

# Inhaltsverzeichnis

<b>Einleitung</b>	<b>1</b>
Wer sollte dieses Buch lesen? .....	2
Was lernt man in diesem Buch? .....	4
Was lernt man in diesem Buch nicht? .....	4
Wie liest man dieses Buch? .....	5
Was ist neu in der 2. Auflage? .....	8
Was ist neu in der 3. Auflage? .....	8
Was ist neu in der 4. Auflage? .....	9
<b>1 Bedrohungssituation</b>	<b>11</b>
1.1 Bedrohung und Wahrscheinlichkeit .....	11
1.2 Risikoverteilung .....	12
1.3 Motivation der Täter .....	15
1.4 Innentäter vs. Außentäter .....	20
1.5 Bestätigung durch die Statistik? .....	23
1.6 Computerkriminalität .....	23
<b>2 Ablauf von Angriffen</b>	<b>29</b>
2.1 Typischer Angriffsverlauf .....	29
2.1.1 Footprinting .....	29
2.1.2 Port- und Protokollscan .....	30
2.1.3 Enumeration .....	30
2.1.4 Exploiting/Penetration .....	31
2.1.5 Hintertüren einrichten .....	31
2.1.6 Spuren verwischen .....	32
2.2 Beispiel eines Angriffs .....	32

<b>3</b>	<b>Incident Response als Grundlage der Computer-Forensik</b>	<b>41</b>
3.1	Der Incident-Response-Prozess . . . . .	41
3.2	Organisatorische Vorbereitungen . . . . .	42
3.3	Zusammensetzung des Response-Teams . . . . .	43
3.4	Incident Detection: Systemanomalien entdecken . . . . .	45
3.4.1	Vom Verdacht zum Beweis . . . . .	45
3.4.2	Netzseitige Hinweise . . . . .	46
3.4.3	Serverseitige Hinweise . . . . .	47
3.4.4	Intrusion-Detection-Systeme . . . . .	48
3.4.5	Externe Hinweise . . . . .	48
3.5	Incident Detection: Ein Vorfall wird gemeldet . . . . .	50
3.6	Sicherheitsvorfall oder Betriebsstörung? . . . . .	53
3.7	Wahl der Response-Strategie . . . . .	56
3.8	Reporting und Manöverkritik . . . . .	57
<b>4</b>	<b>Einführung in die Computer-Forensik</b>	<b>61</b>
4.1	Ziele einer Ermittlung . . . . .	61
4.2	Anforderungen an den Ermittlungsprozess . . . . .	62
4.3	Phasen der Ermittlung . . . . .	63
4.4	Das S-A-P-Modell . . . . .	64
4.5	Welche Erkenntnisse kann man gewinnen? . . . . .	66
4.6	Wie geht man korrekt mit Beweismitteln um? . . . . .	73
4.6.1	Juristische Bewertung der Beweissituation . . . . .	74
4.6.2	Datenschutz . . . . .	75
4.6.3	Welche Daten können erfasst werden? . . . . .	78
4.6.4	Bewertung der Beweisspuren . . . . .	78
4.6.5	Durchgeführte Aktionen dokumentieren . . . . .	79
4.6.6	Beweise dokumentieren . . . . .	80
4.6.7	Mögliche Fehler bei der Beweissammlung . . . . .	82
4.7	Flüchtige Daten sichern: Sofort speichern . . . . .	85
4.8	Speichermedien sichern: forensische Duplikation . . . . .	87
4.8.1	Wann ist eine forensische Duplikation sinnvoll? . . . . .	89
4.8.2	Geeignete Verfahren . . . . .	89

4.9	Was sollte alles sichergestellt werden? . . . . .	91
4.10	Erste Schritte an einem System für die Sicherstellung . . . . .	92
4.10.1	System läuft nicht (ist ausgeschaltet) . . . . .	92
4.10.2	System läuft (ist eingeschaltet) . . . . .	93
4.11	Untersuchungsergebnisse zusammenführen . . . . .	93
4.12	Häufige Fehler . . . . .	95
4.13	Anti-Forensik . . . . .	97
<b>5</b>	<b>Einführung in die Post-mortem-Analyse</b>	<b>101</b>
5.1	Was kann alles analysiert werden? . . . . .	101
5.2	Analyse des File Slack . . . . .	103
5.3	MAC-Time-Analysen . . . . .	107
5.4	NTFS-Streams . . . . .	111
5.5	Vistas TxF . . . . .	112
5.6	Vistas Volumen-Schattenkopien . . . . .	112
5.7	Auslagerungsdateien . . . . .	113
5.8	Versteckte Dateien . . . . .	114
5.9	Dateien oder Fragmente wiederherstellen . . . . .	119
5.10	Unbekannte Binärdateien analysieren . . . . .	120
5.11	Systemprotokolle . . . . .	131
5.12	Analyse von Netzwerkmitschnitten . . . . .	133
<b>6</b>	<b>Forensik- und Incident-Response-Toolkits im Überblick</b>	<b>135</b>
6.1	Grundsätzliches zum Tooleinsatz . . . . .	135
6.2	Sichere Untersuchungsumgebung . . . . .	137
6.3	F.I.R.E. . . . .	139
6.4	Knoppix Security Tools Distribution . . . . .	143
6.5	Helix . . . . .	143
6.6	ForensiX-CD . . . . .	149
6.7	EnCase . . . . .	151
6.8	dd . . . . .	156
6.9	Forensic Acquisition Utilities . . . . .	160
6.10	AccessData Forensic Toolkit . . . . .	161
6.11	The Coroner's Toolkit und TCTUtils . . . . .	164

6.12	The Sleuth Kit	165
6.13	Autopsy Forensic Browser	170
6.14	Eigene Toolkits für Unix und Windows erstellen	174
6.14.1	F.R.E.D.	175
6.14.2	Incident Response Collection Report (IRCR)	175
6.14.3	Windows Forensic Toolchest (WFT)	177
6.14.4	Live View	179
<b>7</b>	<b>Forensische Analyse im Detail</b>	<b>181</b>
7.1	Forensische Analyse unter Unix	181
7.1.1	Die flüchtigen Daten speichern	181
7.1.2	Forensische Duplikation	187
7.1.3	Manuelle P.m.-Analyse der Images	195
7.1.4	P.m.-Analyse der Images mit Autopsy	202
7.1.5	Dateiwiederherstellung mit unrm und lazarus	208
7.1.6	Weitere hilfreiche Tools	209
7.2	Forensische Analyse unter Windows	212
7.2.1	Die flüchtigen Daten speichern	213
7.2.2	Analyse des Hauptspeichers	216
7.2.3	Forensische Duplikation	222
7.2.4	Manuelle P.m.-Analyse der Images	227
7.2.5	P.m.-Analyse der Images mit dem AccessData FTK	228
7.2.6	P.m.-Analyse der Images mit EnCase	233
7.2.7	P.m.-Analyse der Images mit X-Ways Forensics	236
7.2.8	Weitere hilfreiche Tools	240
7.3	Forensische Analyse von mobilen Geräten	255
7.3.1	Was ist von Interesse bei mobilen Geräten?	256
7.3.2	Welche Informationen sind auf der SIM-Karte von Interesse?	257
7.3.3	Grundsätzlicher Ablauf der Sicherung von mobilen Geräten	258
7.3.4	Software für die forensische Analyse von mobilen Geräten im Überblick	260
7.4	Forensische Analyse von Routern	269

<b>8</b>	<b>Empfehlungen für den Schadensfall</b>	<b>273</b>
8.1	Logbuch . . . . .	273
8.2	Den Einbruch erkennen . . . . .	275
8.3	Tätigkeiten nach festgestelltem Einbruch . . . . .	276
8.4	Nächste Schritte . . . . .	280
<b>9</b>	<b>Backtracing</b>	<b>281</b>
9.1	IP-Adressen überprüfen . . . . .	281
9.1.1	Ursprüngliche Quelle . . . . .	281
9.1.2	IP-Adressen, die nicht weiterhelfen . . . . .	282
9.1.3	Private Adressen . . . . .	282
9.1.4	Weitere IANA-Adressen . . . . .	283
9.1.5	Augenscheinlich falsche Adressen . . . . .	284
9.2	Spoof Detection . . . . .	284
9.2.1	Traceroute Hopcount . . . . .	284
9.3	Routen validieren . . . . .	287
9.4	Nslookup . . . . .	291
9.5	Whois . . . . .	293
9.6	E-Mail-Header . . . . .	294
<b>10</b>	<b>Einbeziehung der Behörden</b>	<b>299</b>
10.1	Organisatorische Vorarbeit . . . . .	299
10.2	Strafrechtliches Vorgehen . . . . .	301
10.2.1	Inanspruchnahme des Verursachers . . . . .	301
10.2.2	Möglichkeiten der Anzeigeerstattung . . . . .	301
10.2.3	Einflussmöglichkeiten auf das Strafverfahren . . . . .	304
10.3	Zivilrechtliches Vorgehen . . . . .	305
10.4	Darstellung in der Öffentlichkeit . . . . .	306
10.5	Die Beweissituation bei der privaten Ermittlung . . . . .	307
10.6	Fazit . . . . .	311
<b>Anhang</b>		
	<b>Tool-Überblick</b>	<b>313</b>
	<b>Literaturempfehlungen</b>	<b>319</b>
	<b>Stichwortverzeichnis</b>	<b>321</b>