

Inhaltsverzeichnis

	Vorwort	5
Teil A	Systeme vorbeugend schützen	7
1	Cyberattacken und Systemsicherheit	8
1.1	Wichtige Begriffe	8
1.2	Herausforderungen der Cyber Security	9
1.3	Informationsquellen	10
1.4	Good Practices	13
2	Bedrohungen analysieren	19
2.1	Risk Assessment	20
2.2	Cyber Threat Intelligence (CTI)	28
2.3	Weitere Analysetechniken	29
3	Schwachstellen erkennen	33
3.1	Indikatoren für Schwachstellen	33
3.2	Sicherheitsaudits	37
3.3	Sicherheitstests	40
4	Schwachstellen schliessen und Angreifer täuschen	45
4.1	Vorgaben im Unternehmen	45
4.2	Technische und organisatorische Massnahmen	49
4.3	Verfahren und Werkzeuge zur Irreführung von Angreifern	53
Teil B	Sicherheitsvorfälle erkennen und angemessen reagieren	57
5	Systeme während des Betriebs überwachen	58
5.1	Überwachung	58
5.2	Erkennung	62
5.3	Auswertung	69
5.4	Methoden	71
6	Sicherheitsvorfälle priorisieren und dokumentieren	74
6.1	Zum Umgang mit Incidents	74
6.2	Incidents melden und klassifizieren	75
6.3	Vorfälle priorisieren	76
6.4	Incidents behandeln	78
6.5	Incidents auswerten	79
6.6	Externe Unterstützung anfordern	79
6.7	Aus Incidents lernen	82
7	Sofortmassnahmen ergreifen	84
7.1	Incident Response	84
7.2	Technische Sofortmassnahmen ergreifen	87
7.3	Folgeschäden vermeiden	88
7.4	Beweise sichern	88
7.5	Angriffsspuren beseitigen, System wiederherstellen	90
7.6	Erkenntnisse auswerten	91
8	Wiederherstellung eines IT-Systems unterstützen	92
8.1	Business Continuity Management	92
8.2	Notfall- und Krisenmanagement	96
8.3	Business Continuity Management	98

Teil C	Sicherheitsvorfälle analysieren und bewältigen	101
9	Forensische Analyse	102
9.1	Grundlagen der IT-Forensik	102
9.2	Ablauf einer forensischen Ermittlung	104
9.3	Forensische Werkzeuge	109
9.4	Malware erkennen und richtig reagieren	110
10	Systemgrenzen, Schutzmassnahmen und Sicherheitsorganisation festlegen	117
10.1	Systeme abgrenzen und analysieren	117
10.2	Schutzmassnahmen festlegen	120
10.3	Sicherheitsorganisation definieren	123
11	Machbarkeit prüfen, Aufwand schätzen, Kosten planen und kontrollieren	126
11.1	Machbarkeit prüfen	126
11.2	Aufwand schätzen	130
11.3	Kostenplanung und -kalkulation	135
11.4	Kostenüberwachung und -reporting	138
Teil D	Anhang	141
	Antworten zu den Repetitionsfragen	142
	Weiterführende Literatur und Links	146
	Stichwortverzeichnis	148