

Alexander Otto

Internet-Sicherheit für Einsteiger

Galileo Computing

OOV~

Inhalt

1	Einleitung	13
1.1	Für wen dieses Buch geeignet ist	15
1.2	Wie Sie mit diesem Buch arbeiten können	15
1.3	Inhalt der Kapitel	16
1.4	Noch eine Bitte	18
2	Grundlagen der Datenübertragung im Internet	19
2.1	Die Struktur des Internet	19
2.2	Das Client-Server-Prinzip	20
2.2.1	Ports	21
2.3	Die TCP/IP-Protokoll-Familie	23
2.3.1	Das TCP/IP-Schichtenmodell	23
2.4	Protokolle und Dienste	27
2.4.1	Protokolle der Anwendungsschicht	27
2.4.2	Protokolle der Transportschicht	39
2.4.3	Protokolle der Netzwerkschicht	43
2.4.4	Protokolle der physikalischen Schicht	48
2.5	Grundprinzipien der Internet-Sicherheit	49
2.6	Konzeptionelle Fehler der TCP/IP-Protokollfamilie und daraus resultierende Sicherheitsprobleme	51
2.6.1	TCP-Hijacking	52
2.6.2	FTP-Bounce-Attacke	53
2.7	Quellen im Internet	54
	Gefahren im Internet	55
3.1	Einführung	55
3.1.1	Wie hoch ist die Wahrscheinlichkeit eines Angriffs?	57
3.1.2	Malware	61
3.2	Allgemeine Gefahrenquellen und deren Auswirkungen auf die Internet-Sicherheit	62
3.2.1	Ursachen softwarebedingter Sicherheitslücken	62
3.2.2	Mögliche Folgen softwarebedingter Sicherheitslücken	67
3.3	Computerviren	68
3.3.1	In-the-wild-Viren	69
3.3.2	Was sind eigentlich Computerviren?	70
3.3.3	Wie hoch ist das Risiko einer Virus-Infektion?	71
3.3.4	Viren-Brutstätten und Motive	73

3.3.5	Struktur und Funktionsweise eines Computervirus	74
3.3.6	Virenklassen und Virenarten	77
3.3.7	Virenschutz und Vorsorge	86
3.4	E-Mail-Gefahren	89
3.4.1	E-Mail-Würmer	89
3.4.2	Hoaxes und Kettenbriefe	98
3.4.3	Mailbombing-Angriffe auf E-Mail-Postfächer	100
3.5	Trojanische Pferde	102
3.5.1	Aufspüren und Beseitigen von Trojanern	103
3.6	0190-Dialer	107
3.6.1	Tarifmodelle	107
3.6.2	Wer ist gefährdet?	108
3.6.3	Die Tricks der Abzocker	109
3.6.4	Aufspüren und Entfernen von 0190-Dialern	116
3.6.5	Schutz vor 0190-Dialern	119
3.6.6	Rechtsmittel gegen Anbieter illegaler 0190-Dialer	121
3.7	DoS-Attacken	123
3.7.1	DDoS-Attacken	127
3.8	Quellen im Internet	128
3.8.1	Hersteller von Antivirus-Software	128
3.8.2	Security-Portale	128
4	Datenschutz und Privatsphäre im Internet	129
4.1	User-Tracking	130
4.2	Cookies	130
4.2.1	So werden Cookies missbraucht	133
4.2.2	Cookie-FAQs	135
4.2.3	Cookie-Management im Browser	136
4.2.4	Cookie-Management mit Netscape 7 und Mozilla	136
4.2.5	Cookie-Verwaltung mit dem Internet Explorer 6	143
4.3	Webbug - Der Spion im Pixel	147
4.3.1	Schutz vor spionierenden Bannern und Webbugs	149
4.4	Anonym surfen und mailen	151
4.4.1	Proxy-Einstellungen beim Internet Explorer	152
4.4.2	Proxy-Einstellungen bei Netscape-Browsern	153
4.4.3	Proxy-Tools	153
4.4.4	Browser-Cache löschen	154
4.4.5	Peekabooby	156
4.4.6	Anonyme Remailer	158
4.5	Spamming - Datenmüll im Postfach	159
4.5.1	Problematik und Gefahren von Junk-Mails	161
4.5.2	Kampf gegen Spam - So schützen Sie sich	161
4.5.3	Anti-Spam Tools (Spam-Filter)	165

4.6	Spyware	167
4.6.1	So spionieren Softwarefirmen Sie aus	168
4.6.2	Welche Programme übertragen Daten an einen Internet-Server?	170
4.6.3	Erkennung und Beseitigung von Spionage-Modulen	172
4.7	Quellen im Internet	173
5	Schutz-und Abwehrmaßnahmen	175
5.1	Warum Sie sich schützen sollten	175
5.2	Wie Sie sich schützen können	176
5.3	Umgang mit Passwörtern	177
5.3.1	Internet Explorer-Einstellungen für AutoVervollständigen	178
5.3.2	Netscape 7/Mozilla - Passwort-Manager	179
5.3.3	Was Sie bei der Wahl von Passwörtern beachten sollten	179
5.4	Verhalten in öffentlichen Foren	181
5.5	Datensicherung	182
5.5.1	Datensicherung mit Windows 9x/ME	183
5.5.2	Datensicherung mit Windows XP	184
5.5.3	Wiederherstellung verloren gegangener Daten	187
5.5.4	Systemwiederherstellung	188
5.6	Einstellungssache - Browser-Sicherheit	190
5.6.1	Die Sicherheitseinstellungen des Internet Explorer	191
5.6.2	Erweiterte Internetoptionen	198
5.6.3	Gute Seiten - schlechte Seiten	199
5.7	Outlook Express - Sicherheitsoptionen	201
5.7.1	Der Reiter »Sicherheit«	201
5.7.2	Der Reiter »Senden«	203
5.7.3	Der Reiter »Erstellen«	204
5.7.4	Der Reiter »Lesen«	204
5.8	Regelmäßige Updates installieren	205
5.9	Sicherheits-Software	209
5.10	Antivirus-Software	210
5.10.1	Arbeitsweise einer AV-Software	210
5.10.2	Tipps zur Benutzung von AV-Software	212
5.10.3	Auswahlkriterien für ein Antivirus-Programm	214
5.11	Desktop-Firewalls	222
5.11.1	Grundfunktionen und Komponenten einer Firewall	223
5.11.2	Grenzen von Firewalls	225
5.11.3	Basis-Strategien: Alles erlauben oder alles verbieten?	226
5.11.4	Personal Firewalls-Die Qual der Wahl	227
5.12	Workshop: Norton Internet Security 2002	233
5.12.1	Was ist NIS 2002?	234
5.12.2	Persönliche Firewall	235

5.12.3	Datenschutz	243
5.12.4	Norton AntiVirus	245
5.13	Der Hartetest - Schwachstellen aufdecken	247
5.13.1	Symantec Security Check	248
5.13.2	LeakTest	249
5.14	Quellen im Internet	250
5.14.1	Hersteller von Personal Firewalls	250
5.14.2	Online-Magazine, die Software-Tests veroffentlichen	251
6	Sicherheit im Bereich der Internet-Programmierung	253
6.1	bersicht: Programmiersprachen	254
6.1.1	Compilersprachen vs. Interpretersprachen	256
6.1.2	Skriptsprachen	257
6.2	Buffer-Overflow (Pufferuberlauf)	258
6.3	Ansatze zur sicheren Gestaltung von Programmen	262
6.3.1	Sandbox-Systeme und virtuelle Maschinen	263
6.3.2	Das Konzept der objektorientierten Programmierung	265
6.4	Moderne Web-Technologien und damit verbundene Risiken	267
6.4.1	Allgemeine Gefahren durch aktive Inhalte	269
6.5	JavaScript	270
6.5.1	JavaScript-Objekte	271
6.5.2	Die Sicherheit von JavaScript	272
6.6	Java	274
6.6.1	Das Java-Sicherheitsmodell	278
6.6.2	Schwachstellen von Java	281
6.7	ActiveX	282
6.8	CGI/Perl	285
6.8.1	Allgemeines zur Sicherheit von CGI	286
6.9	PHP/ASP	287
6.9.1	Die Sicherheit von PHP	289
6.10	Quellen im Internet	289
6.10.1	CGI-Sicherheit	289
6.10.2	Sicherheit von Java und ActiveX	290
7	Windows-Sicherheit	291
7.1	Die Evolution der Windows-Architektur	292
7.2	Windows im Heimnetzwerk	295
7.3	Die Sicherheit von Windows 9x/ME	297
7.3.1	Datei- und Druckerfreigabe	297
7.3.2	Freigaben-Check	300

7.3.3	Sichere Nutzung der Datei- und Druckerfreigabe im LAN	301
7.3.4	Der Windows DFÜ-Server	309
7.3.5	Windows 9x Bugreport	312
7.4	Windows NT/2000-Sicherheit	316
7.4.1	FAT(32) vs. NTFS	318
7.4.2	Benutzerverwaltung	320
7.4.3	Security Access Manager	324
7.4.4	Arbeitsgruppe vs. Domäne	325
7.4.5	Sicherheitsmerkmale von Windows 2000	326
7.4.6	Sicherheitstipps für Windows NT/2000	327
7.5	Die Sicherheit von Windows XP Home Edition	329
7.5.1	Licht & Schatten	329
7.5.2	XP-AntiSpy	332
7.5.3	Die Benutzerverwaltung von Windows XP	334
7.5.4	Windows XP-Dienste	336
7.5.5	Internetverbindungsfirewall (IVF)	351
7.5.6	Microsoft Baseline Security Analyzer	354
7.6	Quellen im Internet	356
7.6.1	Windows-Portale	356
7.6.2	Windows-Sicherheit	356
8	Kryptographie und Datenverschlüsselung	357
8.1	Was ist Kryptographie?	360
8.2	Symmetrische Verschlüsselungsverfahren	362
8.3	Asymmetrische Verschlüsselungsverfahren	363
8.4	Hash-Funktionen	365
8.5	Schlüssellängen	366
8.6	Digitale Signaturen	367
8.7	PKI - Public Key Infrastructure	368
8.7.1	Zertifikate und Trustcenter	369
8.8	SSL - Secure Socket Layer	371
8.9	PGP-PrettyGood Privacy	374
8.9.1	Funktionen von PGP 6.5.x	378
8.10	GNU Privacy Guard (GnuPG)	380
8.10.1	Die Module von GnuPG	380
8.11	Daten verschlüsseln mit ArchiCrypt Pro	382
8.12	Quellen im Internet	385

	Sicherheit beim Homebanking	387
9.1	Das Sicherheitskonzept im Homebanking	388
9.2	PIN/TAN-Verfahren	389
9.3	HBCI	390
9.4	Homebanking-Software	392
9.5	Virtuelle Bankräuber	393
9.6	Tipps für sicheres Homebanking	395
9.7	Quellen im Internet	397
10	Sicherheit beim Online-Shopping	399
10.1	Anforderungen an Online-Shops	400
10.2	Gütesiegel - Zertifizierte Online-Shops	401
10.2.1	Trusted Shops	402
10.2.2	EHI Geprüfter Online-Shop	402
10.2.3	S@fer Shopping	403
10.3	Zahlungssysteme im Internet	403
10.3.1	Bezahlung mit Kreditkarte	405
10.3.2	SET-Secure Electronic Transaction	407
10.3.3	Firstgate Click & Buy	408
10.3.4	Microsoft .NET Wallet	408
10.4	Quellen im Internet	410
11	Sicherheit im Heimnetzwerk	411
11.1	Netzwerkarchitekturen	413
11.2	Internetverbindungsfreigabe von Windows	415
11.2.1	Installation der ICS unter Windows 98SE/ME	417
11.2.2	ICS unter Windows XP einrichten	419
11.3	Firewall-Architekturen und-Konzepte	420
11.3.1	Paketfilter (Screening Router)	421
11.3.2	Application-Gateways	422
11.3.3	Screened Host	423
11.4	Jana-Server	424
11.4.1	Installation und Start des Jana-Server	425
11.4.2	Namensauflösung und IP-Adresse	426
11.4.3	DFÜ-Einstellungen	428
11.4.4	Benutzer-Verwaltung	429
11.4.5	Servertypen	430
11.4.6	Konfiguration der Clients	430
11.4.7	Konfiguration des Webbrowsers	431

11.5	WinRoute	431
11.5.1	WinRoute konfigurieren	432
11.6	DSL-Router	434
11.6.1	Netgear RO318 Security Router als Beispiel	436
11.7	Netzwerkanalyse- und Auditing-Tools	437
11.7.1	Netstat	438
11.7.2	TCPView	439
11.7.3	Superscan	440
11.7.4	Essential NetTools	440
11.7.5	Ethereal	441
11.7.6	NMap	442
11.8	Wireless LAN (WLAN)	443
11.8.1	Access Points	444
11.8.2	Angriffe auf Funknetzwerke	445
11.8.3	SSID (Service Set Identifier)	446
11.8.4	WEP (Wired Equivalent Privacy)	447
11.8.5	Sicherheitsanforderungen an WLANs	448
11.8.6	Maßnahmen zur Absicherung drahtloser Netzwerke	449
11.9	Quellen im Internet	451
12	VPN - Virtual private Network	453
12.1	Was ist ein VPN?	454
12.2	VPN-Tunneling	455
12.2.1	PPTP und L2TP	456
12.2.2	IPsec	456
12.3	VPN unter Windows XP	457
12.4	VPN unter Windows 95/98/ME	461
12.4.1	Einrichtung eines VPN-Clients unter Windows ME	461
12.4.2	Einrichtung eines VPN-Clients unter Windows 95/98	463
12.5	Quellen im Internet	463
A	Inhalt der CD-ROM	464
B	Glossar	465
	Index	475