

Inhaltsverzeichnis

1	Snowden, NSA & Co.	21
1.1	Kryptohandys und andere Tarnkappen	24
1.2	Anonym im Internet?	28
1.2.1	Anonymer bzw. verschlüsselter Mailverkehr	43
1.3	Situation aus Sicht der Unternehmen	52
1.3.1	Was macht mich angreifbar?	53
1.3.2	Datenerpresser – wie Ransomware auch Unternehmen schädigt	55
1.3.3	Was man gegen IT-Risiken noch tun kann	57
1.3.4	Welche Sicherheitsarchitektur ist angemessen für mein Unternehmen?	58
	Teil I: Tools: Werkzeuge für Angriff und Verteidigung	61
2	Keylogger: Spionage par excellence	63
2.1	Logkeys	64
2.2	Elite Keylogger	65
2.3	Ardamax Keylogger	66
2.4	Stealth Recorder Pro	67
2.5	Advanced Keylogger	68
2.6	Hardware-Keylogger	69
2.7	Abwehr – generelle Tipps	70
3	Passwortknacker: Wo ein Wille ist, ist auch ein Weg	73
3.1	CMOSPwd	74
3.2	Hydra	74
3.3	Medusa	76
3.4	Ncrack (Nmap-Suite)	78
3.5	VNCRack	79
3.6	PWDUMP (in unterschiedlichen Versionen bis PWDUMP 7.1)	80
3.7	John the Ripper	80
3.8	Hashcat	82

3.9	Ophcrack.....	84
3.10	SAMInside.....	85
3.11	Cain & Abel	85
3.12	L0phtcrack	86
3.13	Distributed Password Recovery	87
3.14	Offline NT Password & Registry Editor	88
3.15	PW-Inspector (Hydra-Suite)	88
3.16	Abwehr – generelle Tipps	89
4	An den Toren rütteln: Portscanner und Co.	91
4.1	Nmap	93
4.2	Lanspy	94
4.3	Essential NetTools.....	95
4.4	Winfingerprint.....	96
4.5	Xprobe2	97
4.6	p0f	99
4.7	Abwehr – generelle Tipps	102
5	Proxy und Socks	103
5.1	ProxyCap.....	104
5.2	Proxy Finder	105
5.3	Abwehr – generelle Tipps	106
6	Remote Access Tools (RAT): Anleitung für Zombie-Macher	107
6.1	Atelier Web Remote Commander	107
6.2	Poison Ivy	108
6.3	Turkojan.....	109
6.4	Optix Pro	110
6.5	Cybergate Excel.....	111
6.6	Abwehr – generelle Tipps	112
7	Rootkits: Malware stealthen	113
7.1	Oddysee_Rootkit.....	114
7.2	Hacker_Defender.....	115
7.3	TDSS alias TDL-4	116
7.4	Abwehr – generelle Tipps	117

8	Security-/Vulnerability-Scanner.....	119
8.1	X-NetStat Professional	119
8.2	GFI LANguard N.S.S.	120
8.3	Nessus	121
8.4	Open Vulnerability Assessment System/OpenVAS	122
8.5	Nikto2	124
8.6	Abwehr – generelle Tipps	125
9	Sniffer: Die Schnüffler im Netzwerk.....	127
9.1	dsniff (dsniff-Suite)	128
9.2	mailsnarf (dsniff-Suite).....	129
9.3	urlsnarf (dsniff-Suite)	131
9.4	arp spoof (dsniff-Suite)	132
9.5	PHoss.....	133
9.6	Driftnet.....	134
9.7	Ettercap/Ettercap NG.....	135
9.8	Bettercap	136
9.9	tcpdump.....	138
9.10	Wireshark.....	139
9.11	Abwehr – generelle Tipps	140
10	Sonstige Hackertools.....	141
10.1	Metasploit Framework (MSF)	141
10.2	USB DUMPER 2.....	143
10.3	USB Switchblade/7zBlade.....	144
10.4	Net Tools 5.0	145
10.5	Troll Downloader	146
10.6	H.O.I.C – High Orbit Ion Cannon.....	146
10.7	Phoenix Exploit's Kit.....	147
10.8	fEvicol	148
10.9	0x333shadow	148
10.10	Logcleaner-NG.....	150
10.11	NakedBind	151
10.12	Ncat (Nmap-Suite)	152
10.13	GNU MAC Changer (macchanger).....	153
10.14	Volatility Framework.....	154
10.15	Abwehr – generelle Tipps	155

11	Wireless Hacking	157
11.1	Kismet.....	158
11.2	Aircrack-NG (Aircrack-NG-Suite)	159
11.3	Aireplay-NG (Aircrack-NG-Suite)	160
11.4	Airodump-NG (Aircrack-NG-Suite).....	161
11.5	Airbase-NG (Aircrack-NG-Suite)	162
11.6	coWPAtty.....	163
11.7	Reaver.....	164
11.8	Wash (Reaver-Suite)	166
11.9	Pyrit	167
11.10	MDK3	168
11.11	Vistumbler	169
11.12	Abwehr – generelle Tipps	171
Teil II: Angriffsszenarien und Abwehrmechanismen		173
12	Die Angreifer und ihre Motive	175
12.1	Die Motive.....	175
12.1.1	Rache	175
12.1.2	Geltungssucht	176
12.1.3	Furcht	176
12.1.4	Materielle Interessen	176
12.1.5	Neugier.....	177
12.2	Die Angreifer	178
12.2.1	Hacker	178
12.2.2	Skriptkiddies	179
12.2.3	IT-Professionals	180
12.2.4	Normalanwender und PC-Freaks	181
13	Szenario I: Datenklau vor Ort	183
13.1	Zugriff auf Windows-PCs	183
13.1.1	Erkunden von Sicherheitsmechanismen	183
13.1.2	Überwinden der CMOS-Hürde	184
13.1.3	Das Admin-Konto erobern	186
13.2	Zugriff auf Linux-Rechner	195
13.2.1	Starten von Linux im Single-User-Mode.....	195
13.2.2	Starten von einem Linux-Boot-Medium	200
13.2.3	Einbinden der zu kompromittierenden Festplatte in ein Fremdsystem	201

13.3	Abwehrmaßnahmen gegen einen physischen Angriff von außen	202
13.4	Zwei-Faktoren-Authentifizierung	204
13.4.1	iKey 2032 von SafeNet.....	204
13.4.2	Chipdrive Smartcard Office	207
13.4.3	Security Suite	210
14	Szenario II: Der PC ist verwandt.....	213
14.1	Software-Keylogger.....	215
14.1.1	Ausforschen von Sicherheitseinstellungen.....	215
14.1.2	Festlegen des Überwachungsumfangs	215
14.1.3	Installation des Keyloggers	216
14.1.4	Sichten, Bewerten und Ausnutzen der gewonnenen Daten.....	219
14.1.5	Die Audiowanze	219
14.2	Big Brother im Büro	221
14.3	Abwehrmaßnahmen gegen Keylogger und Co.....	223
15	Szenario III: Spurensucher im Netz	231
15.1	Google-Hacking.....	232
15.1.1	Angriffe.....	232
15.1.2	Abwehrmaßnahmen.....	241
15.2	Portscanning, Fingerprinting und Enumeration	244
15.2.1	Portscanning.....	244
15.2.2	Fingerprinting und Enumeration	260
15.2.3	Security-Scanner.....	264
15.3	Abwehrmaßnahmen gegen Portscanner & Co.	270
16	Szenario IV: Web Attack.....	277
16.1	Defacements	277
16.2	XSS-Angriffe.....	278
16.3	Angriff der Würmer	279
16.4	DoS-, DDoS- und andere Attacken	279
16.5	Ultima Ratio: Social Engineering oder Brute Force?.....	288
16.6	Sicherheitslücken systematisch erforschen.....	291
16.6.1	AccessDiver	291
16.6.2	Spuren verwischen mit ProxyHunter.....	293
16.6.3	Passwortlisten konfigurieren.....	297
16.6.4	Wortlisten im Eigenbau	299
16.6.5	Websecurity-Scanner: Paros	301

16.6.6	Websecurity-Scanner: WVS	304
16.6.7	Websecurity-Scanner: Wikto	307
16.7	Abwehrmöglichkeiten gegen Webattacks	313
16.7.1	.htaccess schützt vor unbefugtem Zugriff	314
17	Szenario V: WLAN-Attacke	317
17.1	Aufspüren von Funknetzen	319
17.1.1	Hardwareausstattung für Wardriving	319
17.1.2	Vistumbler für Windows	321
17.1.3	Kismet Wireless für Linux	324
17.2	Kartografierung von Funknetzen	338
17.2.1	Kartografierung von Funknetzen mit Google Maps oder OpenStreetMap	339
17.2.2	Kartografierung von Funknetzen mit Google Earth und Vistumbler	343
17.2.3	Kartografierung von Funknetzen mit Google Earth und Kismet.....	345
17.3	Angriffe auf Funknetze	347
17.3.1	Zugriff auf ein offenes WLAN	348
17.3.2	Zugriff auf ein WLAN, dessen Hotspot keine SSID sendet	349
17.3.3	Zugriff auf ein WLAN, das keinen DHCP-Dienst anbietet	352
17.3.4	Zugriff auf ein mit MAC-Filter gesichertes WLAN	357
17.3.5	Zugriff auf ein WEP-verschlüsseltes WLAN	362
17.3.6	Zugriff auf ein WPA2-verschlüsseltes WLAN	376
17.3.7	Zugriff auf ein WPA2-verschlüsseltes WLAN durch die WPS- Schwäche	389
17.3.8	Zugriff auf ein WPA2-verschlüsseltes WLAN durch Softwareschwächen.....	395
17.3.9	WLAN, mon amour – Freu(n)de durch Funkwellen	397
17.4	Sicherheitsmaßnahmen bei Wireless LAN	407
18	Szenario VI: Malware-Attacke aus dem Internet	411
18.1	Angriffe via E-Mail	412
18.1.1	Absendeadresse fälschen	412
18.1.2	Phishen nach Aufmerksamkeit.....	416
18.1.3	Der Payload oder Malware aus dem Baukasten.....	420
18.1.4	Massenattacken und Spamschleudern	425
18.1.5	Office-Attacken	427
18.1.6	Kampf der Firewall	430
18.2	Rootkits	436
18.2.1	Test-Rootkit Unreal	438

18.2.2	AFX-Rootkit	440
18.3	Die Infektion.....	443
18.3.1	Experiment 1: <i>rechnung.pdf.exe</i>	443
18.3.2	Experiment 2: <i>bild-07_jpg.com</i>	446
18.4	Drive-by-Downloads	449
18.5	Schutz vor (un)bekannten Schädlingen aus dem Netz	454
18.5.1	Mailprogramm und Webbrowser absichern	457
18.5.2	Pflicht: Malware- und Virens Scanner.....	458
18.5.3	Malware-Abwehr mit Sandboxie.....	461
18.5.4	Allzweckwaffe Behavior Blocker & HIPS	463
19	Szenario VII: Netzwerkarbyten: Wenn der Feind innen hackt	467
19.1	Der Feind im eigenen Netzwerk.....	467
19.2	Zugriff auf das LAN	468
19.3	Passives Mitlesen im LAN: Sniffing.....	470
19.3.1	Tcpdump	472
19.3.2	Wireshark	476
19.3.3	Ettercap NG.....	479
19.3.4	DSniff-Suite	490
19.3.5	Driftnet	500
19.3.6	Pof.....	501
19.3.7	ARPSpoof.....	503
19.4	Scanning: »Full Contact« mit dem LAN.....	507
19.4.1	Xprobe2.....	507
19.4.2	Nmap.....	511
19.4.3	Open Vulnerability Assessment System/OpenVAS	518
19.5	Der Tritt vors Schienbein: Exploits	535
19.5.1	wunderbar_emporium	536
19.5.2	2009-lsa.zip/Samba < 3.0.20 heap overflow	542
19.5.3	Metasploit Framework.....	546
19.6	Hurra, ich bin root – und nun?	575
19.7	Windows-Rechner kontrollieren.....	575
19.7.1	Integration von Schadsoftware.....	581
19.8	Linux unter Kontrolle: Rootkits installieren	584
19.8.1	evilbs.....	586
19.8.2	Mood-NT.....	590
19.8.3	eNYeLKM	594
19.9	Linux unter Kontrolle: Spuren verwischen mit Logfile-Cleaner.....	600
19.10	Linux unter Kontrolle: Keylogger.....	605

19.11	Linux unter Kontrolle: Passwort-Cracking	606
19.11.1	John the Ripper	607
19.11.2	ophcrack.....	608
19.11.3	Medusa	610
19.11.4	Hydra.....	612
19.12	Schutz vor Scannern, Exploits, Sniffen & Co.	614
Teil III: Prävention und Prophylaxe		617
20	Private Networking	619
20.1	Sicherheitsstatus mit MBSA überprüfen	619
20.2	Überflüssige Dienste	625
20.3	Vor »Dienstschluss« Abhängigkeiten überprüfen	627
20.4	Alle Dienste mit dem Process Explorer im Blick.....	628
20.5	Externer Security-Check tut not	630
20.6	Malware-Check	631
20.7	Risiko: Mehrbenutzer-PCs und Netzwerksharing	644
20.8	Schadensbegrenzung: Intrusion Detection & Prevention	652
21	Company Networking.....	657
21.1	Basiselemente zur Unternehmenssicherheit	663
21.2	Teilbereich Infrastruktur und Organisation	663
21.3	Teilbereich Personal.....	666
21.4	Teilbereich Technik	669
Glossar		673
Stichwortverzeichnis		681