

Inhaltsverzeichnis

Vorwort des Übersetzers	xiii
Vorwort	xv
I Die Grundlagen	1
1 Einführung	3
1.1 Warum Sicherheit?	3
1.2 Auswahl eines Sicherheitskonzepts	6
1.3 Strategien für sichere Datennetze	8
1.4 Ethik der Computersicherheit	17
1.5 WARNUNG	19
2 Ein Überblick über TCP/IP	21
2.1 Die Protokollschichten	21
2.2 Wegwahl: Router und Routing-Protokolle	29
2.3 Das Domain Name System	31
2.4 Standard-Dienste	33
2.5 RPC-basierte Protokolle	39
2.6 Dateitransferprotokolle	45
2.7 Die „r“-Befehle	49
2.8 Informationsdienste	51
2.9 Das X11-System	55
2.10 Vertrauensverhältnisse	56

II	Entwurf einer Firewall	59
3	Firewall-Gateways	61
3.1	Grundidee der Firewall	61
3.2	Plazierung von Firewalls	63
3.3	Paketfilter	64
3.4	Anwendungsschicht-Gateways	89
3.5	Transportschicht-Gateways	91
3.6	Dienstzugang von außen	93
3.7	Gute und böse Tunnel	94
3.8	Joint-ventures	96
3.9	Was Firewalls nicht leisten	97
4	Konstruktion eines Anwendungsschicht-Gateways	101
4.1	Sicherheitskonzept	102
4.2	Mögliche Hardware-Konfigurationen	102
4.3	Anfangsinstallation	105
4.4	Gateway-Werkzeuge	108
4.5	Installation der Dienste	112
4.6	Rückendeckung für die Torwachen	129
4.7	Gateway-Administration	129
4.8	Sicherheitsanalyse – Warum wir unseren Entwurf für einbruchs- und ausfallsicher halten	133
4.9	Durchsatz	135
4.10	TIS Firewall Toolkit	136
4.11	Bewertung von Firewalls	137
4.12	Leben ohne Firewall	138
5	Authentifikation	141
5.1	Benutzerauthentifikation	142
5.2	Host-Host-Authentifikation	146

6	Gateway-Werkzeuge	149
6.1	Proxylib	149
6.2	Syslog	151
6.3	Datennetzpatrouille: tcpdump und Konsorten	153
6.4	Zusätzliche Protokollierung für Standard-Dämonen	154
7	Fallen, Köder und Lockvögel	159
7.1	Was ist zu protokollieren?	159
7.2	Scheinbare Logins	166
7.3	Rückverfolgung einer Verbindung	168
8	Hacker-Werkzeuge	171
8.1	Einleitung	171
8.2	Auskundschaften	173
8.3	Hosts sondieren	177
8.4	Werkzeuge für Netzverbindungen	179
8.5	Routing-Angriffe	180
8.6	Netzüberwachung	181
8.7	Metastasen	182
8.8	Tiger Teams	185
8.9	Weiterführende Literatur	186
III	Ein Blick zurück	189
9	Angriffsarten	191
9.1	Paßwortattacken	191
9.2	Social Engineering	192
9.3	Fehler und Hintertürchen	194
9.4	Versagen der Authentifikationsmechanismen	196
9.5	Protokollfehler	197
9.6	Informationslecks	198

9.7 Denial-of-Service	199
10 Ein Abend mit Berferd	201
10.1 Einleitung	201
10.2 Feindbewegungen	201
10.3 Ein Abend mit Berferd	204
10.4 Der Tag danach	209
10.5 Die „Gummizelle“	210
10.6 Jagd auf Berferd	212
10.7 Berferd kehrt heim	214
11 Wo die wilden Kerle wohnen: Ein Blick in die Protokolle	217
11.1 Ein Jahr des Hackens	219
11.2 Proxy-Benutzung	226
11.3 Angriffsquellen	227
11.4 Signalrauschabstand	229
 IV Verschiedenes	 233
12 Rechtliche Aspekte	235
12.1 Computer Crime Statutes – Amerikanische Gesetze gegen Computer- kriminalität	236
12.2 Protokollaufzeichnungen als Beweismittel	238
12.3 Ist Überwachung legal?	242
12.4 Haftpflicht und Schadensersatzforderungen	247
 13 Sichere Kommunikation über unsichere Netze	 251
13.1 Eine Einführung in die Kryptographie	251
13.2 Das Kerberos-Authentifikationssystem	265
13.3 Leitungsschicht-Verschlüsselung	269
13.4 Netzwerkschicht- und Transportschicht-Verschlüsselung	270
13.5 Anwendungsschicht-Verschlüsselung	272

14 Wie geht's weiter?	279
V Cyberlaw: Die Entwicklung im deutschen Recht	283
15 Einleitung: Cyberlaw – Das Recht in Datennetzen	285
16 Strafrechtliche Verbote in Datennetzen	287
16.1 Allgemeine Fragen	287
16.2 Ausspähen von Daten	290
16.3 Betrieblicher Geheimschutz und Schutz des geistigen Eigentums	291
16.4 Datenveränderung, Computersabotage, Computerbetrug und unbefugte Anlagennutzung	293
16.5 Datenschutzstrafrecht	295
16.6 Verbreitung von Informationen mit strafbarem Inhalt	296
17 Staatliche Ermittlungsbefugnisse in Datennetzen	301
17.1 Allgemeine Fragen	301
17.2 Nationale Zuständigkeit	302
17.3 Einzelne Zwangsmaßnahmen	304
17.4 Computerdaten als Beweismittel	307
18 Rechtsvorschriften über private Sicherungs- und Ermittlungsmaßnahmen	309
18.1 Verpflichtung zu Sicherheitsmaßnahmen	309
18.2 Verbotene Überwachungsmaßnahmen	313
19 Zivilrechtliche Ansprüche	319
19.1 Allgemeine vertragliche Ansprüche	319
19.2 Schadensersatz-, Unterlassungs- und Gegendarstellungsansprüche . . .	322
A Nützliches – frei verfügbar	327
A.1 Bau von Firewalls	328
A.2 Werkzeuge zur Netzadministration und -überwachung	332
A.3 Auditing-Pakete	333

A.4 Kryptographische Software	335
A.5 Informationsquellen	337
B TCP- und UDP-Ports	339
B.1 Fixe Port-Nummern	339
B.2 MBone-Übersicht	342
C Empfehlungen für Hersteller	345
C.1 Allgemein	345
C.2 Hosts	345
C.3 Router	346
C.4 Protokolle	347
C.5 Firewalls	347
Literaturverzeichnis	349
Verzeichnis der ●	371
Index	373