Inhaltsverzeichnis

Einleitung 13

Teil I: Einführung 15

1 Betriebliche Anforderungen an die Informationssicherheit 17

1.1 Warum ist Informationssicherheit immer noch ein Thema? 17

1.1.1 Dezentralisierte Datenverarbeitung und Datenkommunikation schaffen neue Gefahren 19

1.1.2 Wie hoch ist das Sicherheitsbewußtsein? 23

1.2 Welche Informationen müssen wogegen geschützt werden? 24

1.3 Realisierung der Informationssicherheit 26

1.4 BSI-Empfehlungen für den PC-Einsatz 27

1.5 Beurteilung der Sicherheit von Lösungen 29

2 Grundlagen der Informationssicherheit 31

2.1 Einführung in die Kommunikationssicherheit 31

2.1.1 Risiko »Öffentliche Netze« 31

2.1.2 Wer könnte an Informationen interessiert sein? 33

2.1.3 Wie greifen Hacker im Internet an? 35

2.1.4 Wie kann man sich schützen? 35

2.2 Einführung in die Verschlüsselung 38

2.2.1 Kryptoanalyse 38

2.2.2 Wozu dient Verschlüsselung? 40

2.2.3 Manche Staaten möchten mitlesen können 46

2.2.4 Symmetrische oder asymmetrische Algorithmen 47

2.3 Symmetrische Verschlüsselung 48

2.3.1 DES 48

2.3.2 Triple-DES 50

2.3.3 IDEA 51

2.3.4 US-Export-Regelung 51

2.4 Asymmetrische Verschlüsselung (RSA) 52

2.4.1 Die Schlüsselanzahl entscheidet über die Bedienbarkeit 52

2.4.2 Verschlüsseln, Authentisieren, Signieren mit RSA 54

2.5 SKIP 55

2.6 GSS-API 57

2.7 Die digitale Signatur 59

2.7.1 Verbindliche Geschäftsvorgänge durch digitale Signaturen 61

2.7.2 Ablauf der digitalen Signatur 62
2.7.3 Geheime und öffentliche Schlüssel des Public-Key-Verfahrens 63
2.7.4 Die Prüfsumme (Hash) sorgt für Datenintegrität 65
2.7.5 Die Public-Key-Infrastructure (PKI) 66
2.7.6 Pretty Good Privacy (PGP) 72
2.8 Verfahren, die den Zahlungsverkehr schützen 73
2.9 World-Wide-Web-Sicherheit 74
2.10 Firewall-Systeme 75
2.11 SmartCards 77
2.11.1 SmartCards müssen personalisiert werden 78
2.11.2 SmartCard-Management und -Wartung 79
2.11.3 SmartCard-Leser 81

Teil II: Praxisbeispiele 83

3 Sicherheit für das globale Netzwerk einer Bank 87
3.1 Die Anwendung 87
3.2 Sicherheitskonzept 88
3.3 Die Sicherheitslösung 90
3.4 Administration der SmartCards 94
3.5 Praxis der sicheren Anwendung 94

4 Remote Access auf zentrale Daten via Internet 95
4.1 Die Anwendung 95
4.2 Das Sicherheitskonzept 96
4.3 Die Sicherheitslösung 97
4.4 Praxis der sicheren Anwendung 100

5 Remote Access auf zentrale Daten via ISDN 103
5.1 Die Anwendung 103
5.2 Das Sicherheitskonzept 104
5.3 Die Sicherheitslösung 105
5.4 Die Praxis der sicheren Anwendung 108

6 Sicherer Zahlungsverkehr bei der Schweizer Post 109
6.1 Die Anwendung 109
6.2 Das Sicherheitskonzept 109
6.3 Die Sicherheitslösung 111
6.4 Praxis der sicheren Anwendung 116

7 Sicherer Informationsverbund Bonn-Berlin 117
7.1 Die Anwendung 117
7.2 Das Sicherheitskonzept 119

7.3 Die Sicherheitslösung 120
7.3.1 Sichere Kopplung des eigenen Intranets an das Internet 122
7.3.2 Internet-Server 124
7.3.3 Intranet-Sicherheit 125
7.3.4 Höhere End-to-End-Sicherheit 127
7.3.5 Abschottung von Organisationseinheiten untereinander 128
7.3.6 Skalierbare Sicherheit 128
7.3.7 Externe Anbindung und Heimarbeitsplätze 129
7.4 Virengefahr 130
7.4.1 Integration von Virenscannern am Common Point of Trust 131
7.4.2 Weitere technische, personelle und organisatorische Sicherheitsmaßnahmen 134

8 Digitales Signatursystem bei der EU-Kommission 135
8.1 Die Anwendung 136
8.2 Das Sicherheitskonzept 136
8.3 Die Sicherheitslösung 137
8.4 Praxis der sicheren Anwendung 140

9 Sicheres Electronic Banking in Belgien 141
9.1 Die Anwendung 141
9.2 Das Sicherheitskonzept 142
9.3 Die Sicherheitslösung 145
9.4 Die Praxis der sicheren Anwendung 147

10 Windows NT – Sicherheit bei der Dresdner Bank 149
10.1 Sichere PCs und Notebooks unter Windows NT 4.0 150
10.2 Das Sicherheitskonzept 151
10.3 Die Sicherheitslösung 153
10.3.1 Wie schützt SafeGuard Easy? 153
10.3.2 Wie wird SafeGuard Easy installiert? 155
10.4 Die Praxis der sicheren Anwendung 156

11 Sichere Netzwerke durch starke Authentisierung in einer schwedischen Bank 159
11.1 Sichere Authentisierung im Netz 159
11.2 Das Sicherheitskonzept 160
11.3 Die Sicherheitslösung 160
11.3.1 Ausgabe von SmartCards und Zertifikaten 162
11.3.2 Benutzer-Authentisierung 165
11.3.3 Schneller Benutzerwechsel 167
11.3.4 CryptWare-Toolkit 168

11.3.5 SafeGuard Advanced Security für Windows NT 168
11.3.6 SafeGuard LAN Crypt 169
11.3.7 Installation 171
11.4 Die Praxis der sicheren Anwendung 171

Teil III: Gesetzliche Regelungen, technische Normen 173

12 Strafgesetzbuch 175

13 Datenschutzgesetze 177
13.1 Das Bundesdatenschutzgesetz (BDSG) 178
13.2 Maßnahmen zur Realisierung der Forderungen des BDSG 179

14 Das Signaturgesetz (SigG) 183
14.1 Sicherheit durch Kryptografie 184
14.1.1 Darstellung von Dokumenten, Korrektheit des Verfahrens 185
14.1.2 Anforderungen des SigG und der SigV an die digitale Signatur 185
14.2 Zertifizierungsstellen 186
14.3 Internationale Anerkennung digitaler Signaturen 187

15 Kriterien zur Prüfung und Bewertung der Sicherheit von IT-Systemen 189
15.1 BSI-Gesetz 190
15.2 ITSEC 191
15.3 Common Criteria 192

16 Die Kryptokontroverse 195
16.1 Krypto-Reglementierungen 196
16.1.1 Reglementierungen beim Einsatz von Kryptografie im internationalen Vergleich 197
16.1.2 Argumente gegen eine Kryptoregulierung 197
16.1.3 Das Fernmeldeverkehr-Überwachungsgesetz (FÜV) 199
16.1.4 Import/Export-Regulierungen für Kryptografie 199

17 Normen und Standards der Informationssicherheit 203
17.1 Protokolle zur Sicherung der Netzwerkebene 204
17.1.1 SSL 204
17.1.2 IPSEC 206
17.1.3 SKIP 207
17.1.4 GSS 207
17.2 Protokolle zur Sicherung der Anwendungsebene 209
17.2.1 SHTTP 209
17.2.2 SET 209
17.2.3 S/MIME 212

17.2.4 MailTrust 212
17.2.5 ISAKMP 213

A Glossar 215

B Adressen, Literaturhinweise 237

B.1 Adressen 237
B.1.1 Wurzelinstanz, Oberste Zertifizierungsstelle 237
B.1.2 Oberste Zertifizierungsstelle für Betriebssysteme, technische Komponenten, Zertifizierungsstellen 237
B.1.3 CERT in Deutschland 237
B.1.4 Virus Center 238
B.1.5 Firewall-Mailing-Liste 238
B.1.6 Nützliche Internet-Adressen 238
B.1.7 Anbieter der beschriebenen Sicherheitslösungen 238
B.2 Literaturhinweise 239

Stichwortverzeichnis 241