

Inhaltsverzeichnis

Geleitwort	V
Abbildungsverzeichnis	IX
1 Einleitung – gefährliche neue Welt	1
1.1 Erkenntnis- oder Handlungsproblem?	4
1.2 Werkzeugkasten zum Aufklären digitaler Störfälle	6
1.3 Digitale Forensik – ein historischer Überblick	7
1.4 Die virtuelle Welt wird zum Tatort	11
1.5 Cybercrime as a Service	20
1.6 Historischer Exkurs: die Entdeckung der Spuren	25
1.7 Zum Mitnehmen: Fakten im Überblick	29
2 Digitale Forensik in der Wirtschaft – mehr als eine Compliance-Disziplin	31
2.1 Die Geheimnisse der Geheimdienste	32
2.2 DFIR als wichtiges Compliance-Instrument	37
2.3 Differierende Datenschutzkulturen	42
2.4 Der lange Arm ausländischer Behörden	45
2.5 DSGVO stellt neue Anforderungen an Compliance	46
2.6 Erweiterte Pflichten für KRITIS-Betreiber	50
2.7 Service-Teil: Gesetze, Institutionen und Organisationen	54
2.8 Zum Mitnehmen: Fakten im Überblick	70
3 Angriffsszenarien – das Spiel mit der Angst	71
3.1 Profiling im virtuellen Raum	72
3.2 Die Täter – vom Tüftler bis zum Cyberspion	77
A Cyberkriminelle – organisiertes Verbrechen im Netz	77
B Tüftler und Scriptkiddies – Genialität und Naivität in Bits und Bytes	85
C Hacktivisten – Rebellen des Digitalzeitalters	86
D Cyberspione und Cyberkrieger – die Hackerelite	88
3.3 Die Schwachstellen	93
A Einfallstor Mensch	94
B Einfallstor Technik	100
3.4 Zum Mitnehmen: Fakten im Überblick	107

4 Spurensuche – Ablauf einer digitalforensischen Untersuchung	109
4.1 Digitale Beweisaufnahme in sechs Schritten	111
4.2 Beste Vorbereitung: Digital Forensic Readiness	113
4.3 Der Notfallplan	115
4.4 Incident Response – ein Leitfaden	119
4.5 Forensic Data Analytics	135
4.6 eDiscovery	136
4.7 Threat Intelligence	138
4.8 Zum Mitnehmen: Fakten im Überblick	140
5 Die Zukunft von Digital Forensics und Incident Response	143
5.1 Wachsende digitale Angriffsfläche	144
5.2 Der Verteidigungsfall ist längst eingetreten	146
5.3 Smartere Schutzsysteme	151
5.4 Die Kehrseite der Cyberabwehr ist der Cyberangriff	153
5.5 Virtuelle Kriegsführung in neuer Dimension	153
5.6 KI-Entwicklung braucht klare Leitplanken	155
5.7 Cyberschutz muss ein Prozess werden	158
5.8 Zum Mitnehmen: Fakten im Überblick	159
Anhang	161
FAQ	161
Glossar	165
Quellenverzeichnis	171
Über den Autor	185