

1	Einleitung: Warum Cybersecurity Heute Unverzichtbar Ist	1
	Literatur	7
2	Das Cybersecurity-Kompetenzmodell – Basis Einer Ganzheitlichen Ausrichtung auf Cybergefahren	9
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
3	Umsetzung Des Cybersecurity-Kompetenzmodells	33
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

4	Managementperspektiven – Erfahrungen zu Cybersecurity	
	aus der Managementpraxis	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