

Inhaltsverzeichnis

1	Einleitung	11
1.1	Warum dieses Buch?.....	11
1.2	Das finden Sie in diesem Buch.....	12
1.3	Das finden Sie auf der CD.....	15
1.4	Konventionen	16
 Teil A		
	Sich der Risiken bewusst werden.....	17
2	Kurze Einführung ins Thema Internet	19
2.1	Eine kurze Geschichte des Internets	19
2.1.1	Vorgeschichte	19
2.1.2	Das ARPANET	20
2.1.3	E-Mail.....	21
2.1.4	Das Internet.....	21
2.1.5	Das World Wide Web	22
2.1.6	Links zur Geschichte des Internet	23
2.2	Wie funktioniert das Internet?	24
2.2.1	Die Verbindung zum Internet	24
2.2.2	IP-Adressen	26
2.2.3	Kommunikation im Internet: TCP/IP	28
2.2.4	Weiterlesen?	34
3	Welche Risiken gibt es?	35
3.1	Das Internet als »Hort des Bösen«?	35
3.2	Von Hackern, Crackern und Script Kiddies	36
3.3	Das Internet und die Privatsphäre	37
3.3.1	Der gläserne Surfer	37
3.3.2	E-Mail.....	38
3.3.3	Geschützte Daten	39
3.4	Gefahren für Ihren Computer	41
3.5	Beim Geld hört der Spaß auf.....	42
3.6	Gefahren für Dritte	43

3.7	Illegale oder unerwünschte Inhalte.....	44
3.7.1	Recht in einem globalen Medium	44
3.7.2	Filtermöglichkeiten.....	45
3.7.3	Weiterführende Links	45
3.8	Vollständige Sicherheit gibt es nicht.....	46
4	Viren, Würmer, Trojanische Pferde	47
4.1	Was ist Malware?	47
4.2	Malware nach Kategorien.....	49
4.2.1	Dateiviren	49
4.2.2	Bootsektorviren	50
4.2.3	Stealth- oder Tarnkappenviren	51
4.2.4	Makroviren	51
4.2.5	Würmer.....	52
4.2.6	Trojanische Pferde.....	56
4.2.7	Hoaxes.....	59
4.3	Durch Viren verursachte Schäden	61
4.4	Virenbefall vorbeugen.....	63
4.5	Linkliste.....	64
5	Angriffe von außen	67
5.1	Netzspione unterwegs.....	68
5.1.1	Portscan	68
5.1.2	Packet Sniffing.....	72
5.1.3	Man-in-the-Middle.....	73
5.2	Denial of Service Angriffe	75
5.2.1	Die »Klassiker«	76
5.2.2	Distributed Denial of Service Angriffe	80
5.3	»Social Engineering«	83
5.3.1	Beispiele für Social Engineering	84
5.3.2	Was tun?	86
5.4	Links zum Weiterlesen	87
6	Kryptographie.....	89
6.1	Was ist Kryptographie?	89
6.1.1	Anforderungen an die Kryptographie	90
6.1.2	Symmetrische Verschlüsselung.....	92
6.1.3	Asymmetrisches Verfahren	93
6.1.4	Hashfunktionen.....	95
6.1.5	Verschlüsselungsstärke	95
6.1.6	Die elektronische Signatur	96
6.2	Secure Socket Layer (SSL)	98
6.3	PKI – Public Key Infrastructure.....	99
6.3.1	Zertifikate	100
6.3.2	Die Trustcenter.....	101

Teil B

Internetsicherheit in der Praxis..... 105

7 Sicherheit beim Surfen im Web 107

7.1	Internet Explorer konfigurieren	107
7.1.1	Regelmäßige Sicherheitsupdates.....	108
7.2	Sicherheitseinstellungen im Browser.....	109
7.2.1	Internet	110
7.2.2	Lokales Intranet	111
7.2.3	Vertrauenswürdige Sites	112
7.2.4	Eingeschränkte Sites	113
7.2.5	Benutzerdefinierte Einstellungen	114
7.3	Sichere Datenübertragung.....	122
7.3.1	SSL im Internet Explorer	122
7.3.2	Die Verwaltung von Zertifikaten im Browser	124
7.4	Wie Sie Spuren hinterlassen	125
7.4.1	... auf dem Rechner	125
7.4.2	... im lokalen Netzwerk	136
7.4.3	... beim Provider	137
7.4.4	... auf Websites	138
7.5	Dateiendownload aus dem Web.....	143
7.5.1	Dateidownload von Webseiten	144
7.5.2	Adware und Spyware	146
7.5.3	Angriff auf die Telefonrechnung: Dialer-Software.....	147
7.6	Unerwünschte Inhalte vermeiden	151
7.6.1	Der Inhaltsratgeber.....	151
7.6.2	Weitere Filtersysteme für Websites	157
7.6.3	Andere Filter-Software	162

8 E-Mail..... 165

8.1	Privatsphäre bei E-Mails schützen.....	166
8.1.1	Zertifikate einrichten.....	167
8.1.2	E-Mail digital signieren	174
8.1.3	E-Mail verschlüsseln.....	180
8.1.4	Zertifikate sperren lassen.....	182
8.1.5	Nützliche Links	183
8.2	Virengefahr durch E-Mail.....	184
8.2.1	Risikofaktor E-Mail-Attachments.....	184
8.2.2	Risikofaktor HTML-Format.....	186
8.2.3	Sicherheitseinstellungen Outlook Express und Outlook	188
8.2.4	Dateinamenerweiterungen anzeigen lassen.....	192
8.3	Spam und Junk-E-Mail	194
8.3.1	Spam reduzieren	194
8.3.2	Spam blockieren	196

9	Sicher Einkaufen im Internet.....	199
9.1	Online-Shopping – bequem und sicher?	199
9.2	Worauf Sie achten sollten	200
9.2.1	Der erste Eindruck.....	200
9.2.2	Sichere Datenübertragung	201
9.2.3	Sicheres System.....	202
9.2.4	Rückgaberecht.....	203
9.3	Zahlungsweisen und -systeme.....	203
9.3.1	Vorkasse	204
9.3.2	Nachnahme.....	204
9.3.3	Rechnung.....	205
9.3.4	Bankeinzug oder Lastschriftverfahren.....	205
9.3.5	Kreditkarte	206
9.3.6	SET – Secure Electronic Transaction.....	206
9.3.7	Paybox – bezahlen per Handy	207
9.3.8	FIRSTGATE Click & Buy	208
9.3.9	Paysafecard – Prepaid-Karte fürs Internet	209
9.4	Gütesiegel für Online-Shops.....	209
9.4.1	Trusted Shops.....	210
9.4.2	EHI – Geprüfter Online-Shop	211
9.4.3	Safe’n Easy	212
9.4.4	TÜV Online Check.....	212
9.4.5	Bonitrus	213
9.4.6	S@fer-shopping	213
9.5	Microsoft Passport	214
9.6	Ein Beispiel aus der Praxis	214
9.7	Die weiteren Aussichten.....	219
10	Sicheres Internetbanking.....	221
10.1	Kurze Begriffsbestimmung	222
10.1.1	Bestandteile des Sicherheitskonzepts	223
10.1.2	Aufgaben des Sicherheitskonzepts.....	224
10.2	Sicherheitsstandards	224
10.2.1	PIN und TAN.....	225
10.2.2	HBCI.....	228
10.3	Und was ist mit Hackern?.....	231
10.4	Tipps für erfolgreiches Online-Banking.....	233
10.4.1	Tipps für die Praxis	233
10.4.2	Die Ausstattung.....	234
11	Sichere Online-Auktionen.....	237
11.1	Kaufen und Verkaufen bei Online-Auktionen	237
11.2	Das Bewertungssystem.....	243

11.3	Zusätzliche Sicherheit	245
11.3.1	Geprüftes Mitglied	245
11.3.2	Versicherung	245
11.3.3	Treuhandservice	246
11.3.4	Sicherheitsvorkehrungen anderer Anbieter.....	247
11.4	Links zu Auktionen	249
12	Weitere Internetdienste.....	251
12.1	Telnet, SSH und SCP	251
12.2	FTP, SFTP und FTPS	252
12.2.1	So funktioniert FTP	252
12.2.2	SFTP und FTPS	254
12.3	Newsgroups.....	255
12.4	Chat	256
12.4.1	Wie funktioniert Chatten?	257
12.4.2	Risiken im Chat.....	258
12.4.3	Links zum Thema Chat	262
12.5	Instant Messaging.....	262
12.5.1	Windows Messenger.....	263
12.5.2	Jabber	266
12.5.3	Links zu Instant Messaging.....	267
12.6	Netmeeting	268
Teil C		
	Ein sicheres System einrichten	271
13	Ein sicheres System	273
13.1	Sicherheitsrelevante Systemeinstellungen.....	273
13.1.1	Dateiendungen	274
13.1.2	Versteckte Dateien.....	276
13.1.3	Die Zuordnung von Dateitypen	278
13.1.4	Sicherheitseinstellungen in MS Office-Anwendungen.....	281
13.1.5	Eigene Makros selbst zertifizieren.....	283
13.2	Datensicherung.....	287
13.2.1	Backup von Datendateien.....	288
13.2.2	Dateien wiederherstellen.....	294
13.2.3	Systemwiederherstellung.....	295
13.3	Passwortsicherheit und Benutzerverwaltung.....	299
13.3.1	Benutzerverwaltung	299
13.3.2	Passwortsicherheit	305
13.4	Verschlüsseltes Dateisystem	305
13.4.1	Ver- und Entschlüsseln von Dateien und Ordnern	307
13.4.2	Wiederherstellen verschlüsselter Daten	309
13.5	Automatische Updates in Windows XP.....	310
13.6	Microsoft Baseline Security Analyzer	314

14 Firewall.....	317
14.1 Was ist eine Firewall?	317
14.1.1 Firewallkomponenten.....	318
14.1.2 Wo die Firewall nicht hilft.....	322
14.2 Internetverbindungsfirewall	323
14.2.1 Einrichtung mit dem Netzwerkinstallations-Assistenten.....	324
14.2.2 Manuelle Einrichtung der IVF	325
14.3 Andere Firewalls.....	329
14.3.1 ZoneAlarm.....	330
14.3.2 Weitere Anbieter	338
14.4 Sicherheitstests.....	339
14.4.1 Portscan	340
14.4.2 NetBIOS-Test	341
14.4.3 Leakttest.....	343
15 Antivirensoftware	345
15.1 Wie arbeitet Antivirensoftware?.....	345
15.2 Vorbeugen und heilen.....	347
15.2.1 AV-Software zur Vorbeugung.....	347
15.2.2 Notfalldiskette erstellen.....	349
15.2.3 Was tun im Infektionsfall?.....	351
15.3 Antivirensoftware – zwei Beispiele	353
15.3.1 AntiVirenKit professional.....	353
15.3.2 AntiVir	360
15.4 Linkliste.....	364
Index	367