ESV ERICH SCHMIDT VERLAG

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

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