

---

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung .....</b>	<b>1</b>
<b>2</b>	<b>Grundlagen .....</b>	<b>5</b>
2.1	Einführung .....	5
2.2	ISO/OSI-Modell .....	7
2.3	Techniken der Datenübertragung im Internet .....	8
2.3.1	Protokolle der Internetschicht.....	11
2.3.1.1	IPv4 (Internet Protocol Version 4).....	11
2.3.1.2	Routing im Internet.....	16
2.3.1.3	ICMP (Internet Control Message Protocol).....	18
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 .....	27
2.3.3.1	DNS (Domain Name System).....	27
2.3.3.2	FTP (File Transfer Protocol).....	30
2.3.3.3	HTTP (Hypertext Transfer) .....	34
2.3.3.4	IRC (Internet Relay Chat).....	35
2.3.3.5	NNTP (Network News Transfer Protocol) .....	38
2.3.3.6	NFS (Network File System) .....	39
2.3.3.7	POP3 (Post Office Protocol Version 3) .....	40
2.3.3.8	SMTP (Simple Mail Transfer Protocol) .....	41
2.3.3.9	Telnet-Protokoll.....	43
2.4	Allgemeine Sicherheitsmaßnahmen.....	43
2.4.1	Paßwörter.....	44
2.4.2	Evaluation und Zertifizierung von Soft- und Hardware.....	46
<b>3</b>	<b>Gefährdungen bei der Nutzung des Internet .....</b>	<b>49</b>
3.1	Allgemeine Gefährdungen .....	49
3.1.1	Social Engineering.....	56

3.1.2	Vielfalt der Zugangsmöglichkeiten .....	57
3.1.3	Systemanomalien.....	59
3.2	Informationsgewinnung .....	60
3.2.1	Portscanning .....	60
3.2.2	„Geschwätzige“ Dienste .....	61
3.3	Spoofing .....	61
3.3.1	IP-Spoofing.....	62
3.3.2	DNS-Spoofing .....	63
3.3.3	Web-Spoofing.....	65
3.4	Sniffing.....	66
3.5	Spezielle Protokollfehler.....	67
3.5.1	IP .....	67
3.5.2	ICMP .....	70
3.5.3	TCP.....	70
3.5.4	FTP .....	71
3.5.5	Email.....	72
3.5.5.1	Mail-Spamming .....	72
3.5.5.2	Hoax und Kettenbriefe.....	76
3.6	Speicherüberlauf (Buffer Overflow).....	77
3.7	Angriffe aufgrund von geteilten Ressourcen .....	78
3.8	Denial-of-Service-Angriffe (DoS) .....	78
<b>4</b>	<b>Kryptographie.....</b>	<b>81</b>
4.1	Einführung .....	81
4.2	Verschlüsselungsverfahren .....	83
4.2.1	Symmetrische Verschlüsselungsverfahren.....	83
4.2.2	Asymmetrische Verschlüsselungsverfahren.....	90
4.3	Kryptographische Prüfsummen (Message Digest).....	96
4.4	Digitale Signaturen, Zertifikate und Zertifizierungsstellen .....	98
4.4.1	Digitale Signaturen.....	98
4.4.2	Zertifikate und Zertifizierungsstellen .....	99
4.5	Internet-Standards .....	104
4.5.1	SSL (Secure Socket Layer) .....	106
4.5.2	PGP (Pretty Good Privacy) .....	109
4.5.2.1	Funktionen von PGP 2.6.3i.....	109
4.5.2.2	Funktionen von PGP 6.5.1.....	117

---

4.5.2.3	Schlüsselverwaltung und -weitergabe mit PGP.....	119
4.5.3	PEM (Privacy Enhanced Mail).....	127
4.5.4	S/MIME.....	129
4.5.5	SSH (Secure Shell).....	130
4.5.6	Kerberos.....	130
4.6	Wirksamkeit von Verschlüsselungsverfahren.....	132
4.7	Steganographie.....	134
<b>5</b>	<b>Firewalls.....</b>	<b>137</b>
5.1	Einführung.....	137
5.2	Bestandteile einer Firewall.....	139
5.2.1	Sicherheitspolitik.....	139
5.2.2	Filter.....	143
5.2.2.1	Packet-Filter.....	143
5.2.2.2	Zustandsabhängige Packet-Filter.....	149
5.2.2.3	Application-Gateway.....	150
5.2.3	Sicherheitsmanagement.....	155
5.3	Firewall-Architekturen.....	158
5.3.1	Einsatz nur eines Packet-Filters.....	159
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.....	164
5.3.5	Anordnung der DNS-Server.....	166
5.3.6	Firewalls und Verschlüsselung.....	169
5.3.7	Firewalls und ausführbare Inhalte.....	171
5.4	Protokollierung: Erzeugung, Analyse und Reaktion.....	174
5.4.1	Protokollierung.....	174
5.4.2	Intrusion Detection und Intrusion Response.....	177
5.4.3	Verhalten im Falle eines Angriffs.....	181
5.5	Konfiguration einer Firewall.....	185
5.5.1	DNS.....	188
5.5.2	FTP.....	190
5.5.3	HTTP.....	192
5.5.4	NNTP.....	193
5.5.5	SMTP.....	194
5.5.6	Telnet.....	196

5.6	Ausblicke .....	197
<b>6</b>	<b>Informationsserver .....</b>	<b>199</b>
6.1	Einleitung .....	199
6.2	Sicherheitspolitik .....	202
6.3	Rechnersicherheit .....	203
6.3.1	Minimalsystem .....	204
6.3.2	Zugangsschutz, Protokollierung und Integritätskontrolle .....	207
6.3.3	Schutz und Aktualisierung der Daten .....	207
6.4	Server-Software .....	211
6.4.1	Installation eines HTTP-Servers .....	212
6.4.2	Installation eines FTP-Servers .....	218
6.4.3	Sicherheitstests .....	222
6.5	CGI, SSI .....	224
6.5.1	CGI-Programme .....	225
6.5.2	Server Side Includes .....	235
<b>7</b>	<b>Browser .....</b>	<b>241</b>
7.1	Einführung .....	241
7.2	Netscape Navigator 3 .....	244
7.2.1	Einstellung der Proxy-Server .....	244
7.2.2	Ausführbare Inhalte (Java, JavaScript) .....	245
7.2.3	Allgemeine Sicherheitseinstellungen .....	246
7.2.4	Kennwörter .....	247
7.2.5	Persönliche Zertifikate .....	247
7.2.6	Netsite-Zertifikate .....	248
7.3	Netscape Navigator 4.6 .....	250
7.3.1	Einstellung der Proxy-Server .....	250
7.3.2	Ausführbare Inhalte (Java, JavaScript) .....	251
7.3.3	Allgemeine Sicherheitseinstellungen .....	259
7.3.4	Kennwörter .....	262
7.3.5	Zertifikate .....	263
7.4	Internet Explorer 3.0 .....	265
7.4.1	Einstellung der Proxy-Server .....	265
7.4.2	Zertifikate .....	267
7.4.3	Ausführbare Inhalte .....	268

7.4.4	Zusätzliche Sicherheitseinstellungen.....	269
7.5	Internet Explorer 4.0 .....	271
7.5.1	Einstellung der Proxy-Server .....	271
7.5.2	Zertifikate .....	273
7.5.3	Weitere Sicherheitseinstellungen .....	274
7.5.4	Sicherheitszonen.....	277
7.5.5	Persönliche Einstellungen .....	285
7.6	Internet Explorer 5.0 .....	288
7.6.1	Einstellungen für Verbindungen und Proxy-Server .....	289
7.6.2	Zertifikate und persönliche Einstellungen.....	291
7.6.3	Sicherheitszonen.....	295
7.6.4	Weitere Sicherheitseinstellungen .....	301
<b>8</b>	<b>Telearbeit und Videokonferenzen.....</b>	<b>305</b>
8.1	Einführung .....	305
8.2	Formen der Telearbeit.....	306
8.3	Gefährdungen beim Einsatz von Telearbeit.....	308
8.3.1	Gefährdungen am Telearbeitsplatz.....	309
8.3.2	Gefährdungen bei der Datenübertragung .....	311
8.3.3	Bedrohungen an der Schnittstelle zum LAN.....	312
8.4	Sicherheitsanforderungen beim Einsatz von Telearbeit.....	313
8.4.1	Maßnahmen zur Absicherung der Telearbeitsplätze .....	313
8.4.2	Maßnahmen zum Schutz der Telekommunikationsverbindung .....	314
8.4.3	Maßnahmen zur Absicherung des Zugangs zum Intranet .....	317
8.5	Authentisierung.....	319
8.5.1	Authentisierungsverfahren .....	319
8.5.2	Authentisierungsprotokolle .....	323
8.6	Videokonferenzen .....	326
8.6.1	Bestandteile einer Videokonferenz nach H.323 .....	326
8.6.2	Ablauf einer Videokonferenz nach H.323.....	332
8.6.3	RTP (Real Time Protocol) und RTCP (Real Time Control Protocol).....	335
8.6.4	T.120.....	336
8.6.5	Bedrohungen beim Einsatz von Videokonferenzen .....	341
8.6.6	Sicherheitsmaßnahmen beim Einsatz von Videokonferenzen.....	342
8.6.6.1	Packet-Filter.....	342
8.6.6.2	Einsatz von Verschlüsselungsverfahren .....	343

8.6.6.3	Application-Level-Gateway.....	344
<b>9</b>	<b>Anonymität, Privatsphäre und Recht im Internet .....</b>	<b>347</b>
9.1	Spuren im Internet.....	347
9.1.1	Cookies.....	348
9.1.2	Personal Privacy Preferences (P3P) .....	355
9.2	Anonyme und pseudonyme Nutzung von Internet-Diensten .....	357
9.2.1	Email.....	357
9.2.2	HTTP .....	362
9.3	Rechtliche Aspekte .....	363
<b>10</b>	<b>Electronic Commerce.....</b>	<b>373</b>
10.1	Zahlungssysteme im Internet .....	373
10.1.1	Einführung.....	373
10.1.2	Unterschiede und Gemeinsamkeiten .....	375
10.1.3	Ecash, CAFE und Mondex .....	377
10.1.4	CyberCash und First Virtual.....	380
10.1.5	iKP.....	385
10.1.6	SET .....	387
10.2	Ausführbarer Inhalt (Executable Content).....	392
10.2.1	Allgemeine Gefährdungen beim Einsatz aktiver Inhalte.....	392
10.2.2	Java.....	395
10.2.3	JavaScript .....	404
10.2.4	ActiveX.....	409
10.2.5	Plug-ins, Helper-Applications und MIME-Types .....	412
<b>Anhang</b>	<b>.....</b>	<b>417</b>
I	Adressen.....	417
II	Programme .....	422
III	Notfallplan für einen Angriff aus dem Internet.....	428
IV	Benutzerordnung für die Nutzung des Internet.....	431
V	Glossar .....	436
VI	Literaturverzeichnis .....	444
VII	Stichwortverzeichnis.....	451