

Digitale Forensik

Praxiswissen Cybercrime für Manager

Von

Bodo Meseke

ERICH SCHMIDT VERLAG

Weitere Informationen zu diesem Titel finden Sie im Internet unter
ESV.info/978-3-503-18268-8

Gedrucktes Werk: ISBN 978-3-503-18267-1
eBook: 978-3-503-18268-8

Alle Rechte vorbehalten
© Erich Schmidt Verlag GmbH & Co. KG, Berlin 2019
www.ESV.info

Ergeben sich zwischen der Version dieses eBooks
und dem gedruckten Werk Abweichungen,
ist der Inhalt des gedruckten Werkes verbindlich.

Satz: L101 Agentur für Mediengestaltung und -produktion, Fürstenwalde

Geleitwort

2015 hatte jeder Internetnutzer im Durchschnitt 90 verschiedene Nutzerkennungen, 2020 sollen es 200 sein. Dann könnte es weltweit zudem bereits 30 Milliarden vernetzte Geräte geben – in Privathaushalten und Unternehmen. Auch die klassische Büro-IT wird vielfältiger: 66 Prozent der deutschen Unternehmen nutzen bereits Cloud-Dienste, nahezu alle Unternehmen mit mehr als 250 Mitarbeitern setzen mobile Geräte für ihre Teams ein. Wir leben mittlerweile in einer virtualisierten und vernetzten Cyberlandschaft und sind von einer Vielzahl digitaler Systeme und ihrer Vernetzung abhängig.

In dem Maße, in dem Virtualisierung und Vernetzung zunehmen, stärkere Abhängigkeiten entstehen, steigt auch die Bedrohung. Cyberangriffe gehören zur Tagesordnung von Unternehmen und staatlichen Behörden. Einfache Kriminelle, organisierte Gruppen, ausländische Nachrichtendienste – sie alle haben Interesse am Eindringen in Systeme, an der Entwendung von Daten, an der Erpressung, der Manipulation von Transaktionen oder der Störung von Betriebsabläufen. Jeder Verantwortliche in Wirtschaft und Staat muss sich auf diese Bedrohung einstellen.

Dabei hilft die Digitale Forensik: Forensische Methoden bringen Licht in die undurchsichtige IT-Welt. Sie helfen bei der Prävention, dem Entdecken von Angreifern, der Analyse gestohlener Daten, der Sicherung von Beweisen und zunehmend bei der Dokumentation der Compliance eines IT-Systems. Digitale Forensik ist ein Schlüssel, um komplexe Cyberlandschaften zu beherrschen.

Vor dem Hintergrund langjähriger praktischer Erfahrungen erklärt Bodo Meseke auf leicht verständliche Art die Anwendungen der Digitalen Forensik. Er stellt die Bedingungen für die Abwehr von Cyberangriffen ebenso dar wie die neuen Compliance-Anforderungen, die sich aus verstärkter Gesetzgebung zur IT-Sicherheit und zum Datenschutz ergeben. Sein Buch liefert Führungskräften eine alltagsnahe Orientierung beim Einsatz forensischer Methoden, ohne überbordende Fachtermini zu gebrauchen. Zugleich blickt es in die Zukunft, in der uns der Einsatz der künstlichen Intelligenz oder eine automatisierte Kriegsführung im Cyberraum vor neue Herausforderungen stellen wird.

April 2019

*Martin Schallbruch
Deputy Director
Digital Society Institute, ESMT Berlin*

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