Inhaltsverzeichnis

Über die Autoren 5

Übersicht 15

Vorwort 19

1 **Einleitung: Gesellschaftlicher Wandel und IT-Sicherheit** 21
1.1 Entwicklung von Informationstechnologie und IT-Sicherheit 21
1.2 Siegeszug des Internet 24
1.3 Allgemeine Bedrohungen aus dem Internet 26
1.4 Notwendigkeit von IT-Sicherheit 26
1.5 IT-Sicherheit als Wirkungs- und Handlungszusammenhang 29
1.6 Chancen und Risiken der Informationstechnik 31
1.7 Der VPN-Markt 33
1.8 Fazit 35

2 **Notwendigkeiten, Ziele und Anwendungsformen von VPN-Systemen** 37
2.1 Idee und Definition von VPNs 37
2.2 Analogien 38
2.3 Moderne IT-Konzepte und IT-Sicherheit 40
2.4 Corporate Network versus öffentliche Kommunikationsinfrastruktur 41
2.5 Zielsetzung eines VPN 44
2.6 Anwendungsformen von VPNs 45

3 **Bedrohungen im Netz** 49
3.1 Angriffsmöglichkeiten in Kommunikations-Systemen 50
3.1.1 Passive Angriffe 50
3.1.2 Zufällige Verfälschungsmöglichkeiten 57
3.2 Weitere Aspekte potentieller Bedrohungen bei Internet-Kommunikation 59
3.2.1 Angriffstools aus dem Internet 60
3.2.2 Implementierungsfehler in Anwendungen und fehlerhafte Konfigurationen 61

3.2.3 Echelon 61
3.3 Wie hoch ist das Risiko? 62
3.4 Schadenskategorien und Folgen 63
3.4.1 Verstoß gegen Gesetze/Vorschriften/Verträge 63
3.4.2 Beeinträchtigung der persönlichen Unversehrtheit 64
3.4.3 Beeinträchtigung der Aufgabenerfüllung 64
3.4.4 Negative Außenwirkung 65
3.4.5 Finanzielle Auswirkungen 65
3.5 Ergebnisse der KES/Utimaco-Studien 65
3.6 Zusammenfassung 66

4 Grundlegende Sicherheitsmechanismen 67
4.1 Sicherheitsmechanismen für Verschlüsselung und Digitale Signatur 67
4.1.1 Private-Key-Verfahren 67
4.1.2 Public-Key-Verfahren 68
4.1.3 One-Way-Hashfunktion 70
4.1.4 Hybride Verschlüsselungstechnik 71
4.1.5 Ein Wettlauf um die Sicherheit 71
4.1.6 Zertifizierungs-Systeme 72
4.1.7 Chipkarte (SmartCard) 79
4.2 Kryptographische Algorithmen 82
4.2.1 Einführung 82
4.2.2 Symmetrische Verschlüsselungs-Verfahren 86
4.2.2.1 Data Encryption Standard (DES) 86
4.2.2.2 Triple-DES 88
4.2.2.3 International Data Encryption Algorithm (IDEA) 90
4.2.2.4 Blowfish 92
4.2.2.5 RC4 und RC5 93
4.2.2.6 Advanced Encryption Standard (AES) 94
4.2.3 Asymmetrische Verschlüsselungs-Verfahren 97
4.2.3.1 Diffie-Hellman 97
4.2.3.2 RSA 99
4.2.3.3 ElGamal und DSA 103
4.2.4 Hash-Verfahren 104
4.2.4.1 Message Digest 4 (MD4) 105
4.2.4.2 Message Digest 5 (MD5) 106

4.2.4.3 Secure Hash Algorithm (SHA) 107
4.2.4.4 HMAC 109
4.3 Infrastruktur von Zertifizierungs-Systemen 111
4.3.1 X.509-Zertifikate 112
4.3.2 Pretty Good Privacy (PGP) 117
4.3.3 Verzeichnisdienste und das LDAP-Protokoll 119

5 Konzepte von Virtual Private Networks 121
5.1 Ein VPN-Sicherheitssystem als transparente Lösung 121
5.1.1 Black-Box-Lösung 122
5.1.2 Security Sublayer im Endgerät: End-to-End-Verschlüsselung 124
5.1.3 Sicherheit in LAN-Segmenten 125
5.1.4 Kopplung von LAN-Segmenten mit einer Security Bridge 127
5.1.5 Kopplung von LAN-Segmenten über öffentliche Netze 129
5.1.6 Bildung von kryptographisch gesicherten logischen Netzen (VPN) 132
5.1.7 VPN-Client 132
5.1.8 Anwendungsfälle 134
5.2 Topologien von VPNs 136
5.2.1 Die 1:1-Topologie 137
5.2.2 Die 1:n-Topologie 138
5.2.3 Die m:n-Topologie 139
5.3 Sicherheitsmanagement für VPN-Systeme 140
5.3.1 Anforderungen an ein Sicherheitsmanagement 140
5.3.2 Systeme zum Sicherheitsmanagement 143
5.3.3 Zertifizierungs-Systeme 145
5.3.4 Directory-Service 148
5.3.5 Schlüssel-Management 150

6 VPN-Verfahren 151
6.1 VPN-Protokolle 151
6.1.1 IPSec 151
6.1.2 Point-to-Point Tunneling Protocol (PPTP) 159
6.1.3 Secure Shell (SSH) 161
6.2 Schlüsselaustausch – Methoden/Protokolle 165
6.2.1 Pre-Shared key 166
6.2.2 Simple Key Management for Internet Protocols (SKIP) 167
6.2.3 Internet Key Exchange (IKE) 171
6.2.4 Schlüsselaustausch bei SSH 174

7 Praktischer Einsatz von Virtual Private Networks 177
7.1 Fallstudien 177
7.1.1 Sichere Ankopplung von Außendienstmitarbeitern eines Versicherungsunternehmens 177
7.1.2 Vertrauenswürdige Kommunikation über ein internationales IP-Netzwerk 179
7.1.3 Angebot eines vertrauenswürdigen IP-Netzes durch einen Service Provider 181
7.1.4 Vertrauenswürdige Vernetzung von Polizeidienststellen 183
7.2 VPN-Implementierungen 184
7.2.1 FreeSWAN unter Linux 185
7.2.2 Checkpoint Firewall-1 187

8 VPNs für E- und M-Business 195
8.1 Geschäftsabwicklung über Netzwerke 195
8.2 Risiken von E- und M-Business ohne VPN 196
8.2.1 Internet-Zugang über PC 196
8.2.2 Kommunikation über Mobiltelefon 197
8.2.3 Internet-Zugang über Mobiltelefon 198
8.2.4 Fazit 199
8.3 VPN-Systeme zum E-Commerce 199
8.4 Das »Jedermann-VPN« 200
8.5 Protokolle im E- und M-Business 201
8.5.1 Secure Socket Layer (SSL) 202
8.5.2 Wireless Application Protocol (WAP) 204
8.5.3 Secure Electronic Transaction (SET) 207

9 VPN-Sicherheitspolitik und weitere Sicherheitsmaßnahmen 209
9.1 VPN-Sicherheitspolitik 209
9.1.1 Sicherheitsziele 210
9.2 Zusätzliche Sicherheitsmaßnahmen 210
9.2.1 Infrastruktur 211
9.2.2 Organisation 212
9.2.3 Personal 216
9.2.4 Notfall 219

10 VPN: Eine Investition für die Zukunft 221
10.1 Total Cost of Ownership 221
10.1.1 Beschaffungsphase eines VPN 221
10.1.2 Aufrechterhaltung des Betriebs eines VPN 224
10.1.3 Zusammenfassung aller Kosten im Sinne der Total Cost of Ownership 227
10.2 Kosten-Nutzen-Betrachtung im Hinblick auf die Sicherheit 227
10.3 Wahrscheinlichkeit eines bestimmten Profits 228
10.4 Kosten-Nutzen-Betrachtung im Hinblick auf die Kommunikation . 230
10.5 Kosten-Nutzen-Betrachtung im Hinblick auf die Nicht-Realisierung von Kommunikation 232

11 Evaluierung und Zertifizierung von VPNs 233
11.1 ITSEC-Zertifizierung 234
11.2 Wirksamkeit von VPN-Sicherheitsmechanismen 240

12 VPN-Systeme versus Firewall-Systeme 245
12.1 Die Idee von Firewall-Systemen 245
12.2 Grundsätzliche Unterschiede von VPN- und Firewall-Systemen ... 247
12.3 Kombinationen von VPN- und Firewall-Systemen 249
12.3.1 VPN-System vor einem Firewall-System 249
12.3.2 VPN-System vor einem Firewall-System, dahinter ein weiteres VPN-System 250
12.3.3 VPN-System hinter einem Firewall-System 251
12.3.4 VPN- und Firewall-System zusammen realisiert 252
12.3.5 VPN- und Firewall-System parallel 253
12.4 Grundelemente von Firewall-Systemen 254
12.4.1 Packet Filter 254
12.4.2 Zustandsorientierte Packet Filter (stateful inspection) 267
12.4.3 Application Gateway / Proxy-Technik 270
12.4.4 Proxies 274
12.4.5 Adaptive Proxy 291
12.4.6 Anwendungsgebiete von Application Gateways 293
12.4.7 Firewall-Elemente und das Verhältnis von Geschwindigkeit zu Sicherheit 294
12.4.8 Unterschiedliche Firewall-Konzepte 294

13 Weiterführende Aufgabenstellungen bei VPN-Systemen 297
13.1 Verfügbarkeit 297
13.2 Redundanzsysteme 297
13.2.1 Parallele VPN-Gateways 298
13.2.2 Passives Redundanzsystem 298
13.2.3 Aktives Redundanzsystem 298
13.2.4 Redundanzsystem im »Spanning Tree« 299
13.3 Realisierungsformen für VPN-Gateways 300
13.3.1 VPN-Realisierung im Router 300
13.3.2 VPN-Gateways als separate Sicherheitskomponenten 300
13.4 Verwaltung großer VPN-Netzwerke 301
13.5 Zukünftige Entwicklungen bei VPN-Systemen 306

A Computerkriminalität – Fakten und Zahlen 309
A.1 Kriminalitätsstatistik des BKA 309
A.2 Schätzungen der Schadenshöhe 312
A.3 Fallbeispiele 313

B Recht im Internet 319
B.1 Aktuelle Formen des Delikts »Computerkriminalität« 319
B.1.1 Persönlichkeitsrechtsverletzungen 320
B.1.2 Wirtschaftsdelikte 320
B.1.3 Sonstige Delikte 322
B.2 Rechtsfragen 322
B.3 Paradigmenwechsel und Perspektiven 323
B.4 Zusammenfassung 326

C TCP/IP-Technologie für Internet und Intranet 327
C.1 Von den Anfängen bis heute 327
C.2 Vorteile der TCP/IP-Technologie 329
C.3 Das OSI-Referenzmodell 330
C.4 TCP/IP-Protokollarchitektur 332
C.5 Internet-Adressen 334
C.6 Die Kommunikationsprotokolle 337
C.6.1 IP-Protokoll 337
C.6.2 Routing Protokolle 339
C.6.3 ICMP 340
C.6.4 Portnummern 343

C.6.5 UDP ... 344
C.6.6 TCP ... 345
C.6.7 DNS ... 347
C.6.8 Telnet ... 348
C.6.9 FTP ... 349
C.6.10 SMTP ... 349
C.6.11 HTTP ... 350
C.6.12 NNTP ... 351

D Wichtige Adressen und Web-Links 353
D.1 Adressen zur Informationssicherheit ... 353
D.2 CERT ... 354
D.3 Informationen zu VPNs im Internet ... 355

E VPN-Anbieterverzeichnis ... 357

F Literaturverzeichnis ... 359

G Glossar, Abkürzungen ... 367

H Legende ... 391

Stichwortverzeichnis ... 395