

# Inhalt

Vorwort	7
Über den Autor	8
Abbildungsverzeichnis	15
<b>1 Einleitung</b>	<b>17</b>
<b>2 Was ist Sicherheit?</b>	<b>19</b>
<b>3 Was ist das Internet?</b>	<b>20</b>
3.1 Geschichte	20
3.2 Organisation	21
3.3 Kommunikation	22
3.4 Dienste	23
3.4.1 E-Mail	24
3.4.2 Usenet News	24
3.4.3 File Transport	25
3.4.4 Telnet	25
3.4.5 World Wide Web	26
3.4.6 Real Audio/Real Video	26
3.4.7 Internet Phone	26
3.4.8 Domain Name System	26
3.4.9 Ping und Traceroute	27
<b>4 Wer sind die „Bösen“?</b>	<b>28</b>
<b>5 Was kann passieren?</b>	<b>30</b>
<b>6 Wo sind die Angriffspunkte?</b>	<b>31</b>
<b>7 Schutz der Kommunikation</b>	<b>32</b>
7.1 Vergleich mit sonstiger Kommunikation	33
7.2 Verschlüsselung	33
7.2.1 Geschichte	33
7.2.2 Technische Grundlagen	34
7.2.3 Ausgewählte Verschlüsselungsalgorithmen	35
7.2.3.1 Symmetrische Verschlüsselungsalgorithmen	35
7.2.3.2 Asymmetrische Verschlüsselungsalgorithmen	36
7.3 Einsatzgebiete	37
7.4 Programmbeispiele	39

7.4.1	PGP	39
7.4.2	Secure Web-Server	40
7.4.3	Secure Shell	41
7.5	Certification Authorities	41
7.6	Rechtslage zur Verschlüsselung und elektronischen Unterschrift	42
<b>8</b>	<b>Schutz der Rechner und des eigenen Rechnernetzwerkes</b>	<b>44</b>
8.1	Wann wird eine Firewall benötigt?	45
8.2	Technische Grundlagen	45
8.2.1	Adressierung	46
8.2.2	TCP versus UDP	47
8.2.3	ICMP	48
8.2.4	Protokollbeispiele	48
8.2.4.1	Domain Name System	48
8.2.4.2	Simple Mail Transfer Protocol	48
8.2.4.3	Net News Transfer Protocol	49
8.2.4.4	Telnet	49
8.2.4.5	File Transport Protocol	49
8.2.4.6	Hyper Text Transfer Protocol und Secure Socket Layer	51
8.2.4.7	Real Audio	51
8.2.5	IP-Filter	51
8.2.6	Network Address Translation	52
8.2.7	Proxies	53
8.2.8	Vor- und Nachteile von IP-Filtering, Dynamic Filtering und Proxies	54
8.2.9	RFC 1918	55
8.3	Philosophische Grundlagen	56
8.4	Betriebssysteme	57
8.5	Architekturbeispiele für Firewalls	58
8.6	Erweiterungsmöglichkeiten	61
8.7	Grenzen	62
8.7.1	Executable Content	62
8.7.1.1	Java	63
8.7.1.2	ActiveX	64
8.7.2	Viren	65
8.7.3	Was macht die verwendete Software?	67
8.7.4	Denial-of-Service-Attacken	68
8.8	Beurteilungskriterien	70
8.9	Firewall-Produkte	72
8.9.1	TIS Toolkit	72
8.9.2	AltaVista	74
8.9.3	Checkpoint	74
8.9.4	Private Internet eXchange	75
8.10	Was ist, wenn ...?	75

---

<b>9 Virtual Private Networks</b>	<b>77</b>
9.1 Netztopologie	77
9.2 Ausbaustufen von VPNs	79
9.3 Produkte	80
9.3.1 Cisco	81
9.3.2 Checkpoint Firewall 1	81
9.3.3 AltaVista Tunnel	81
<b>10 WWW-Server</b>	<b>83</b>
10.1 Positionierung des WWW-Servers	83
10.2 Sicherheit des WWW-Servers	85
10.3 Secure-Server	85
10.4 Angriffsszenarien	86
<b>11 Konfiguration am Beispiel typischer Firmen</b>	<b>90</b>
11.1 Elektronikvertrieb Emil	90
11.2 Anlageberatung Aktienfondus	91
11.3 Krankenhaus Königshügel	92
11.4 Versicherungsgesellschaft Vielfalt	93
11.5 Reiseveranstalter Rudi	94
11.6 Ticketservice Theaterspaß	96
11.7 Weitere Anforderungen	98
11.7.1 Standleitungen zu anderen Niederlassungen	98
11.7.2 Modemverbindungen zu anderen Niederlassungen	99
11.7.3 Austausch von beliebigen Daten	99
11.7.4 Diverse Modems	100
11.7.5 Wartungszugänge	100
11.7.6 Andere Netzwerkprotokolle	101
<b>12 Konfiguration am Beispiel weitverbreiteter Produkte</b>	<b>103</b>
12.1 Cisco Router	103
12.2 Cisco PIX	106
12.3 Checkpoint Firewall 1	107
12.4 AltaVista Firewall	109
12.5 AltaVista Tunnel	110
<b>13 Organisatorische Maßnahmen</b>	<b>112</b>
13.1 Vorgangsweise bei einer Firewall-Installation	112
13.1.1 Erstellung einer Sicherheitspolitik	112
13.1.2 Checkliste	112
13.1.3 Entscheidung für ein Produkt	114
13.1.4 Installation und Konfiguration von Firewall und Router	114
13.1.5 Überprüfung der Sicherheitseinrichtungen	115

13.2 Schulung des Sicherheitsverantwortlichen	115
13.3 Benutzungsrichtlinien	116
13.4 Schulung aller Mitarbeiter	118
13.5 Erkennen von Einbruchversuchen	118
13.6 Laufende Wartung	120
13.7 Regelmäßige Checks	120
<b>14 Schutz der Privatsphäre</b>	<b>122</b>
14.1 In der eigenen Organisation	122
14.2 Beim eigenen ISP	122
14.3 E-Mail	123
14.4 WWW-Proxy	123
14.5 Bei anderen ISP	123
14.6 News	124
14.7 WWW-Server	124
14.8 Cookies	124
<b>15 Intranet</b>	<b>126</b>
15.1 Topologie des Intranets	126
15.2 Interne E-Mail	127
15.3 Interne Newsgroups	127
15.4 Interner Information-Server	128
15.5 WWW als Interface zu internen Applikationen	128
<b>16 Extranet</b>	<b>129</b>
16.1 Electronic Commerce	129
16.2 E-Mail	129
16.3 WWW-Server	129
16.4 Verteilte Datenbanken	130
<b>17 Network Computing</b>	<b>131</b>
<b>18 Mobile Computing</b>	<b>132</b>
<b>19 Zahlungsverkehr</b>	<b>133</b>
19.1 Was ist Bezahlung?	133
19.2 Wie funktioniert Bezahlung derzeit?	133
19.3 Besonderheit der Bezahlung im Internet	134
19.4 Anforderungen an die Bezahlung im Internet	135
19.4.1 Übertragungssicherheit	135
19.4.2 Wertsicherheit	135
19.4.3 Nachvollziehbarkeit	136
19.4.4 Anonymität	136
19.4.5 Einfachheit und weite Verbreitung	137

19.4.6 Geringe Kosten	137
19.5 Bestehende Möglichkeiten	137
19.5.1 Bezahlung außerhalb des Netzes	137
19.5.2 Nachbildung bestehender Systeme	138
19.5.3 Elektronisches Geld	139
19.6 Zukunftsaussichten	140
19.6.1 Kleinstbeträge	140
19.6.2 Kleinbeträge	140
19.6.3 Mittlere Beträge	140
19.6.4 Hohe Beträge	140
19.7 Beispiele	141
19.7.1 Secure Electronic Transaction (SET)	141
19.7.2 DigiCash	142
<b>20 Telebanking</b>	<b>145</b>
<b>21 Allgemeine Rechtslage</b>	<b>148</b>
21.1 Grundlagen	148
21.1.1 E-Mail	149
21.1.2 Mailing-Listen	150
21.1.3 News	150
21.1.4 WWW und FTP	152
21.1.5 Real Audio/Real Video	153
21.1.6 Internet Phone/CU See Me	153
21.2 Derzeitige Situation	154
21.2.1 Telekommunikation	154
21.2.2 Verschlüsselung	155
21.2.3 Elektronische Unterschrift	156
21.2.4 Urheberrecht	157
21.2.5 Vertragsrecht	157
21.2.6 Strafrecht	158
21.2.7 Sonstiges	158
<b>22 Diverses zur Sicherheit</b>	<b>159</b>
22.1 Einzelne Rechner im Netz	159
22.2 Paßwörter	159
22.3 Lockscreen	160
22.4 Backups	160
22.5 Social Engineering	160
22.6 Chipkarten	161
22.7 Zukünftige Entwicklungen	162
<b>23 Wichtiges zum Internet</b>	<b>164</b>
23.1 Was ist ein guter Provider?	164

23.2 E-Mail-Adressen	165
23.3 Domain Names	167
23.3.1 Abfragen	167
23.3.2 Struktur	168
23.3.3 Registrierung und rechtliche Aspekte	169
23.4 InterNIC und RIPE	170
23.5 IPsec	170
23.6 IPv6	170
23.7 Netiquette	171
23.8 Spam Mails	172
<b>24 Zukunftsaussichten des Internets</b>	<b>173</b>
24.1 Technisch	173
24.1.1 Kurzfristig	173
24.1.2 Langfristig	174
24.2 Organisatorisch	174
<b>25 Zusammenfassung und Schlußwort</b>	<b>176</b>
Anhang 1: Informations- und Kommunikationsdienste-Gesetz	177
Anhang 2: Telekommunikationsgesetz	185
Anhang 3: NetzMayer, die deutsche Übersetzung der Netiquette	200
Anhang 4: Liste der Portnummern	209
Anhang 5: Glossar	224
Anhang 6: Verzeichnis wichtiger URLs	234
Anhang 7: Index	235

# Abbildungsverzeichnis

---

Abbildung 1: Verbindungsstruktur	23
Abbildung 2: Asymmetrische Verschlüsselung	36
Abbildung 3: Klassisches FTP	49
Abbildung 4: FTP mit Passive Mode	50
Abbildung 5: IP-Adressen bei NAT	52
Abbildung 6: Architekturbeispiel mit IS zwischen Router und Firewall	58
Abbildung 7: Architekturbeispiel mit IS am Router	59
Abbildung 8: Architekturbeispiel mit IS an der Firewall	60
Abbildung 9: Anschluß eines Firmennetzes	69
Abbildung 10: Topologie von VPN	78
Abbildung 11: Position des WWW-Servers	83
Abbildung 12: Netzwerkstruktur für Beispielskonfiguration	103
Abbildung 13: Topologie des Intranets	127
Abbildung 14: Ablauf einer SET-Bezahlung	142
Abbildung 15: Ablauf einer DigiCash-Bezahlung	143
Abbildung 16: Server für Telebanking	146
Abbildung 17: Datenfluß bei E-Mail	149
Abbildung 18: Austausch von News	151
Abbildung 19: Datenfluß bei WWW	152
Abbildung 20: Ablauf einer DNS-Abfrage	167
Abbildung 21: Struktur von Telekabelnetzen	173