt sich seit 20 Jahren mit den Fragestellungen rund um das Thema Cybersecurity. Als Managing Partner hat er die auf Cybersecurity spezialisierte Beratungsfirma Eraneos Cybersecurity aufgebaut.



# Einleitung: Warum Cybersecurity Heute Unverzichtbar Ist

# 1

## Wie der Onlinekurs das Buch bereichert

Als Leser\*in dieses Buches können Sie kostenfrei auf den zugehörigen Onlinekurs zugreifen. Nutzen Sie dazu diesen Link ([sn.pub/95FWv4](https://sn.pub/95FWv4)).

Der Kurs ergänzt dieses Buch inhaltlich und liefert zudem Hilfestellungen für erfolgreiche Umsetzung in den Alltag.

## Fragen

- Was sind die Risiken für die Geschäftsleitung?
- Was sind die Top-Trends für Cybersecurity?
- Was sagen die Marktforscher und Strategieberater?

In einer zunehmend vernetzten Welt, in der digitale Technologien unser tägliches Leben durchdringen, gewinnt Cybersecurity eine entscheidende Bedeutung. Die rasante Digitalisierung bringt zwar zahlreiche Vorteile mit sich, birgt jedoch auch eine Vielzahl von Risiken und Herausforderungen.

Unternehmen, Organisationen und Individuen stehen vor der stetig wachsenden Bedrohung durch Cyberangriffe, die nicht nur ihre Sicherheit, sondern auch ihren Erfolg bedrohen können.

Angesichts der ständig zunehmenden Professionalität, Raffinesse und Kreativität der Angreifer ist es von entscheidender Bedeutung, dass Verantwortliche für Cybersecurity aber auch Geschäftsführer, Vorstände und Aufsichtsräte stets über die neuesten Trends und Entwicklungen in diesem Bereich informiert sind und entsprechend handeln können. Hackerangriffe haben bereits zu Insolvenzen bei Unternehmen geführt – prominentes Beispiel ist die Traditionsfahrradmarke Prophete [5]. Vor diesem Hintergrund der potenziellen substanziellen Folgen von