

Inhaltsverzeichnis

1	Einleitung	1
2	Grundlagen	5
2.1	Einführung	5
2.2	ISO/OSI-Modell	7
2.3	Techniken der Datenübertragung im Internet	8
2.3.1	Protokolle der Internetschicht	10
2.3.1.1	IPv4 (Internet Protocol Version 4)	10
2.3.1.2	Routing im Internet	15
2.3.1.3	ICMP (Internet Control Message Protocol)	17
2.3.1.4	IPv6 (Internet Protocol Version 6)	18
2.3.2	Protokolle der Transportschicht	22
2.3.2.1	TCP (Transmission Control Protocol)	22
2.3.2.2	UDP (User Datagram Protocol)	26
2.3.3	Protokolle der Anwendungsschicht	26
2.3.3.1	DNS (Domain Name System)	26
2.3.3.2	FTP (File Transfer Protocol)	29
2.3.3.3	HTTP (Hypertext Transfer Protocol)	32
2.3.3.4	IRC (Internet Relay Chat)	33
2.3.3.5	NNTP (Network News Transfer Protocol)	36
2.3.3.6	NFS (Network File System)	37
2.3.3.7	POP3 (Post Office Protocol Version 3)	37
2.3.3.8	IMAP4 (Internet Message Access Protocol Version 4)	39
2.3.3.9	SMTP (Simple Mail Transfer Protocol)	40
2.3.3.10	Telnet-Protokoll	42
2.4	Allgemeine Sicherheitsmaßnahmen	43
2.4.1	Passwörter	43
2.4.2	Evaluation und Zertifizierung von Soft- und Hardware	45
3	Gefährdungen bei der Nutzung des Internet	47
3.1	Allgemeine Gefährdungen	48
3.1.1	Social Engineering	54
3.1.2	Vielfalt der Zugangsmöglichkeiten	55
3.1.3	Systemanomalien	56

3.2	Informationsgewinnung	58
3.2.1	Portscanning	58
3.2.2	„Geschwätzige“ Dienste	58
3.3	Spoofing	59
3.3.1	IP-Spoofing	59
3.3.2	DNS-Spoofing	60
3.3.3	Web-Spoofing	63
3.4	Sniffing	63
3.5	Spezielle Protokollfehler	65
3.5.1	IP-Fragmentierung	65
3.5.2	ICMP	67
3.5.3	TCP-Hijacking	68
3.5.4	FTP-Bounce-Attacke	68
3.5.5	E-Mail	69
3.5.5.1	Mail-Spamming	69
3.5.5.2	Hoax und Kettenbriefe	72
3.6	Speicherüberlauf (Buffer Overflow)	74
3.7	Angriffe aufgrund von geteilten Ressourcen	74
3.8	Denial-of-Service-Angriffe (DoS)	75
3.9	Verteilte Denial-of-Service-Angriffe (DDoS)	77
4	Kryptographie	79
4.1	Einführung	79
4.1.1	Leitungsverschlüsselung	80
4.1.2	Ende-zu-Ende-Verschlüsselung	81
4.2	Verschlüsselungsverfahren	82
4.2.1	Symmetrische Verschlüsselungsverfahren	82
4.2.2	Asymmetrische Verschlüsselungsverfahren	88
4.2.3	Hybride Verschlüsselung	93
4.3	Kryptographische Prüfsummen (Message Digest)	94
4.4	Digitale Signaturen, Zertifikate und Zertifizierungsstellen	96
4.4.1	Digitale Signaturen	96
4.4.2	Zertifikate und Zertifizierungsstellen	97
4.5	Internet-Standards	103
4.5.1	SSL (Secure Socket Layer)	103
4.5.2	PGP (Pretty Good Privacy)	107
4.5.2.1	Funktionen von PGP 2.6.3i	108
4.5.2.2	Funktionen von PGP 6.5.1	115
4.5.2.3	Schlüsselverwaltung und -weitergabe mit PGP	117
4.5.3	GnuPG (GNU Privacy Guard)	123
4.5.4	PEM (Privacy Enhanced Mail)	128
4.5.5	S/MIME	131
4.5.6	SSH (Secure Shell)	131
4.5.7	Kerberos	132
4.6	Wirksamkeit von Verschlüsselungsverfahren	133
4.7	Steganographie	135

5	Firewalls	137
5.1	Einführung	137
5.2	Bestandteile einer Firewall	139
5.2.1	Sicherheitspolitik	139
5.2.2	Filter	143
5.2.2.1	Paketfilter	143
5.2.2.2	Zustandsabhängige Paketfilter	148
5.2.2.3	Application-Gateway	150
5.2.3	Sicherheitsmanagement	155
5.3	Firewall-Architekturen	158
5.3.1	Einsatz nur eines Paketfilters	158
5.3.2	Einsatz nur eines Application-Gateways	159
5.3.3	Screened Subnet mit Single-Homed Gateway	161
5.3.4	Screened Subnet mit Multi-Homed Gateway	163
5.3.5	Anordnung der DNS-Server	165
5.3.5.1	DNS-Konzept ohne Application-Gateway	166
5.3.5.2	DNS-Konzept mit Application Gateway	167
5.3.6	Firewalls und Verschlüsselung	168
5.3.7	Firewalls und aktive Inhalte	171
5.4	Protokollierung: Erzeugung, Analyse und Reaktion	173
5.4.1	Protokollierung	174
5.4.2	Verhalten im Falle eines Angriffs	176
5.5	Intrusion Detection und Intrusion Response	181
5.5.1	Intrusion-Detection-Systeme (IDS)	181
5.5.1.1	Datensammlung	181
5.5.1.2	Datenanalyse	182
5.5.1.3	Grenzen eines Netz-basierten IDS	185
5.5.2	Intrusion Response System (IRS)	186
5.5.3	Integration eines IDS in eine Firewall	187
5.5.4	Einbindung des IDS in das Netzwerkmanagement	189
5.5.5	Erwartungen an ein Intrusion Detection System	190
5.6	Konfiguration einer Firewall	191
5.6.1	DNS	194
5.6.2	FTP	195
5.6.3	HTTP	197
5.6.4	NNTP	197
5.6.5	SMTP	198
5.6.6	Telnet	199
5.7	Ausblicke	200
6	Informationsserver	203
6.1	Einleitung	203
6.2	Sicherheitspolitik	205
6.3	Rechnersicherheit	208
6.3.1	Minimalsystem	208
6.3.2	Zugangsschutz, Protokollierung und Integritätskontrolle	211

6.3.3	Schutz und Aktualisierung der Daten	212
6.4	Server-Software	215
6.4.1	Installation eines HTTP-Servers	216
6.4.2	Installation eines FTP-Servers	221
6.4.3	Sicherheitstests	225
6.5	CGI, SSI	227
6.5.1	CGI-Programme	228
6.5.2	Server Side Includes	238
7	Browser	241
7.1	Einführung	241
7.2	Netscape Navigator 3	244
7.2.1	Einstellung der Proxy-Server	244
7.2.2	Aktive Inhalte (Java, JavaScript)	245
7.2.3	Allgemeine Sicherheitseinstellungen	245
7.2.4	Kennwörter	247
7.2.5	Persönliche Zertifikate	247
7.2.6	Netsite-Zertifikate	248
7.3	Netscape Navigator 4.7	250
7.3.1	Einstellung der Proxy-Server	250
7.3.2	Aktive Inhalte (Java, JavaScript)	250
7.3.3	Allgemeine Sicherheitseinstellungen	258
7.3.4	Kennwörter	260
7.3.5	Zertifikate	261
7.4	Mozilla 0.9 und Netscape Navigator 6	262
7.4.1	Einstellung der Proxy-Server	263
7.4.2	Aktive Inhalte	263
7.4.3	Allgemeine Sicherheitseinstellungen	264
7.4.4	Zertifikate und Verschlüsselung	267
7.5	Internet Explorer 3.0	268
7.5.1	Einstellung der Proxy-Server	268
7.5.2	Zertifikate	270
7.5.3	Aktive Inhalte	271
7.5.4	Zusätzliche Sicherheitseinstellungen	272
7.6	Internet Explorer 4.0	273
7.6.1	Einstellung der Proxy-Server	273
7.6.2	Zertifikate	275
7.6.3	Weitere Sicherheitseinstellungen	276
7.6.4	Sicherheitszonen	279
7.6.5	Persönliche Einstellungen	286
7.7	Internet Explorer 5 und 6	288
7.7.1	Einstellungen für Verbindungen und Proxy-Server	289
7.7.2	Zertifikate und persönliche Einstellungen	291
7.7.3	Sicherheitszonen	295
7.7.4	Weitere Sicherheitseinstellungen	300
7.8	Opera 5	303

7.8.1	Einstellungen für Verbindungen und Proxy-Server	303
7.8.2	Zertifikate und persönliche Einstellungen	304
7.8.3	Aktive Inhalte	306
7.8.4	Weitere Sicherheitseinstellungen	306
7.9	Konqueror	308
7.9.1	Einstellungen des Proxy-Servers	308
7.9.2	Aktive Inhalte	308
7.9.3	Einstellungen zur Verschlüsselung	308
7.9.4	Weitere Sicherheitseinstellungen	309
8	Inhaltsfilterung	311
8.1	Einsatzgebiete für Inhaltsfilter	311
8.1.1	Filtertechnik	312
8.1.2	Proxy-Lösung	313
8.1.3	Client-basierte Lösung	313
8.2	Anforderungen an ein Filtersystem	314
8.3	Grenzen der Inhaltsfilterung	316
8.4	Selbstkontrollsysteme	317
8.5	Zusatzsoftware für den Web-Zugriff	321
8.5.1	Internet-Junkbuster	321
8.5.2	Webwasher	322
9	Personal Firewalls	325
9.1	Einleitung	325
9.2	Funktionen von Personal Firewalls	326
9.3	Beispielhafte Konfiguration einer Personal Firewall	330
9.4	Einsatzszenarien für Personal Firewalls	334
10	Telearbeit und Videokonferenzen	337
10.1	Einführung	337
10.2	Formen der Telearbeit	338
10.3	Gefährdungen beim Einsatz von Telearbeit	340
10.3.1	Gefährdungen am Telearbeitsplatz	341
10.3.2	Gefährdungen bei der Datenübertragung	343
10.3.3	Bedrohungen an der Schnittstelle zum LAN	344
10.4	Sicherheitsanforderungen beim Einsatz von Telearbeit	345
10.4.1	Maßnahmen zur Absicherung der Telearbeitsplätze	345
10.4.2	Maßnahmen zum Schutz der Telekommunikations- verbindung	347
10.4.3	Maßnahmen zur Absicherung des Zugangs zum Intranet	349
10.5	Authentisierung	351
10.5.1	Authentisierungsverfahren	351
10.5.2	Authentisierungsprotokolle	355
10.5.2.1	RADIUS und TACACS	355
10.5.2.2	PAP und CHAP	357
10.6	Videokonferenzen	358

10.6.1	Bestandteile einer Videokonferenz nach H.323	358
10.6.2	Ablauf einer Videokonferenz nach H.323	363
10.6.3	RTP und RTCP	366
10.6.4	T.120	367
10.6.5	Bedrohungen beim Einsatz von Videokonferenzen	371
10.6.6	Sicherheitsmaßnahmen beim Einsatz von Videokonferenzen	372
10.6.6.1	Paketfilter	373
10.6.6.2	Einsatz von Verschlüsselungsverfahren	374
10.6.6.3	Application-Level-Gateway	375
11	Anonymität, Privatsphäre und Recht im Internet	377
11.1	Spuren im Internet	377
11.1.1	Cookies	377
11.1.2	Personal Privacy Preferences (P3P)	384
11.2	Anonyme und pseudonyme Nutzung von Internet-Diensten	387
11.2.1	E-Mail	387
11.2.2	HTTP	390
11.2.3	Anonymity 4 Proxy	391
11.3	Rechtliche Aspekte	393
12	Electronic Commerce	401
12.1	Zahlungssysteme im Internet	401
12.1.1	Einführung	401
12.1.2	Unterschiede und Gemeinsamkeiten	404
12.1.3	Ecash, CAFE und Mondex	405
12.1.4	CyberCash und First Virtual	408
12.1.5	iKP	412
12.1.6	SET	415
12.2	Online-Banking und HBCI	419
12.3	Aktive Inhalte (Executable Content)	421
12.3.1	Allgemeine Gefährdungen beim Einsatz aktiver Inhalte	422
12.3.2	Java	425
12.3.3	JavaScript	433
12.3.4	ActiveX	438
12.3.5	Plug-ins, Helper-Applications und MIME-Types	441
Anhang		445
I	Adressen	445
II	Programme	450
III	Notfallplan für einen Angriff aus dem Internet	456
IV	Benutzerordnung für die Nutzung des Internet	459
V	Glossar	464
Literaturverzeichnis		473
Stichwortverzeichnis		479