Inhaltsverzeichnis

Teil I: Einleitung 29

Kapitel 1 Warum dieses Buch geschrieben wurde ... 31

1.1 Der Bedarf an Datensicherheit 33
1.2 Die Wurzel allen Übels 35
1.2.1 Fehlkonfiguration des Netzwerks oder von Hosts 35
1.2.2 Mängel bei Betriebssystemen und Anwendungen 37
1.2.3 Unzureichende Qualitätskontrolle durch die Hersteller 40
1.2.4 Fehlende Qualifikation von Fachleuten 44
1.3 Warum Fortbildung im Bereich Sicherheit wichtig ist 46
1.3.1 Die Wirtschaft 46
1.3.2 Schulen und Universitäten 48
1.3.3 Behörden 48
1.4 Aus der Sicht des Betrachters 49

Kapitel 2 Wie Sie dieses Buch verwenden... 53

2.1 Dieses Buch verwenden? Puh...! 54
2.1.1 Die allgemeine Struktur dieses Buches 54
2.2 Ansätze für das Arbeiten mit diesem Buch 55
2.2.1 Grundlegendes zur Datensicherheit lernen 55
2.2.2 Eine bestehende Netzwerkumgebung sichern 56
2.2.3 Verwendung des Buches zu Forschungszwecken 56
2.3 Der Aufbau des Buches 57
2.3.1 Teil I: »Einleitung« 57
2.3.2 Teil II: »Sicherheitskonzepte« 57
2.3.3 Teil III: »Das 1 x 1 des Hackens« 57
2.3.4 Teil IV: »Aus dem Nähkästchen der Verteidiger« 58
2.3.5 Teil V: »Virtuelle Massenvernichtungswaffen« 58
2.3.6 Teil VI: »Plattformen und Sicherheit« 58
2.3.7 Teil VII: »Die Fäden laufen zusammen« 59
2.4 Die Grenzen dieses Buches 59
2.4.1 Aktualität 59

2.4.2 Nutzen
2.5 Was Sie noch über den »Neuen Hacker's Guide« wissen sollten 60
2.6 Der Inhalt der CD-ROM 60
2.6.1 FTP-Clients 61
2.6.2 Packer 61
2.6.3 Viewer und Reader 62
2.7 Programmiersprachen 63
2.8 Fazit 64
65

Teil II: Sicherheitskonzepte 67

Kapitel 3 Der Fahrplan zur Absicherung Ihres Unternehmens 69
3.1 Offensive vs. defensive Modelle 70
3.2 Einschätzung Ihrer momentanen Situation 71
3.3 Werte ermitteln 72
3.4 Werte schützen 73
3.4.1 Sicherheitslücken erkennen und entfernen 74
3.4.2 Standards implementieren 75
3.4.3 Richtlinien und Prozesse entwickeln und implementieren 76
3.5 IR 76
3.6 Benutzer und Administratoren schulen 79
3.7 ...und daraus nun ein Päckchen schnüren 80
3.8 Fazit 81

Kapitel 4 Eine kurze Einführung in TCP/IP 83
4.1 Was ist TCP/IP? 84
4.1.1 Das OSI-Referenzmodell 84
4.1.2 Die Geschichte von TCP/IP 87
4.1.3 Die RFCs 87
4.1.4 TCP/IP-Implementierungen 88
4.1.5 Wie funktioniert TCP/IP? 89
4.2 Die einzelnen Protokolle 90
4.2.1 Protokolle auf Netzwerkebene 97
4.2.2 Protokolle auf der Anwendungsebene

4.3 IPSec, IPv6, VPNs und was die Zukunft sonst noch bringt
4.4 Fazit

Kapitel 5 Hacker und Cracker

5.1 Hacker und Cracker – wo ist der Unterschied?
5.2 Der Werkzeugkasten
5.2.1 Reconnaissance
5.3 Exploits und die SANS-Hitliste
5.3.1 Exploits
5.3.2 Die Top Ten von SANS
5.4 Fazit

Kapitel 6 Das Internet heute: Eine Welt im Kriegszustand

6.1 Hacker, Cracker und andere Bösewichte
6.2 Regierungen im Krieg
6.2.1 Kann das Internet zur Spionage genutzt werden?
6.2.2 Die Bedrohung kommt näher…
6.2.3 Wer hält die Karten in der Hand?
6.2.4 Kann Amerika seine nationale Dateninfrastruktur schützen
6.2.5 Wie kann ein Informationsangriff aussehen?
6.3 Die Situation bei den staatlichen Stellen
6.3.1 DISN: Das Netzwerk der Verteidigungsdatensysteme
6.3.2 Die Navy und die NASA
6.3.3 Die Pentagon-Attacken
6.3.4 Andere geknackte Sites der US-Regierung
6.3.5 Sicherheitsmaßnahmen der Regierung
6.3.6 NIPC: Das National Infrastructure Protection Center
6.3.7 Fazit zu den Sicherheitslücken bei behördlichen Systemen
6.4 Die Situation in der Privatwirtschaft
6.4.1 Der Fall StarWave oder: Beutezug im Cyberspace
6.4.2 Das Kreditkartenproblem nimmt zu
6.4.3 Die Tendenzen
6.5 Eine Warnung
6.6 Fazit
6.6.1 Internetressourcen zum Informationskrieg
6.6.2 Bücher zum Informationskrieg

Teil III: Das 1 x 1 des Hackens 161

Kapitel 7 Spoofing 163

7.1 Was ist »Spoofing«? 164
7.2 Grundprinzipien der Internetsicherheit 164
7.2.1 Authentifizierungsmethoden 164
7.2.2 RHOSTS 165
7.3 Wie Spoofing funktioniert 167
7.3.1 Der schnelle Weg zum erfolgreichen Spoofing... 170
7.3.2 ... und wie man sich dann ein bequemeres Sicherheitsloch öffnet 171
7.3.3 Wer kann ein Opfer von Spoofing werden? 171
7.3.4 Wie häufig tritt Spoofing auf? 172
7.3.5 Programme für Spoofing und Session Hijacking 172
7.4 IP-Spoofing: Onlineressourcen 174
7.5 Wie kann ich Spoofing-Angriffe verhindern? 175
7.6 Ausgefallene Varianten 176
7.6.1 ARP-Spoofing 176
7.6.2 DNS-Spoofing 177
7.7 Fazit 179

Kapitel 8 Anonym bleiben 181

8.1 Stufen der Preisgabe 182
8.1.1 Menschliche Spione 182
8.2 Wie das Surfen im Web die Privatsphäre gefährdet 185
8.2.1 Internetstruktur und Privatsphäre 185
8.2.2 Wie Daten auf Servern gespeichert werden 185
8.2.3 *finger* 186
8.2.4 MasterPlan 190
8.2.5 Was es sonst noch so gibt... 191
8.3 Browsersicherheit 192
8.3.1 Die IP-Adresse und den Browsercache ausspionieren 192
8.3.2 Cookies 194
8.3.3 Werbebanner und Webwanzen 198
8.4 E-Mail und Newsgroups 200
8.4.1 Google Groups (früher DejaNews) 203
8.4.2 Der WHOIS-Dienst 204

8.5 Eine Warnung
8.5.1 Internetressourcen
8.5.2 Artikel, Vorträge und relevante Websites

Kapitel 9 Schluss mit den Ammenmärchen

9.1 Wann treten Angriffe auf?
9.1.1 Warum man Ziel eines Angriffs wird
9.1.2 Einwahlverbindung vs. Standleitung
9.1.3 Welche Betriebssysteme anfällig sind
9.1.4 Meine Firewall wird die Schweine schon aufhalten'
9.2 Welche Arten von Angreifern es gibt
9.2.1 Skriptkids: Die größte Bedrohung?
9.2.2 Black Hats: Die Bösen
9.2.3 White Hats: Die Guten
9.3 Welche Betriebssysteme Cracker benutzen
9.3.1 Windows
9.3.2 Linux/NetBSD/FreeBSD
9.3.3 OpenBSD
9.4 Gibt es »typische« Attacken?
9.4.1 DoS-Angriffe
9.4.2 Viren, Trojaner sowie bösartige Skripten und Webinhalte
9.4.3 Tagging oder: Die Kunst, eine Website zu verunstalten
9.4.4 Interne Attacken
9.5 Wer sind die Opfer?
9.5.1 Privatpersonen und kleine Unternehmen
9.5.2 Große Unternehmen und Global Players
9.5.3 Behörden und militärische Einrichtungen
9.5.4 Kreditinstitute
9.6 Welche Motive hinter den Angriffen stehen
9.6.1 Eitelkeit – der elitäre Ansatz
9.6.2 Niederträchtigkeit und Zerstörungswut
9.6.3 Politische Meinungsäußerungen
9.6.4 Bereicherung
9.6.5 Wissen
9.6.6 Einbruch für den Einbruch
9.7 Fazit

Teil IV: Aus dem Nähkästchen der Verteidiger 241

Kapitel 10 Firewalls 243

10.1 Was ist eine Firewall? 244
10.2 Weitere Eigenschaften verschiedener Firewall-Produkte 245
10.3 Firewalls sind nicht narrensicher 247
10.4 Firewalls unter die Haube geschaut 249
10.4.1 Firewalls, die auf Paketfiltern basieren 249
10.4.2 SPF-basierte Firewalls 251
10.4.3 Proxybasierte Firewalls 251
10.5 Firewalls und ihre Tücken 253
10.6 Firewall-Appliances 255
10.7 Firewalls implementieren 256
10.7.1 Topologie-, Anwendungs- und Protokollanforderungen bestimmen 258
10.7.2 Vertrauensverhältnisse und Kommunikationswege in der Organisation analysieren 260
10.7.3 Firewall-Produkte erproben und auswählen 260
10.7.4 Firewalls implementieren und testen 262
10.8 Beispiele für das Versagen von Firewalls 263
10.8.1 Das Oje-wo-ist-denn-mein-Webserver-hin-Problem 263
10.8.2 Mit SSH Regelsätze umgehen 265
10.9 Eine Firewall mit dem Firewall Toolkit bauen 266
10.10 Kommerzielle Firewalls 269
10.10.1 BorderManager 269
10.10.2 FireBOX 269
10.10.3 Firewall-1 269
10.10.4 FireWall Server 270
10.10.5 Gauntlet Internet Firewall 270
10.10.6 GNAT Box Firewall 270
10.10.7 Guardian 270
10.10.8 NetScreen 271
10.10.9 PIX Firewall 271
10.10.10 Raptor Firewall 271
10.10.11 SideWinder 271
10.10.12 Sonicwall 272

10.11 Fazit 272
10.11.1 Bücher und Veröffentlichungen 272
10.11.2 Internetressourcen 273

Kapitel 11 Scanner – Tools zur Erkennung von Sicherheitslücken 275

11.1 Die Geschichte der Scanner 276
11.2 Wie Scanner funktionieren 278
11.3 Auswahlkriterien für Scanner 280
11.4 Grundlegende Mängel 282
11.5 Empfehlenswerte Scanner 283
11.5.1 Axent NetRecon 283
11.5.2 ISS Internet Scanner 284
11.5.3 Network Associates Cybercop Scanner 285
11.5.4 Das Open-Source-Projekt Nessus 285
11.5.5 Whisker 286
11.6 Weitere Scanner 286
11.6.1 BindView HackerShield 287
11.6.2 Cisco NetSonar 287
11.6.3 SAINT 287
11.6.4 SARA 287
11.6.5 Webtrends Security Analyzer 287
11.7 Fazit 288

Kapitel 12 Intrusion-Detection-Systeme 289

12.1 Intrusion Detection: Eine Einführung 290
12.1.1 Wer IDS-Systeme verwenden sollte 292
12.2 NIDS 292
12.3 HIDS-Systeme 294
12.4 Auswahlkriterien für IDS-Systeme 295
12.4.1 Allgemeine Kriterien 296
12.5 SNORT und andere Open-Source-Lösungen 298
12.6 IDS-Produkte 299
12.6.1 Anzen Flight Jacket 299
12.6.2 Axent/Symantec NetProwler/Intruder Alert 300
12.6.3 Cisco Secure IDS 300
12.6.4 CyberSafe Centrax IDS 301
12.6.5 Enterasys Dragon IDS 301

12.6.6 ISS RealSecure 301
12.6.7 Network ICE BlackICE Sentry 302
12.6.8 NFR Security Intrusion Detection System 302
12.7 Fazit 303
12.8 Lektüre zur Vertiefung 303
12.8.1 Internetressourcen 303
12.8.2 Bücher 303

Kapitel 13 Protokollierungs- und Auditing-Tools 305

13.1 Warum überhaupt protokollieren? 306
13.2 Protokolle aus Crackersicht 306
13.3 Wie man eine Protokollierungsstrategie entwickelt 307
13.4 Tools zur Netzwerküberwachung und zur Datensammlung 310
13.4.1 SWATCH (The System Watcher) 310
13.4.2 Watcher 311
13.4.3 lsof (List Open Files) 311
13.4.4 Private-I 312
13.4.5 WebSense 312
13.4.6 Win-Log Version 1 313
13.4.7 NOCOL/NetConsole Version 4 313
13.5 Tools zur Analyse von Protokolldateien 313
13.5.1 NestWatch 313
13.5.2 NetTracker 314
13.5.3 LogSurfer 314
13.5.4 WebTrends für Firewalls und VPNs 314
13.5.5 Analog 315
13.6 Spezielle Protokollierungsprogramme 316
13.6.1 Courtney 316
13.6.2 Gabriel 317
13.7 Fazit 317

Kapitel 14 Kennwortknacker 319

14.1 Wie man Kennwörter knackt: Eine Einführung 320
14.1.1 Das Einmaleins der Kennwortverschlüsselung 322
14.2 Wie Kennwörter geknackt werden 329
14.3 Lösungen 330
14.4 Kennwortknacker für Windows NT 330
14.4.1 l0phtCrack 331

14.4.2	John The Ripper	332
14.4.3	NTCrack	332
14.4.4	Notwendige Zubehörprogramme	333
14.5	Kennwortknacker für UNIX	334
14.5.1	Kennwortschutz unter UNIX	334
14.5.2	Crack	335
14.5.3	John The Ripper	337
14.5.4	CrackerJack	337
14.5.5	PaceCrack95	338
14.5.6	Star Cracker	338
14.5.7	Merlin	339
14.6	Wie man Kennwörter für Cisco-Systeme und Anwendungen aller Art knackt	340
14.6.1	Kennwörter unter Cisco IOS knacken	341
14.6.2	Kommerzielle Kennwortknacker für Anwendungen	341
14.6.3	ZipCrack	342
14.6.4	Glide	343
14.6.5	AMI Decode	343
14.6.6	PGPCrack	343
14.7	Weitere Ressourcen	344
14.7.1	Onlineressourcen	345
14.7.2	Publikationen und Artikel	346
14.8	Fazit	346

Kapitel 15 Sniffer 349

15.1	Sicherheitsrisiko Sniffer	350
15.1.1	Datenverkehr in LANs	351
15.1.2	Transport und Auslieferung von Paketen	352
15.2	Wie groß ist das Risiko, dem man durch Sniffer ausgesetzt ist?	352
15.3	Welche Sniffer-Attacken hat es schon gegeben?	352
15.4	Welche Daten fangen Sniffer ab?	354
15.5	Wo Sniffer vorkommen...	355
15.6	... und wo man sie bekommt	356
15.6.1	Kommerzielle Lösungen	356
15.6.2	Kostenlos erhältliche Sniffer	362
15.7	Wie man Sniffer-Angriffe zurückschlägt	365
15.7.1	Sniffer entdecken und beseitigen	365

15.7.2 Sichere Topologie 367
15.7.3 Verschlüsselte Arbeitssitzungen 368
15.8 Fazit 369
15.9 Weitere Ressourcen 369

Teil V: Virtuelle Massenvernichtungswaffen 371

Kapitel 16 DoS-Angriffe 373

16.1 Was sind DoS-Angriffe? 374
16.1.1 Wie funktionieren DoS-Angriffe? 375
16.2 DoS-Angriffe im richtigen Leben 378
16.2.1 Mailbomben 379
16.2.2 Protokollbasierte Angriffe 384
16.3 DoS-Angriffe: Eine Übersicht 385
16.3.1 DoS-Angriffe 385
16.3.2 Historisch bedeutsame DoS-Angriffe 387
16.3.3 Verteilte DoS-Angriffe 393
16.4 Fazit 396
16.5 Weiterführende Informationen 396

Kapitel 17 Viren und Würmer 399

17.1 Viren und Würmer verstehen 400
17.1.1 Was ist ein Computervirus? 401
17.1.2 Was ist ein Computerwurm? 403
17.2 Anfällige Objekte 403
17.3 Wer schreibt Viren und warum? 404
17.3.1 Wie werden Viren erzeugt? 406
17.3.2 Was bedeutet eigentlich »In the Wild«? 407
17.3.3 Wie arbeiten Viren? 408
17.3.4 Boot-Sektor-Viren 410
17.3.5 Dateiviren (parasitische Viren) 412
17.3.6 Mehrteilige Viren 413
17.3.7 Makroviren 413
17.3.8 Skriptviren 414
17.3.9 Memetische Viren 414
17.3.10 Wie arbeiten Würmer? 416

17.3.11 Viruseigenschaften 418
17.4 Anti-Virus-Utilities 420
17.5 Die Zukunft der Virus-Malware 423
17.6 Veröffentlichungen und Websites 424
17.7 Zusammenfassung 428

Kapitel 18 Trojanische Pferde 431

18.1 Was ist ein Trojaner? 432
18.1.1 Ursprung 432
18.1.2 Definitionen 433
18.1.3 Ich habe es nicht so gemeint 433
18.1.4 Klassifizierungen 436
18.2 Woher kommen Trojaner? 445
18.3 Wie oft werden Trojaner wirklich entdeckt? 446
18.4 Wie groß ist die Bedrohung durch Trojaner? 447
18.5 Wie erkennt man einen Trojaner? 448
18.5.1 MD5 451
18.5.2 Tripwire 452
18.5.3 TAMU 454
18.5.4 Hobgoblin 454
18.5.5 Auf anderen Plattformen 454
18.6 Informationsquellen 455
18.7 Zusammenfassung 456

Teil VI: Plattformen und Sicherheit 457

Kapitel 19 Microsoft 459

19.1 MS-DOS 460
19.1.1 IBM-kompatible Systeme 460
19.1.2 Tastatur-Recorder 461
19.1.3 Zugriffskontrollsoftware für DOS 462
19.1.4 Websites mit DOS-Sicherheitstools 464
19.2 Windows for Workgroups, Windows 9x und Windows Me 464
19.2.1 Das Passwortlisten-(PWL-)Passwortschema 464
19.2.2 Zusammenfassung für DOS, Windows for Workgroups, Windows 9x und Windows Me 466

19.3	Windows NT	466
19.3.1	Allgemeine Schwachstellen in Windows NT	467
19.3.2	Andere wichtige Schwachstellen mit geringerer Bedeutung	469
19.4	Interne Sicherheit von Windows NT	470
19.4.1	Interne Sicherheit im Allgemeinen	470
19.4.2	Eine gute interne Sicherheit aufbauen	471
19.4.3	Ein Tipp für die Ersteinrichtung eines NT-Servers	472
19.4.4	Zusammenfassung zu Windows NT	472
19.5	Windows 2000	472
19.5.1	Bessere Sicherheitsfunktionen	473
19.5.2	Übersicht über die verteilte Sicherheit in Windows 2000	474
19.5.3	Allgemeine Schwachstellen in Windows 2000	475
19.5.4	Zusammenfassung zu Windows 2000	477
19.6	Schwachstellen in Microsoft-Anwendungen	478
19.6.1	Microsoft Internet Explorer	478
19.6.2	Microsoft Exchange Server	481
19.6.3	IIS (Internet Information Server)	485
19.6.4	Tools	488
19.6.5	Zugriffskontrollsoftware	496
19.6.6	Gute Online-Informationsquellen	502
19.6.7	Bücher zum Thema Sicherheit für Windows 2000 und Windows NT	504
19.7	Zusammenfassung	505
Kapitel 20	**UNIX**	507
20.1	Eine kleine Reise in die Geschichte von UNIX	508
20.2	UNIX-Distributionen klassifizieren	511
20.2.1	Unreife Distributionen	511
20.2.2	Mainstream-Distributionen	511
20.2.3	Wie sicher ist Open Source?	514
20.2.4	Gehärtete Betriebssysteme	517
20.2.5	Multilevel Trusted Systems	521
20.3	Sicherheitsaspekte bei der Auswahl einer Distribution	527
20.4	Sicherheitsrisiken von UNIX	528
20.4.1	Benutzer-Accounts	530
20.4.2	Sicherheit des Dateisystems	534
20.4.3	Dateisystem – Risiken	538

20.4.4	Dateisystem – Gegenmaßnahmen	541
20.4.5	Das set-uid-Problem	542
20.5	set-uid-Programme knacken	547
20.5.1	Nützliche Tools für Experimente	550
20.6	Rootkits und Verteidigungsmaßnahmen	553
20.6.1	Rootkits – Gegenmaßnahmen	554
20.6.2	Kernel-Rootkits	556
20.6.3	Schutz gegen Kernel-Angriffe	559
20.7	Netzwerksicherheit auf dem Host	560
20.7.1	Netzwerkdienste: Allzweck gegen zweckdienlich	560
20.7.2	Netzwerkdienste – Risiken	561
20.7.3	Netzwerkdienste sichern	564
20.7.4	Netzwerkdienste deaktivieren	564
20.7.5	Ein Wort zu privilegierten Ports	566
20.7.6	Schutz gegen Angriffe, die Dienste kidnappen	568
20.7.7	Gefälschte Serverdienste erkennen	568
20.8	Telnet	569
20.8.1	TELNET-Protokoll – Risiken	570
20.8.2	Telnet sichern	573
20.9	Ein unverzichtbares Tool: Secure Shell	573
20.9.1	Die SSH-Protokolle	574
20.9.2	SSH-Server	574
20.9.3	SSH-Clients	575
20.9.4	Informationsquellen zum Thema SSH	576
20.10	FTP	577
20.10.1	FTP – Risiken	577
20.10.2	FTP sichern	579
20.11	Die r-Dienste	580
20.11.1	r-Dienste – Risiken	580
20.11.2	Gegenmaßnahmen	581
20.12	REXEC	581
20.12.1	REXEC – Risiken	581
20.12.2	REXEC sichern	582
20.13	SMTP	582
20.13.1	SMTP – Risiken	582
20.13.2	SMTP sichern	583
20.14	DNS	584

20.14.1	DNS – Risiken	585
20.14.2	DNS sichern	587
20.15	Finger	588
20.16	SNMP	589
20.16.1	SNMP – Risiken	589
20.16.2	SNMP sichern	590
20.17	Network File System	590
20.17.1	NFS – Risiken	591
20.17.2	NFS sichern	591
20.18	Vorbehalte gegen chroot	592
20.19	Je besser man den Dämon kennt...	593
20.20	Bewerten Sie Ihre UNIX-Systeme in Hinblick auf ihre Schwachstellen	595
20.20.1	Host-Lockdown	598
20.20.2	Host-Hardening-Tools	599
20.21	Zusammenfassung	605
Kapitel 21	**NetWare**	607
21.1	Das Betriebssystem – die nackten Tatsachen	608
21.2	Die großen Drei	609
21.2.1	Serverumgebung	609
21.2.2	Physikalische Sicherheit	611
21.2.3	Eine unsichere Konsole sichern	612
21.2.4	Clientumgebung	618
21.2.5	Novell Directory Services (NDS)	619
21.2.6	Die besten NDS-Praktiken verstehen und anwenden	623
21.2.7	NDS-Audit-Tools	624
21.2.8	Kommerzielle Produkte für sichere Remotekontrolle	626
21.2.9	Nützliche Freeware	627
21.2.10	Bücher zum Thema	628
21.3	Zusammenfassung	628
Kapitel 22	**Cisco-Router und -Switches**	631
22.1	Infrastrukturgeräte – Probleme	632
22.2	Über IOS-Revisionen auf dem Laufenden bleiben	633
22.3	Cisco-Router sichern und konfigurieren	634
22.3.1	Login-Punkte sichern	635

22.3.2	Administratoren verantwortlich machen	636
22.3.3	Unnötige Dienste deaktivieren	637
22.4	Überlegungen zum Thema Netzwerkmanagement	638
22.4.1	Protokollierung zentralisieren	638
22.4.2	Überlegungen zum Thema Passwortaufbewahrung	639
22.4.3	Zeitsynchronisierung	640
22.4.4	Überlegungen zum Thema SNMP	641
22.4.5	Spoofing und andere Paket-Spielchen verhindern	642
22.4.6	Ausgangsfilter	642
22.4.7	Dumme Paket-Spielchen stoppen	643
22.5	Zusammenfassung	644
22.6	Informationsquellen	644
Kapitel 23	**Macintosh**	647
23.1	Der Macintosh als Server	648
23.1.1	WebSTAR Server Suite bei der U.S. Army	649
23.1.2	Hotline für gemeinsame Ideen und Dateien	649
23.2	Schwachstellen auf der Macintosh-Plattform	650
23.2.1	Schwachstelle AtEase-Zugriff	650
23.3	Dateifreigaben und Sicherheit	656
23.3.1	Dateisicherheit unter MacOS 9	657
23.4	Servermanagement und Sicherheit	657
23.4.1	EtherPeek von WildPackets, Inc.	658
23.4.2	InterMapper 3.0 von Dartmouth Software Development	658
23.4.3	MacPork 3.0	659
23.4.4	MacRadius von Cyno	660
23.4.5	Network Security Guard	661
23.4.6	Oyabun Tools	662
23.4.7	Silo 1.0.4	662
23.4.8	Timbuktu Pro 2000	662
23.5	Interne Sicherheit	663
23.5.1	BootLogger	663
23.5.2	DiskLocker	663
23.5.3	Empower by Magna	663
23.5.4	Ferret	664
23.5.5	Filelock	664
23.5.6	FullBack	665

23.5.7 Invisible Oasis 665
23.5.8 KeysOff und KeysOff Enterprise 665
23.5.9 LockOut 666
23.5.10 MacPassword 666
23.5.11 OnGuard-Notfallpasswörter 666
23.5.12 Password Key 667
23.5.13 Notfallpasswort über das Kontrollfeld Passwortsicherheit 667
23.5.14 Secure-It Locks 667
23.5.15 Super Save 2.02 668
23.6 Passwort-Knacker und ähnliche Utilities 668
23.6.1 FirstClass Thrash! 668
23.6.2 FMProPeeker 1.1 669
23.6.3 FMP Password Viewer Gold 2.0 669
23.6.4 Killer Cracker 669
23.6.5 MacKrack 669
23.6.6 MagicKey 3.2.3a 669
23.6.7 McAuthority 670
23.6.8 MasterKeyII 670
23.6.9 Meltino 670
23.6.10 PassFinder 670
23.6.11 Password Killer 671
23.7 Anonyme E-Mail und E-Mail-Bombing 671
23.8 Macintosh OS X 672
23.9 Speziell für America Online entwickelte Tools 672
23.10 Zusammenfassung 673
23.11 Informationsquellen 673
23.11.1 Bücher und Artikel 673
23.11.2 Websites mit Tools und Munition 674
23.11.3 E-Zines und elektronische Online-Magazine 675

Kapitel 24 VAX/VMS 677

24.1 Die Geschichte von VAX 678
24.2 VMS 681
24.3 Sicherheit in VMS 683
24.4 Einige alte Sicherheitslöcher 685
24.4.1 mountd-Sicherheitsloch 685
24.4.2 Sicherheitsloch Monitor-Utility 686

24.4.3 Ganz frühe Probleme: Der Wank-Wurm-Vorfall 686
24.5 Auditing und Monitoring 688
24.5.1 watchdog.com 689
24.5.2 Stealth 689
24.5.3 GUESS_PASSWORD 689
24.5.4 WATCHER 689
24.5.5 Checkpass 690
24.5.6 Crypt 690
24.5.7 DIAL 690
24.5.8 CALLBACK.EXE 691
24.5.9 TCPFILTER (G. Gerard) 691
24.6 Andere Zeiten 691
24.7 Zusammenfassung 692
24.8 Informationsquellen 693

Teil VII: Die Fäden laufen zusammen 695

Kapitel 25 Waffen im Kampf gegen das Böse 697

25.1 Kampf dem Informationsüberschuss 698
25.2 Wie viel Sicherheit Sie brauchen 700
25.3 Allgemeine Informationsquellen 701
25.3.1 CERT (Computer Emergency Response Team) 701
25.3.2 CIAC (Computer Incident Advisory Capability) 702
25.3.3 CSRC (Computer Security Resource Clearinghouse) 704
25.3.4 Die BUGTRAQ-Archive 704
25.3.5 FIRST (Forum of Incident Response and Security Teams) 705
25.3.6 BSI (Bundesamt für Sicherheit in der Informationstechnologie) 705
25.4 Mailinglisten 706
25.5 Newsgroups 707
25.6 Weitere Informationsquellen und Ressourcen 709
25.6.1 Silicon Graphics Sicherheitszentrale 709
25.6.2 Das Sicherheitsbulletinarchiv von Sun 709
25.6.3 Die Sicherheitslückendatenbank von Xforce 710
25.6.4 NIH (National Institutes of Health) 710
25.6.5 Eugene Spaffords »Security Hotlist« 710
25.6.6 Das SANS-Institut 710
25.7 Fazit 711

Kapitel 26 Richtlinien, Prozeduren und ihre Durchsetzung 713

26.1 Die Bedeutung von Sicherheitsrichtlinien 714
26.2 Standort- und Infrastrukturrichtlinien 714
26.2.1 Einrichtungen und physikalische Sicherheit 715
26.2.2 Infrastruktur und Computerumgebung 718
26.3 Benutzerrichtlinien 738
26.3.1 Administrative Sicherheitsrichtlinien 738
26.3.2 Richtlinien für Benutzer 739
26.4 Durchsetzung der Richtlinien 740
26.5 Zusammenfassung 742
26.5.1 Passwortsicherheit 743
26.5.2 Audits und Analyse 743
26.5.3 Standortsicherheitsrichtlinien 743
26.5.4 Handhabung von Vorfällen 743
26.5.5 Systemkonfiguration 743
26.5.6 Firewalls 743

Kapitel 27 Interne Sicherheit 745

27.1 Interne Sicherheit – das ungeliebte Stiefkind 746
27.2 Interne Risiken: Arten der Sicherheitsverletzung und Vektoren 747
27.2.1 Ignorante Mitarbeiter 749
27.2.2 IT-Mitarbeiter 750
27.3 Risikominderung: Richtlinien 751
27.3.1 Physikalische Sicherheit 751
27.3.2 Einstellung neuer Mitarbeiter 753
27.3.3 Sicherung von Desktops 754
27.3.4 Inhalte einschränken 755
27.3.5 Administrative Zusammenarbeit 757
27.4 Produkte 757
27.4.1 Desktop-Management 757
27.4.2 Laptop-/PDA-Sicherheit 758
27.4.3 Physikalische Sicherheit 759
27.4.4 Content-Management 760
27.5 Informationsquellen 761
27.6 Zusammenfassung 762

Kapitel 28 Überlegungen zum Thema Netzwerkarchitektur 763

28.1 Netzwerkarchitektur 764
28.1.1 Netzwerkkomponenten 764
28.1.2 Bedrohungen 767
28.1.3 Netzwerkarchitektur – Ein Ansatz 769
28.1.4 Sicherheitszonen 771
28.2 Die Burg schützen 774
28.2.1 Isolierung und Trennung 774
28.2.2 Netzwerktrennung 783
28.2.3 Netzwerkisolierung 786
28.3 Zusammenfassung 792

Kapitel 29 Sprachen, Erweiterungen und die Entwicklung sicherer Anwendungen 793

29.1 Sicherheit und Software 794
29.2 Was ist eine sichere Anwendung? 795
29.2.1 Der Feind im Innern 796
29.2.2 Konfigurationsfragen 796
29.2.3 Race-Conditions 797
29.2.4 Pufferüberlauf 800
29.2.5 Datensicherheit 802
29.2.6 Temporärspeicherung 803
29.2.7 DoS-Angriffe 804
29.2.8 Ein-/Ausgabemethoden 805
29.3 Eine Sicherheitsarchitektur 806
29.3.1 Komponenten der Sicherheitsarchitektur 806
29.3.2 Sicherheitsanforderungen 810
29.3.3 Identifikation der Risikobereiche 818
29.3.4 Die Reaktion im Krisenfall 819
29.4 Sicherheitsbewusste Strukturen 820
29.4.1 Analyse der Strukturierungsphase 820
29.5 Das A und O: Sichere Codes 829
29.5.1 C 830
29.5.2 Perl 836
29.5.3 Java 838
29.5.4 Die UNIX-Shells 839

29.5.5	Internet-Appliances	840
29.6	Fazit	840
Anhang A	**Bibliografie zum Thema Sicherheit – weiterführende Literatur**	843
A.1	Allgemeine Internetsicherheit	844
A.2	TCP/IP	854
A.3	NetWare	857
Anhang B	**Grundkurs Internet**	859
B.1	Die Anfänge: 1962 bis 1969	860
B.2	UNIX wird geboren: 1969 bis 1973	862
B.2.1	Die Programmiersprache C	863
B.3	Die prägenden Jahre des Internets: 1972 bis 1975	863
B.3.1	UNIX wird erwachsen	864
B.3.2	UNIX und das Internet entwickeln sich gemeinsam weiter	865
B.3.3	Die grundlegenden Merkmale von UNIX	866
B.3.4	Welche Art von Anwendungen laufen unter UNIX?	868
B.3.5	UNIX und Internetsicherheit	868
B.4	Das Internet der 90er	870
B.4.1	Die Zukunft	871
Anhang C	**Weiterführende Informationsquellen**	873
C.1	Offizielle Informationsquellen	874
C.1.1	Websites	874
C.1.2	Berichte und Publikationen	877
C.1.3	Artikel	881
C.1.4	Tools	882
C.1.5	Technische Berichte, Regierungsstandards und Dokumente	887
Anhang D	**Anbieter aus dem Bereich Sicherheit**	897
D.1	Vorbemerkung	898
D.2	Die Unternehmen	898
D.2.1	ACROS, d.o.o. (Slowenien)	898
D.2.2	Armor Security, Inc. (USA)	898
D.2.3	AS Stallion Ltd. (Estland)	899
D.2.4	ASCIItech (Kanada)	899

D.2.5	AtBusiness Communications (Finnland, Deutschland, Russland)	899
D.2.6	Atlantic Computing Technology Corporation (USA)	900
D.2.7	beTRUSTed (weltweit)	900
D.2.8	Baltimore Technologies	901
D.2.9	Biodata Information Technology (Deutschland)	901
D.2.10	Cambridge Technology Partners, Inc. (weltweit)	901
D.2.11	Canaudit, Inc. (USA)	902
D.2.12	CobWeb Applications (Großbritannien)	902
D.2.13	Command Systems (USA)	902
D.2.14	Computer Associates Services eTrust (weltweit)	903
D.2.15	CorpNet Security (USA)	903
D.2.16	Counterpane Internet Security (USA)	903
D.2.17	Cryptek Secure Communications LLC (USA)	904
D.2.18	CygnaCom Solutions (USA)	904
D.2.19	Data Fellows (Europa, Nordamerika, Asien)	904
D.2.20	Data Systems West (USA)	905
D.2.21	DataLynx, Inc. (USA)	905
D.2.22	Dataway, Inc. (USA, Irland)	906
D.2.23	debis Systemhaus Information Security Services GmbH (Deutschland)	906
D.2.24	Delphi Consulting, LLC (USA)	906
D.2.25	EAC Network Integrators (USA)	907
D.2.26	ECG Management Consultants (USA)	907
D.2.27	EGAN Group Pty Limited (Australien)	907
D.2.28	Energis (Großbritannien)	908
D.2.29	EnGarde Systems, Inc. (USA)	908
D.2.30	EnterEdge Technology LLC (USA)	909
D.2.31	Ernst & Young LLP (USA)	909
D.2.32	eSoft (USA, Großbritannien, Singapur)	909
D.2.33	Espiria (USA)	910
D.2.34	ESTec Systems Corporation (Nord- und Lateinamerika, Asien)	910
D.2.35	Flavio Marcelo Amaral (Brasilien)	910
D.2.36	FMJ/PADLOCK Computer Security Systems (USA)	911
D.2.37	Galaxy Computer Services, Inc. (USA)	911
D.2.38	Gemini Computers, Inc. (USA)	911
D.2.39	GeNUA (Deutschland)	912
D.2.40	Getronics Government Services (USA)	912

D.2.41 GlobalCenter (USA) 913
D.2.42 Global Privacy Solutions (USA) 913
D.2.43 Graham Information Security and Management Services (Australien) 913
D.2.44 Grand Designs Ltd./ConfluX.net (USA) 914
D.2.45 Gregory R. Block (Großbritannien) 914
D.2.46 The GSR Consulting Group Inc. (Kanada) 914
D.2.47 Guardent Inc (Nordamerika, Großbritannien) 915
D.2.48 Hyperon Consulting (USA) 915
D.2.49 I.T. NetworX Ltd. (Irland) 915
D.2.50 Infoconcept GmbH (Deutschland) 916
D.2.51 INFOSEC Engineering (USA) 916
D.2.52 Infosecure Australia (Australien) 916
D.2.53 Ingenieurbüro Dr. Ing. Markus a Campo (Deutschland) 917
D.2.54 Integrity Sciences, Inc. (USA) 917
D.2.55 InterNet Guide Service, Inc. (USA) 917
D.2.56 Internet Security Systems, Inc. (ISS) (USA) 918
D.2.57 Interpact, Inc./Infowar.Com (USA) 918
D.2.58 Jerboa, Inc. (USA) 918
D.2.59 Karl Nagel & Company (USA) 919
D.2.60 Kinetic, Inc. (USA) 919
D.2.61 Learning Tree International (USA) 920
D.2.62 Livermore Software Labs (weltweit) 920
D.2.63 Lucent Worldwide Services Security Consulting (USA und UK) 920
D.2.64 Lunux Network Security Services (USA) 921
D.2.65 Lurhq Corporation (USA) 921
D.2.66 marchFIRST (USA) 922
D.2.67 Maxon Services (Kanada) 922
D.2.68 Merdan Group, Inc. (USA) 922
D.2.69 Merilus Technologies (USA) 923
D.2.70 Milvets System Technology, Inc. (USA) 923
D.2.71 MIS Corporate Defence Solutions (Niederlande und Großbritannien) 923
D.2.72 Myxa Corporation (USA) 924
D.2.73 NetraCorp LLC. (USA) 924
D.2.74 Nett & So GmbH (Deutschland) 925
D.2.75 Network Associates, Inc. (USA) 925
D.2.76 Network Security Assurance Group (USA) 925

D.2.77 Network Technology Solutions, Inc. (USA) 926
D.2.78 NH&A (USA) 926
D.2.79 NovaTech Internet Security (Australien) 926
D.2.80 Pacificnet Internet Services (USA) 927
D.2.81 Pangeia Informatica LTDA (Brasilien) 927
D.2.82 Pentex Net, Inc. (USA) 927
D.2.83 Predictive Systems (USA) 928
D.2.84 PSINet Consulting Solutions (weltweit) 928
D.2.85 R.C. Consulting, Inc. (Kanada) 928
D.2.86 Rainbow Technologies, Spectra Division (USA) 929
D.2.87 Ritter Software Engineering (USA) 929
D.2.88 Saffire Systems (USA) 930
D.2.89 SAGUS Security, Inc. (Kanada) 930
D.2.90 Schlumberger Network Solutions (USA) 930
D.2.91 SecTek, Inc. (USA) 931
D.2.92 secunet Security Networks AG (Deutschland) 931
D.2.93 Security First Technologies, Inc. (USA) 932
D.2.94 Security Sciences (Europa, Naher Osten, Nordamerika, Afrika) 932
D.2.95 Siam Relay Ltd. (Thailand) 932
D.2.96 Slmsoft.com (Kanada) 933
D.2.97 SmallWorks, Inc. (USA) 933
D.2.98 STRATESEC, Inc. (USA, weltweit) 933
D.2.99 Sword & Shield Enterprise Security, Inc. (USA) 934
D.2.100 Symantec Security Services (weltweit) 934
D.2.101 Sysman Computers (P) Ltd. (Indien) 934
D.2.102 Sytex, Inc. (USA) 935
D.2.103 tec-gate.com (USA) 935
D.2.104 Triumph Technologies, Inc. (USA) 935
D.2.105 Utimaco SafeWare AG (weltweit) 936
D.2.106 Verio (USA) 936
D.2.107 Visionary Corporate Computing Concepts (USA) 936
D.2.108 VoteHere.net (USA) 937
D.2.109 WatchGuard Technologies, Inc. (USA) 937
D.2.110 WorldCom (Großbritannien) 938

Anhang E Anbieterinformationen und Sicherheitsstandards 939

E.1 Sicherheitsinformationen von Anbietern 940
E.1.1 Hewlett-Packard 940

E.1.2 IBM 940
E.1.3 Linux 941
E.1.4 Microsoft 942
E.1.5 Sun Microsystems 943
E.2 Sicherheitsrelevante RFCs 943

Anhang F Die CD-ROM 963

F.1 Advanced Administrative Tools 964
F.2 Bastille 964
F.3 DumpSec 964
F.4 Ethereal 964
F.5 FileAudit 965
F.6 Fragrouter: Network Intrusion Detection Evasion Toolkit 965
F.7 Libnet Packet Assembly System 965
F.8 Mail Essentials 965
F.9 MRTG (Multi Router Traffic Grapher) 965
F.10 Nessus 966
F.11 Nmap (Network Mapper) 966
F.12 Npasswd 966
F.13 Ntop 966
F.14 NTRama 967
F.15 OpenSSH 967
F.16 OpenSSL 967
F.17 SAINT (Security Administrator's Integrated Network Tool) 967
F.18 SATAN (Security Administrator Tool for Analyzing Networks) 968
F.19 Scotty/Tkined 968
F.20 Security-Enhanced Linux 968
F.21 Snort 969
F.22 Sudo 969
F.23 TITAN 969
F.24 Trinux 970
F.25 Tripwire 970
F.26 UserLock 970
F.27 YASSP 970
F.28 Zlib 971

Anhang G Glossar zum Thema Sicherheit 973

Stichwortverzeichnis 991