

Inhaltsverzeichnis

Einleitung	1
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 6. Auflage?	8
Was ist neu in der 5. Auflage?	8
Was ist neu in der 4. Auflage?	9
Was ist neu in der 3. Auflage?	9
Was ist neu in der 2. Auflage?	9
 1 Bedrohungssituation	 11
1.1 Bedrohung und Wahrscheinlichkeit	11
1.2 Risikoverteilung	12
1.3 Motivation der Täter	16
1.4 Innentäter vs. Außentäter	21
1.5 Bestätigung durch die Statistik?	25
1.6 Computerkriminalität	26
 2 Ablauf von Angriffen	 33
2.1 Typischer Angriffsverlauf	33
2.2 Beispiel eines Angriffs	36

3	Incident Response als Grundlage der Computer-Forensik	45
3.1	Der Incident-Response-Prozess	45
3.2	Organisatorische Vorbereitungen	46
3.3	Zusammensetzung des Response-Teams	47
3.4	Incident Detection: Systemanomalien entdecken	49
3.5	Incident Detection: Ein Vorfall wird gemeldet	54
3.6	Sicherheitsvorfall oder Betriebsstörung?	57
3.7	Wahl der Response-Strategie	60
3.8	Reporting und Manöverkritik	61
4	Einführung in die Computer-Forensik	65
4.1	Ziele einer Ermittlung	65
4.2	Anforderungen an den Ermittlungsprozess	66
4.3	Phasen der Ermittlung	67
4.4	Das S-A-P-Modell	68
4.5	Welche Erkenntnisse kann man gewinnen?	70
4.6	Wie geht man korrekt mit Beweismitteln um?	77
4.7	Flüchtige Daten sichern: Sofort speichern	88
4.8	Speichermedien sichern: Forensische Duplikation	91
4.9	Was sollte alles sichergestellt werden?	94
4.10	Erste Schritte an einem System für die Sicherstellung	96
4.11	Untersuchungsergebnisse zusammenführen	98
4.12	Häufige Fehler	100
4.13	Anti-Forensik	102
5	Einführung in die Post-mortem-Analyse	107
5.1	Was kann alles analysiert werden?	107
5.2	Analyse des File Slack	109
5.3	Timeline-Analysen	113
5.4	NTFS-Streams	119
5.5	NTFS TxF	120
5.6	NTFS-Volumen-Schattenkopien	122
5.7	Windows-Registry	126
5.8	Windows UserAssist Keys	130
5.9	Windows Prefetch-Dateien	131
5.10	Auslagerungsdateien	134

5.11	Versteckte Dateien	135
5.12	Dateien oder Fragmente wiederherstellen	139
5.13	Unbekannte Binärdateien analysieren	140
5.14	Systemprotokolle	153
5.15	Analyse von Netzwerkmitschnitten	155
6	Forensik- und Incident-Response-Toolkits im Überblick	157
6.1	Grundsätzliches zum Tooleinsatz	157
6.2	Sichere Untersuchungsumgebung	159
6.3	F.I.R.E.	161
6.4	Knoppix Security Tools Distribution	165
6.5	Helix	166
6.6	ForensiX-CD	171
6.7	C.A.I.N.E. und WinTaylor	173
6.8	DEFT und DEFT-Extra	176
6.9	EnCase	178
6.10	dd	182
6.11	Forensic Acquisition Utilities	187
6.12	AccessData Forensic Toolkit	188
6.13	The Coroner's Toolkit und TCTUtils	191
6.14	The Sleuth Kit	192
6.15	Autopsy Forensic Browser	198
6.16	Eigene Toolkits für Unix und Windows erstellen	203
7	Forensische Analyse im Detail	209
7.1	Forensische Analyse unter Unix	209
7.2	Forensische Analyse unter Windows	240
7.3	Forensische Analyse von mobilen Geräten	292
7.4	Forensische Analyse von Routern	308
8	Empfehlungen für den Schadensfall	311
8.1	Logbuch	311
8.2	Den Einbruch erkennen	313
8.3	Tätigkeiten nach festgestelltem Einbruch	314
8.4	Nächste Schritte	318

9	Backtracing	319
9.1	IP-Adressen überprüfen	319
9.2	Spoof Detection	322
9.3	Routen validieren	325
9.4	Nslookup	329
9.5	Whois	330
9.6	E-Mail-Header	332
10	Einbeziehung der Behörden	335
10.1	Organisatorische Vorarbeit	335
10.2	Strafrechtliches Vorgehen	337
10.3	Zivilrechtliches Vorgehen	341
10.4	Darstellung in der Öffentlichkeit	342
10.5	Die Beweissituation bei der privaten Ermittlung	343
10.6	Fazit	347
	Anhang	349
A	Tool-Überblick	351
B	C.A.I.N.E.-Tools	359
C	DEFT-Tools	367
	Literaturempfehlungen	373
	Index	375