Harlan Carvey; Windows Forensics Analysis Toolkit; Advanced Analysis Techniques for Windows 7; Waltham, MA (Syngress/Elsevier) 2012; 3. Auflage; 271 Seiten; US-$ 69,95 (Paperback)

Harlan Carvey; Windows Registry Forensics; Advanced Digital Forensic Analysis of the Windows Registry; Waltham, MA (Syngress/Elsevier) 2011; 248 Seiten; US-$ 69,95 (Paperback)

Lorenz Kuhlee, Victor Völzow; Computer Forensik Hacks; Köln (O'Reilly) 2012; 322 Seiten; € 34,90 (Paperback)

John Sammons; The Basics of Digital Forensics; The Primer for Getting Started in Digital Forensics; Waltham, MA (Syngress/Elsevier) 2012; 177 Seiten; US-$ 29,95 (Paperback)

Michael G. Solomon, K. Rudolph, Ed Tittel, Neil Broom, Diane Barrett; Computer Forensics JumpStart; Hoboken, NJ (John Wiley) 2011; 2. Auflage; 336 Seiten; US-$ 29,99 (Paperback)

Wer sich als Einsteiger rasch einen Überblick über die Digitalforensik verschaffen möchte, dem mag der schmale Band „The Basics of Digital Forensics" von John Sammons reichen. Das Buch liegt in englischer Sprache vor, daher ist das Kapitel über rechtliche Aspekte stark US-amerikanisch geprägt. Hierzulande wäre wichtiger, das BDSG samt Zulässigkeit der Auswertung von E-Mails, Chats und Konsorten zu diskutieren. Zielgruppe sind wirklich nur Einsteiger, schon Leser mit nur mittleren Vorkenntnissen greifen besser zur Fortgeschrittenen-Lektüre.

Mit den online verfügbaren Unterlagen ist das Werk grundsätzlich für einen Einführungskurs geeignet – sinnvoller erscheint es allerdings, eigene Unterlagen zu verwenden. Gelegentlich mischen sich Plattitüden in die Erklärungen, knapp erläutert er wichtige technische Begriffe. Die schwarz-weißen Grafiken zu Datenspeicherung und Schlupfspeicher überzeugen didaktisch nicht ganz. Erst beim dritten Hinsehen erkennt man, worauf es ankommt. Themen sind unter anderem Zertifizierung, Akkreditierung, verschiedene Rollen, Sicherheit und Risikomanagement, Standard-Vorgehensweisen sowie Qualitätssicherung.

Ein eigenes Kapitel ist dem Vorgehen bei der Beweissicherung gewidmet. Auf den 16 Seiten zu Artefakten geht es ausschließlich um Windows-Systeme – als Übersicht ganz gut, jedoch etwas unklar in der Gliederung. Carvey (siehe unten) fehlt als weiterführende Literatur. Weitere Kapitel betreffen die Spuren bei Internet und E-Mail, Netz- und Mobilgeräteforensik. Erstaunlich, dass diese Einführung sogar ein 22-seitiges Kapitel über Antiforensik enthält. Darin geht es um das Verbergen (Ver- und Entschlüsselung, Steganografie) sowie aktive Vernichten von Daten, nicht jedoch um Angriffe auf IT-forensische Werkzeuge. Als Herausforderungen der Digitalforensik werden angesprochen: wachsende Datenmengen und rechtliche Rahmenbedingungen. Dank Clouds und SSDs bleibt es spannend. Wer eine deutlich praxisorientiertere Einführung sucht, dem sei „Computer Forensics Jump Start" (Wiley) empfohlen.

Dagegen bietet „Computer Forensik Hacks" der beiden IT-Forensiker an der hessischen Polizeiakademie, Kuhlee und Völzow, knackigen Inhalt zu erschwinglichem Preis in handlichem Format. Mit Hacks sind hier Ideen, Methoden, Tipps und Tricks gemeint. Eine Sammlung von Kniffen quer durch die IT-Forensik von Praktikern für Praktiker hat bislang gefehlt. Dieser Schatz an Erfahrungswissen hält, was er verspricht: 100 kurze, praxiserprobte Rezepte in acht Kapiteln, vergnüglich präsentiert in lockerer Sprache. Linux und Windows dienen als Untersuchungsgegenstände sowie als Auswertungsumgebung. Soweit möglich, beschreiben die Autoren, wie es mit kostenloser Software funktioniert.

Themen sind unter anderem die Analyse und Wiederherstellung von Daten, die Auswertung von Artefakten, Incident Response (Angriffsvektoren und Aufklärung von Sicherheitsvorfällen) und als grundlegende Technik die Virtualisierung forensischer Images. Dabei geht es schnell zur Sache: Schon Hack #4 nutzt den direkten Speicherzugriff unter Firewire, um Hauptspeicher trotz Kennwortschutz zu sichern, Hack #5 zeigt einen Kalt-Boot-Angriff. Hack #24 schlägt gar vor, einen eigenen Parser für MFT-Einträge zu schreiben. So jagt dicht gedrängt ein Highlight das andere. Dieses Buch braucht jede IT-forensische Bibliothek. Selbst wer in IT-Forensik schult, kann hier noch etwas lernen.

Alle, die sich in Details zur digitalen forensischen Analyse von Windows-7-Systemen vertiefen möchten, sollten unbedingt zu Carveys englischsprachigem „Windows Forensic Analysis Toolkit" in der dritten Auflage greifen. Man benötigt außerdem die zweite, denn tatsächlich ergänzen sich beide Bücher. Die zweite Auflage konzentriert sich auf Windows XP und schaut nach vorne auf Windows 7, während die dritte gerade Windows 7 untersucht und auswertet. Jedem der Kapitel sind eine übersichtliche Gliederung und wichtige Begriffe vorangestellt, nachgestellt sind Zusammenfassung und Literaturangaben. Die acht Kapitel umfassen Konzepte zur Analyse, die unmittelbare Reaktion auf einen Sicherheitsvorfall, die Analyse des Artefakts Volume-Schattenkopien (VSCs), die von Dateien, die des Artefakts Windows Registry, Entdeckung von Malware, Zeitleisten- und Anwendungs-Analyse.

Bei diesen Konzepten sei beispielhaft das Stellen der richtigen Fragen, die Suche nach indirekten Spuren sowie nach der Abwesenheit von Artefakten genannt. Im Kapitel zu Schattenkopien sind verschiedene Auswertungsmethoden, die zuvor nur verstreut beschrieben waren, endlich an einer Stelle versammelt. Das Kapitel zur Windows Registry behandelt auf über 40 Seiten vor allem Neuerungen zu Windows 7. Dennoch dürfte man dazu ergänzend Carveys „Windows Registry Forensics" zur Hand haben wollen. Jedes Kapitel für sich ist studierenswert und bringt neue Einsichten – allerdings eignet sich Carvey nicht als Nachttischlektüre. Er schafft es immer wieder, anregende Fragen zu stellen, bislang übersehene Aspekte aufzudecken und Sachverhalte mit enormer Tiefe auszuloten. An diesem Buch führt zumindest für IT-Forensiker kein Weg vorbei. Das Warten auf die Analyse für Windows 8 hat begonnen.

ALEXANDER SIGEL

Klaus Leopold,
Siegfried Kaltenecker

Kanban in der IT

Eine Kultur der kontinuierlichen Verbesserung schaffen

München, Wien 2012
Carl Hanser
xv + 315 Seiten
34,90 €
ISBN 978-3-446-43059-4

Der Begriff Kanban besteht aus den japanischen Worten kan (Signal) und ban (Karte). Ursprünglich eingeführt bei Toyota, dient das Konzept der kontinuierlichen Verbesserung der Produktion. Sie erfolgt nach dem Pull-Prinzip: Eine nachgelagerte Produktionsstufe holt sich die Arbeit aus der vorgelagerten. Wann die Arbeit der jeweiligen Stufe fertig ist, stellen die Karten dar. Sie zeigen Leerlauf und Überlastung an und bieten eine unmittelbare Rückmeldung für eine Verbesserung der Produktion.

Kanban in der IT ist eine für die Softwareentwicklung adaptierte Variante des Prinzips: Einzelne Arbeitstypen wie Change Request oder Bugfix werden definiert sowie einzelne Stufen der Bearbeitung wie Analyse, Umsetzung und Test. Wichtig ist eine Begrenzung der Arbeit der einzelnen Schritte (Work in Progress). Das WIP-Limit sorgt dafür, das nicht zu viele Aufgaben gleichzeitig wahrgenommen werden. Die so entfallenden Kontextwechsel allein resultieren schon in erhöhter Produktivität.

Die hier angerissenen Prinzipien erläutern die Autoren im ersten Teil ausführlich. Viel Stoff, der gut verdaulich daherkommt und den Wunsch weckt, mit dem erworbenen Wissen gleich loszulegen. Aber zu schnell sollte der Leser nicht starten. Denn der Rest des Buchs ist mindestens ebenso wichtig. Da kommt im zweiten Teil „Change und Management“. Hier geht es um Veränderungen im Allgemeinen, die dadurch ausgelösten Emotionen und Konflikte, Unternehmenskultur, organisatorische und persönliche Änderungen. Stoff, der zunächst nichts mit dem ersten Teil des Buchs zu tun zu haben scheint. Und der lange nicht so spannend rüberkommt.

Erst im dritten Teil geht es um Details. Kanban schafft eine Kultur kontinuierlicher Veränderungen. Und es ist behutsam einzuführen, sonst besteht die Gefahr zu scheitern. Dies wird dem Leser im dritten Teil klar. Er zeigt auf, wie man die Einführung von Kanban sorgsam vorbereitet und umsetzt. Hierzu berichten die Autoren immer wieder von Fallbeispielen aus ihrer Praxis. Eine Botschaft lautet: Obwohl Kanban im Kern vom Entwicklerteam gelebt wird, müssen es alle wichtige Stakeholder tragen. Deshalb ist das Buch für alle, die an Softwareentwicklung teilhaben, ob Manager oder Entwickler, interessant. Vorausgesetzt, die Bereitschaft, neue Wege zu gehen, ist da.

MICHAEL MÜLLER