

# Inhaltsverzeichnis

<b>1</b>	<b>Nine-Eleven, Snowden und die Folgen .....</b>	<b>17</b>
1.1	Mit dem Smartphone sicher und anonym? .....	19
1.2	Anonym im Internet? .....	20
1.2.1	Anonymer bzw. verschlüsselter Mailverkehr.....	32
1.3	Situation aus Sicht der Unternehmen .....	38
1.3.1	Was macht mich angreifbar? .....	38
1.3.2	Wie gehe ich mit diesen Gefahren um?.....	40
1.3.3	Welche Sicherheitsarchitektur ist angemessen für mein Unternehmen? .....	41
	<b>Teil I: Tools – Werkzeuge für Angriff und Verteidigung .....</b>	<b>43</b>
<b>2</b>	<b>Keylogger – Spionage par excellence.....</b>	<b>45</b>
2.1	Logkeys.....	46
2.2	Elite Keylogger .....	47
2.3	Ardamax Keylogger .....	48
2.4	Stealth Recorder Pro .....	49
2.5	Advanced Keylogger .....	50
2.6	Hardware-Keylogger .....	51
2.7	Abwehr – generelle Tipps .....	52
<b>3</b>	<b>Passwortknacker: Wo ein Wille ist, ist auch ein Weg .....</b>	<b>55</b>
3.1	CMOSPwd .....	55
3.2	Hydra .....	56
3.3	Medusa .....	58
3.4	Ncrack (Nmap-Suite) .....	60
3.5	VNCRack .....	61
3.6	PWDUMP (in unterschiedlichen Versionen bis PWDUMP 7.1) .....	62
3.7	John the Ripper .....	63
3.8	oclHashcat-plus .....	64
3.9	Ophcrack.....	65

3.10	SAMInside.....	66
3.11	Cain & Abel .....	67
3.12	L0phtcrack .....	68
3.13	Distributed Password Recovery .....	69
3.14	Offline NT Password & Registry Editor .....	70
3.15	PW-Inspector (Hydra-Suite) .....	70
3.16	Abwehr – generelle Tipps .....	71
4	An den Toren rütteln: Portscanner & Co.....	73
4.1	Nmap .....	75
4.2	Lanspy .....	77
4.3	Essential NetTools.....	78
4.4	Winfingerprint .....	79
4.5	Xprobe2 .....	80
4.6	p0f .....	82
4.7	Abwehr – generelle Tipps .....	84
5	Proxy & Socks.....	85
5.1	ProxyCap.....	86
5.2	Proxy Finder .....	87
5.3	Abwehr – generelle Tipps .....	88
6	Remote Access Tools (RAT) – Anleitung für Zombie-Macher .....	89
6.1	Atelier Web Remote Commander .....	89
6.2	Poison Ivy .....	90
6.3	Turkojan .....	91
6.4	Optix Pro .....	92
6.5	Cybergate Excel.....	93
6.6	Abwehr – generelle Tipps .....	94
7	Rootkits – Malware stealthen .....	95
7.1	Oddyssee_Rootkit.....	96
7.2	Hacker_Defender.....	97
7.3	TDSS alias TDL-4 .....	98
7.4	Abwehr – generelle Tipps .....	99
8	Security-/Vulnerability-Scanner .....	101
8.1	X-NetStat Professional .....	101
8.2	GFI LANguard N.S.S. ....	102

8.3	Nessus .....	103
8.4	Open Vulnerability Assessment System/OpenVAS .....	104
8.5	Nikto2 .....	106
8.6	Abwehr – generelle Tipps .....	107
9	Sniffer: Die Schnüffler im Netzwerk.....	109
9.1	dsniff (dsniff-Suite) .....	110
9.2	mailsnarf (dsniff-Suite).....	111
9.3	urlsnarf (dsniff-Suite) .....	113
9.4	arp spoof (dsniff-Suite) .....	114
9.5	PHoss.....	115
9.6	Driftnet.....	116
9.7	Ettercap/Ettercap NG.....	117
9.8	tcpdump.....	118
9.9	Wireshark.....	119
9.10	Abwehr – generelle Tipps .....	120
10	Sonstige Hackertools.....	121
10.1	Metasploit Framework (MSF) .....	121
10.2	USB DUMPER 2.....	122
10.3	USB Switchblade/7zBlade.....	123
10.4	Net Tools 5.0 .....	124
10.5	Troll Downloader .....	125
10.6	H.O.I.C – High Orbit Ion Cannon.....	126
10.7	Phoenix Exploit's Kit.....	127
10.8	fEvicol .....	127
10.9	0x333shadow .....	128
10.10	Logcleaner-NG.....	129
10.11	NakedBind .....	131
10.12	Ncat (Nmap-Suite) .....	131
10.13	GNU MAC Changer (macchanger).....	133
10.14	Volatility Framework.....	134
10.15	Abwehr – generelle Tipps .....	135
11	Wireless Hacking .....	137
11.1	Kismet-Newcore .....	138
11.2	Aircrack-NG (Aircrack-NG-Suite) .....	139
11.3	Aireplay-NG (Aircrack-NG-Suite) .....	140
11.4	Airodump-NG (Aircrack-NG-Suite) .....	141

11.5	Airbase-NG (Aircrack-NG-Suite) .....	142
11.6	coWPatty.....	143
11.7	Reaver.....	144
11.8	Wash (Reaver-Suite).....	146
11.9	Pyrit .....	147
11.10	MDK3 .....	148
11.11	Vistumbler .....	149
11.12	Abwehr – generelle Tipps .....	150
Teil II: Angriffsszenarien und Abwehrmechanismen .....		151
12	Die Angreifer und ihre Motive .....	153
12.1	Die Motive.....	153
12.1.1	Rache .....	153
12.1.2	Geltungssucht .....	154
12.1.3	Furcht .....	154
12.1.4	Materielle Interessen .....	154
12.1.5	Neugier.....	155
12.2	Die Angreifer .....	156
12.2.1	Hacker.....	156
12.2.2	Skriptkiddies .....	157
12.2.3	IT-Professionals .....	158
12.2.4	Normalanwender und PC-Freaks .....	159
13	Szenario I: Datenklau vor Ort .....	161
13.1	Zugriff auf Windows-PCs .....	161
13.1.1	Erkunden von Sicherheitsmechanismen .....	161
13.1.2	Überwinden der CMOS-Hürde .....	162
13.1.3	Das Admin-Konto erobern .....	164
13.2	Zugriff auf Linux-Rechner .....	173
13.2.1	Starten von Linux im Single-User-Mode.....	173
13.2.2	Starten von einem Linux-Boot-Medium .....	177
13.2.3	Einbinden der zu kompromittierenden Festplatte in ein Fremdsystem .....	178
13.3	Abwehrmaßnahmen gegen einen physischen Angriff von außen .....	179
13.4	Zwei-Faktoren-Authentifizierung .....	181
13.4.1	iKey 2032 von SafeNet.....	182

13.4.2	Chipdrive Smartcard Office .....	185
13.4.3	Security Suite .....	189
14	Szenario II: Der PC ist verwandt.....	193
14.1	Software-Keylogger.....	195
14.1.1	Ausforschen von Sicherheitseinstellungen.....	195
14.1.2	Festlegen des Überwachungsumfangs .....	195
14.1.3	Installation des Keyloggers .....	196
14.1.4	Sichten, Bewerten und Ausnutzen der gewonnenen Daten.....	199
14.1.5	Die Audiowanze .....	199
14.2	Big Brother im Büro .....	201
14.3	Abwehrmaßnahmen gegen Keylogger & Co. ....	203
15	Szenario III: Spurensucher im Netz .....	211
15.1	Google-Hacking.....	212
15.1.1	Angriffe .....	212
15.1.2	Abwehrmaßnahmen.....	222
15.2	Portscanning, Fingerprinting und Enumeration .....	225
15.2.1	Portscanning.....	225
15.2.2	Fingerprinting und Enumeration .....	241
15.2.3	Security-Scanner.....	245
15.3	Abwehrmaßnahmen gegen Portscanner & Co. ....	251
16	Szenario IV: Web Attack.....	259
16.1	Defacements .....	259
16.2	XSS-Angriffe.....	260
16.3	Angriff der Würmer .....	261
16.4	DoS-, DDoS- und andere Attacken .....	261
16.5	Ultima Ratio – Social Engineering oder Brute Force? .....	270
16.6	Sicherheitslücken systematisch erforschen.....	273
16.6.1	AccessDiver .....	273
16.6.2	Spuren verwischen mit ProxyHunter .....	275
16.6.3	Passwortlisten konfigurieren.....	279
16.6.4	Wortlisten im Eigenbau .....	281
16.6.5	Websecurity-Scanner: Paros .....	283
16.6.6	Websecurity-Scanner: WVS .....	286
16.6.7	Websecurity-Scanner: Wikto .....	289
16.7	Abwehrmöglichkeiten gegen Webattacks .....	296
16.7.1	.htaccess schützt vor unbefugtem Zugriff.....	296

<b>17</b>	<b>Szenario V: WLAN-Attacke .....</b>	<b>299</b>
17.1	Aufspüren von Funknetzen .....	301
17.1.1	Hardwareausstattung für Wardriving .....	301
17.1.2	Vistumbler für Windows .....	303
17.1.3	Kismet-Newcore für Linux.....	307
17.2	Kartografierung von Funknetzen .....	322
17.2.1	Kartografierung von Funknetzen mit Google Maps oder OpenStreetMap .....	323
17.2.2	Kartografierung von Funknetzen mit Google Earth und Vistumbler .....	326
17.2.3	Kartografierung von Funknetzen mit Google Earth und Kismet- Newcore .....	329
17.3	Angriffe auf Funknetze.....	331
17.3.1	Zugriff auf ein offenes WLAN .....	332
17.3.2	Zugriff auf ein WLAN, dessen Hotspot keine SSID sendet .....	333
17.3.3	Zugriff auf ein WLAN, das keinen DHCP-Dienst anbietet .....	336
17.3.4	Zugriff auf ein mit MAC-Filter gesichertes WLAN .....	340
17.3.5	Zugriff auf ein WEP-verschlüsseltes WLAN.....	345
17.3.6	Zugriff auf ein WPA2-verschlüsseltes WLAN .....	359
17.3.7	Zugriff auf ein WPA2-verschlüsseltes WLAN durch die WPS- Schwäche .....	372
17.3.8	Zugriff auf ein WPA2-verschlüsseltes WLAN durch Softwareschwächen.....	379
17.3.9	WLAN, mon amour – Freu(n)de durch Funkwellen .....	381
17.4	Sicherheitsmaßnahmen bei Wireless LAN .....	391
<b>18</b>	<b>Szenario VI: Malware-Attacke aus dem Internet .....</b>	<b>395</b>
18.1	Angriffe via E-Mail .....	396
18.1.1	Absendeadresse fälschen .....	396
18.1.2	Phishen nach Aufmerksamkeit.....	400
18.1.3	Der Payload oder Malware aus dem Baukasten.....	404
18.1.4	Massenattacken und Spamschleudern .....	409
18.1.5	Office-Attacken .....	411
18.1.6	Kampf der Firewall .....	414
18.2	Rootkits .....	420
18.2.1	Test-Rootkit Unreal .....	422
18.2.2	AFX-Rootkit .....	424
18.3	Die Infektion.....	427
18.3.1	Experiment 1: <i>rechnung.pdf.exe</i> .....	427
18.3.2	Experiment 2: <i>bild-07.jpg.com</i> .....	430

18.4	Drive-by-Downloads .....	433
18.5	Schutz vor (un)bekannten Schädlingen aus dem Netz .....	439
18.5.1	Mailprogramm und Webbrowser absichern .....	441
18.5.2	Pflicht: Malware- und Antivirens Scanner .....	442
18.5.3	Malware-Abwehr mit Sandboxie .....	445
18.5.4	Allzweckwaffe Behavior Blocker & HIPS .....	447
19	Szenario VII: Netzwerkarbyten: Wenn der Feind innen hackt .....	451
19.1	Der Feind im eigenen Netzwerk .....	451
19.2	Zugriff auf das LAN .....	452
19.3	Passives Mitlesen im LAN: Sniffing .....	454
19.3.1	Tcpdump .....	456
19.3.2	Wireshark .....	460
19.3.3	Ettercap NG .....	463
19.3.4	DSniff-Suite .....	474
19.3.5	Driftnet .....	484
19.3.6	Pof .....	485
19.3.7	ARPSpoof .....	487
19.4	Scanning: »Full Contact« mit dem LAN .....	491
19.4.1	Xprobe2 .....	491
19.4.2	Nmap .....	495
19.4.3	Open Vulnerability Assessment System/OpenVAS .....	502
19.5	Der Tritt vors Schienbein: Exploits .....	513
19.5.1	wunderbar_emporium .....	514
19.5.2	2009-lsa.zip/Samba < 3.0.20 heap overflow .....	520
19.5.3	Metasploit Framework .....	524
19.6	Hurra, ich bin root – und nun? .....	553
19.7	Windows-Rechner kontrollieren .....	553
19.7.1	Integration von Schadsoftware .....	559
19.8	Linux unter Kontrolle: Rootkits installieren .....	562
19.8.1	evilbs .....	564
19.8.2	Mood-NT .....	568
19.8.3	eNYeLKM .....	572
19.9	Linux unter Kontrolle: Spuren verwischen mit Logfile- Cleaner .....	578
19.10	Linux unter Kontrolle: Keylogger .....	583
19.11	Linux unter Kontrolle: Password-Cracking .....	585
19.11.1	John the Ripper .....	586
19.11.2	ophcrack .....	586
19.11.3	Medusa .....	588

19.11.4	Hydra .....	590
19.12	Schutz vor Scannern, Exploits, Sniffen & Co. ....	593
Teil III: Prävention und Prophylaxe .....		597
20	Private Networking .....	599
20.1	Sicherheitsstatus mit MBSA überprüfen .....	599
20.2	Überflüssige Dienste .....	605
20.3	Vor »Dienstschluss« Abhängigkeiten überprüfen .....	607
20.4	Alle Dienste mit dem Process Explorer im Blick.....	608
20.5	Externer Security-Check tut Not .....	610
20.6	Malware-Check .....	611
20.7	Risiko: Mehrbenutzer-PCs und Netzwerksharing .....	624
20.8	Schadensbegrenzung: Intrusion Detection & Prevention .....	632
21	Company Networking.....	637
21.1	Basiselemente zur Unternehmenssicherheit .....	642
21.2	Teilbereich Infrastruktur und Organisation .....	643
21.3	Teilbereich Personal.....	646
21.4	Teilbereich Technik .....	649
Stichwortverzeichnis .....		655