

Inhaltsverzeichnis

1 Grundlagen	9
1.1 Einleitung.....	9
1.1.1 Der Cyberraum und seine Bedeutung	14
1.1.2 Grundlagen der Cybersecurity	16
1.1.3 Relevanz für Wirtschaftsprüfer	16
1.1.4 Zielsetzung und Aufbau des Leitfadens	19
1.2 Akteure im Cyberraum.....	21
1.2.1 Anwender (Fokus: Wirtschaftsprüfer und Steuerberater)	22
1.2.2 Angreifer und ihre Motivationen	23
1.3 Aktuelle Bedrohungen und Herausforderungen	39
1.3.1 Sensible Daten und die Cloud	39
1.3.2 Digitalisierung kritischer Infrastrukturen	40
1.3.3 Crime-as-a-Service / Hacktivismus	40
1.3.4 Einsatz von KI auf der Angreiferseite	41
1.4 Standards und Zertifizierungen.....	42
1.4.1 ISO/IEC-2700x-Reihe	43
1.4.2 IT-Grundschutz nach den BSI-Empfehlungen	45
1.4.3 BSI-C5-Testat.....	53
1.4.4 NIS-2-Richtlinie.....	57
1.5 Relevante Zertifikate für Fachkräfte.....	59
1.5.1 CISSP.....	59
1.5.2 T.I.S.P.....	61
2 Angriffe verhindern	63
2.1 Schwachstellen, Exploits und CVEs.....	64
2.1.1 Schwachstellen.....	65
2.1.2 Exploits.....	65
2.1.3 CVEs.....	66

2.2	Entwicklung eines Schutzkonzepts.....	67
2.2.1	Informationssicherheitsleitlinie	68
2.2.2	Der Schutzbedarf von Informationen	70
2.2.3	Der Informationssicherheitsbeauftragte.....	71
2.2.4	Layered Security und Defense in Depth.....	73
2.2.5	Architekturen und DMZ-Konzepte.....	81
2.3	Schlüsseltechnologien der Cybersecurity	83
2.3.1	Firewall und Proxy.....	83
2.3.2	Patchmanagement	85
2.3.3	Backup	87
3	Auf Angriffe vorbereitet sein.....	91
3.1	Business Continuity Management.....	92
3.1.1	Definition und Zielsetzung	93
3.1.2	Risiken und Szenarien	97
3.1.3	Krisenvorsorge und -bewältigung	101
3.2	Grundlagen der Vorbereitung und Evaluationsmöglichkeiten ...	115
3.2.1	White-, Black- und Grey-Box-Ansätze.....	116
3.2.2	Schwachstellenanalysen.....	116
3.2.3	Penetrationstests	118
3.2.4	Continuous Penetration Testing	119
3.2.5	Red Teaming	122
3.2.6	Zusammenfassung der technischen Evaluationen.....	123
3.3	Angriffserkennung und Incident Response.....	124
3.4	Intrusion Detection und Prevention Systems.....	127
3.5	Honeypots / Deception Networks	131
3.6	Incident-Response-Prozess.....	132
3.7	Anti-Malware und EDR/XDR.....	135
3.8	Security Operations Center (SOC) und MSSP	137
3.9	Awareness Trainings	139
3.9.1	Phishing-Simulationen	139
3.9.2	Zielgruppenorientierte Schulungen (z.B. für Software- entwickler, Vorstände, Finanzabteilungen)	142

3.10 Physische Sicherheitsprüfungen.....	144
3.11 Cyberversicherungen	145
4 Während des Angriffs.....	148
4.1 Sofortmaßnahmen und Erstreaktion.....	148
4.2 Kommunikations- und Krisenmanagement.....	149
4.3 Technische Incident Response.....	150
4.4 Koordination mit Behörden und Partnern.....	151
4.5 Sicherheit vs. Verfügbarkeit während der Krise.....	152
4.6 Dokumentation und Nachverfolgung.....	152
5 Nach einem Angriff.....	154
5.1 Schadensbewertung und Analyse.....	154
5.2 Wiederanlauf der Systeme.....	156
5.3 Lessons Learned und Optimierung.....	157
5.4 Prävention zukünftiger Angriffe.....	159
6 Fazit.....	161
Stichwortverzeichnis.....	164