

Inhalt

Abbildungsverzeichnis	13
Vorwort zur 2. Auflage	15
Vorwort zur 1. Auflage	15
Über den Autor	17
1 Einleitung	19
2 Was ist Sicherheit?	21
3 Was ist das Internet?	22
3.1 Geschichte	22
3.2 Organisation	23
3.3 Kommunikation	24
3.4 Dienste	25
3.4.1 E-Mail	26
3.4.2 Usenet News	26
3.4.3 File Transport	27
3.4.4 Telnet	27
3.4.5 World Wide Web	28
3.4.6 Real Audio/Real Video	28
3.4.7 Internet Phone	28
3.4.8 Domain Name System	29
3.4.9 Ping und Traceroute	29
4 Wer sind die „Bösen“?	30
5 Was kann passieren?	32
6 Wo sind die Angriffspunkte?	33
7 Schutz der Kommunikation	34
7.1 Vergleich mit sonstiger Kommunikation	35
7.2 Verschlüsselung	35
7.2.1 Geschichte	35
7.2.2 Technische Grundlagen	36
7.2.3 Ausgewählte Verschlüsselungsalgorithmen	37
7.2.3.1 Symmetrische Verschlüsselungsalgorithmen	37
7.2.3.2 Asymmetrische Verschlüsselungsalgorithmen	38
7.3 Einsatzgebiete	39
7.4 Programmbeispiele	41

7.4.1	PGP	41
7.4.2	Secure Web-Server	42
7.4.3	Secure Shell	43
7.5	Certification Authorities	43
7.6	Rechtslage zur Verschlüsselung und elektronischen Unterschrift	44
8	Schutz der Rechner und des eigenen Rechnernetzwerkes	46
8.1	Wann wird eine Firewall benötigt?	47
8.2	Technische Grundlagen	47
8.2.1	Adressierung	48
8.2.2	TCP versus UDP	49
8.2.3	ICMP	50
8.2.4	Protokollbeispiele	50
8.2.4.1	Domain Name System	50
8.2.4.2	Simple Mail Transfer Protocol	50
8.2.4.3	Net News Transfer Protocol	51
8.2.4.4	Telnet	51
8.2.4.5	File Transport Protocol	51
8.2.4.6	Hyper Text Transfer Protocol und Secure Socket Layer	53
8.2.4.7	Real Audio	53
8.2.5	IP-Filter	53
8.2.6	Network Address Translation	54
8.2.7	Proxies	55
8.2.8	Vor- und Nachteile von IP-Filtering, Dynamic Filtering und Proxies	56
8.2.9	RFC 1918	57
8.3	Philosophische Grundlagen	58
8.4	Betriebssysteme	59
8.5	Architekturbeispiele für Firewalls	60
8.6	Komplexe Architekturen	63
8.7	Redundante Firewalls	65
8.8	Erweiterungsmöglichkeiten	65
8.9	Grenzen	67
8.9.1	Executable Content	67
8.9.1.1	Java	67
8.9.1.2	ActiveX	69
8.9.2	Viren	70
8.9.3	Trojaner	71
8.9.4	Was macht die verwendete Software?	72
8.9.5	Denial-of-Service-Attacken	73
8.10	Beurteilungskriterien	76
8.11	Firewall-Produkte	77
8.11.1	TIS Toolkit	77
8.11.2	Netscreen	79

8.11.3 Private Internet eXchange	79
8.11.4 Checkpoint	80
8.12 Was ist, wenn ...?	81
9 Virtual Private Networks	83
9.1 Netztopologie	83
9.2 Ausbaustufen von VPNs	85
9.3 Protokoll IPsec	86
9.4 Produkte	87
9.4.1 Cisco	87
9.4.2 Checkpoint Firewall 1	87
9.4.3 Secure Shell (SSH)	88
10 WWW-Server	89
10.1 Positionierung des WWW-Servers	89
10.2 Sicherheit des WWW-Servers	91
10.3 Secure-Server	91
10.4 Angriffsszenarien	92
11 Konfiguration am Beispiel typischer Firmen	96
11.1 Elektronikvertrieb Emil	96
11.2 Anlageberatung Aktienfondus	97
11.3 Krankenanstalt Königshügel	98
11.4 Versicherungsgesellschaft Vielfalt	99
11.5 Reiseveranstalter Rudi	100
11.6 Ticketservice Theaterspaß	102
11.7 Weitere Anforderungen	104
11.7.1 Standleitungen zu anderen Niederlassungen	104
11.7.2 Modemverbindungen zu anderen Niederlassungen	104
11.7.3 Austausch von beliebigen Daten	105
11.7.4 Diverse Modems	105
11.7.5 Wartungszugänge	106
11.7.6 Anbindung von Partnern	107
11.7.7 Abschottung des internen Netzwerks	108
11.7.8 Andere Netzwerkprotokolle	108
12 Konfiguration am Beispiel weitverbreiteter Produkte	110
12.1 Cisco Router	110
12.2 Netscreen Firewall	113
12.3 Cisco PIX	114
12.4 Checkpoint Firewall 1 auf Nokia	115
13 Organisatorische Maßnahmen	117
13.1 Vorgangsweise bei einer Firewall-Installation	117

13.1.1	Erstellung einer Sicherheitspolitik	117
13.1.2	Checkliste	119
13.1.3	Entscheidung für ein Produkt	120
13.1.4	Installation und Konfiguration von Firewall und Router	121
13.1.5	Überprüfung der Sicherheitseinrichtungen	121
13.2	Schulung des Sicherheitsverantwortlichen	121
13.3	Benutzungsrichtlinien	122
13.4	Notfallplan	126
13.5	Schulung aller Mitarbeiter	127
13.6	Erkennen von Einbruchversuchen	128
13.7	Laufende Wartung	129
13.8	Regelmäßige Checks	130
13.9	Dokumentation	131
14	Schutz der Privatsphäre	133
14.1	In der eigenen Organisation	133
14.2	Beim eigenen Internet Service Provider	133
14.3	E-Mail	134
14.4	WWW-Proxy	134
14.5	Bei anderen Internet Service Providers	134
14.6	News	135
14.7	WWW-Server	135
14.8	Cookies	135
15	Intranet	137
15.1	Topologie des Intranets	137
15.2	Interne E-Mail	138
15.3	Interne Newsgroups	138
15.4	Interner Information-Server	139
15.5	WWW als Interface zu internen Applikationen	139
16	Extranet	141
16.1	Electronic Commerce	141
16.2	E-Mail	141
16.3	WWW-Server	141
17	Ausfallssicherheit der Netzanbindung	142
18	Mobile Computing	144
19	Zahlungsverkehr	145
19.1	Was ist Bezahlung?	145
19.2	Wie funktioniert Bezahlung derzeit?	145
19.3	Besonderheit der Bezahlung im Internet	146

19.4 Anforderungen an die Bezahlung im Internet	147
19.4.1 Übertragungssicherheit	147
19.4.2 Wertsicherheit	148
19.4.3 Nachvollziehbarkeit	148
19.4.4 Anonymität	148
19.4.5 Einfachheit und weite Verbreitung	149
19.4.6 Geringe Kosten	149
19.5 Bestehende Möglichkeiten	149
19.5.1 Bezahlung außerhalb des Netzes	149
19.5.2 Nachbildung bestehender Systeme	150
19.5.3 Elektronisches Geld	151
19.6 Zukunftsaussichten	151
19.6.1 Kleinstbeträge	152
19.6.2 Kleinbeträge	152
19.6.3 Mittlere Beträge	152
19.6.4 Hohe Beträge	152
19.7 Beispiele	152
19.7.1 Secure Electronic Transaction (SET)	153
19.7.2 DigiCash	154
20 Telebanking	156
21 Allgemeine Rechtslage	159
21.1 Grundlagen	159
21.1.1 E-Mail	160
21.1.2 Mailing-Listen	161
21.1.3 News	161
21.1.4 WWW und FTP	163
21.1.5 Real Audio/Real Video	164
21.1.6 Internet Phone/CU See Me	164
21.2 Derzeitige Situation	165
21.2.1 Domain-Namen	165
21.2.2 Telekommunikation	166
21.2.3 Verschlüsselung	166
21.2.4 Elektronische Unterschrift	167
21.2.5 Urheberrecht	170
21.2.6 Vertragsrecht	170
21.2.7 Strafrecht	170
21.2.8 Sonstiges	171
22 Diverses zur Sicherheit	172
22.1 Einzelne Rechner im Netz	172
22.2 Passwörter	172
22.3 Lockscreen	173

22.4 Backups	173
22.5 Social Engineering	173
22.6 Chipkarten	174
22.7 Zukünftige Entwicklungen	175
23 Wichtiges zum Internet	177
23.1 Was ist ein guter Provider?	177
23.2 E-Mail-Adressen	178
23.3 Domain Names	180
23.3.1 Abfragen	180
23.3.2 Struktur	181
23.3.3 Registrierung und rechtliche Aspekte	182
23.4 Registrierungsstellen	183
23.5 Traffic Shaping	183
23.6 IPv6	184
23.7 Netiquette	185
23.8 Spam Mails	185
24 Zukunftsaussichten des Internets	187
24.1 Technisch	187
24.1.1 Kurzfristig	187
24.1.2 Langfristig	187
24.2 Organisatorisch	188
25 Zusammenfassung und Schlusswort	189
Anhang 1: Die Grünberg & Waxmann Story	190
Anhang 2: NetzMayer, die deutsche Übersetzung der Netiquette	200
Anhang 3: Liste der Portnummern	209
Anhang 4: Glossar	224
Anhang 5: Verzeichnis wichtiger URLs	234
Anhang 6: Index	235