

1 Informationen zu diesem Buch	4	9 Standalone-Virenschutz.....	68
1.1 Voraussetzungen und Ziele.....	4	9.1 Einfache Virenprävention	68
1.2 Aufbau und Konventionen	5	9.2 Gängige Antivirus-Software	74
2 Was ist Sicherheit?.....	6	9.3 Computer scannen	76
2.1 Vertraulichkeit.....	6	9.4 Viren entfernen.....	78
2.2 Integrität.....	6	10 Unternehmensweiter Virenschutz	82
2.3 Verfügbarkeit	7	10.1 Client/Server-Konzept von Norton	
3 Risikolage für Unternehmen	8	Antivirus.....	82
3.1 Warum ist das Internet nicht "sicher"?	8	10.2 Installation.....	83
3.2 Schadensmöglichkeiten.....	9	10.3 Konfiguration.....	87
3.3 Überlebenschancen	10	10.4 Überwachen eines Firmennetzwerkes.....	89
4 Angriffsvorbereitung	12	11 IT-Sicherheitsstandards.....	90
4.1 Hacker, Cracker und Script-Kids.....	12	11.1 Standards im Bereich	
4.2 Netzwerkskans	13	Informationssicherheit	90
4.3 Wardialing	18	11.2 IT-Grundschutzhandbuch.....	92
4.4 Wardriving.....	18	11.3 Security Policy.....	93
4.5 Social Engineering	19	12 Symmetrische Kryptografie	94
5 Angriffe auf Server.....	22	12.1 Das Problem von Alice und Bob.....	94
5.1 Exploits.....	22	12.2 Einfache Verschlüsselungsmethoden	96
5.2 Rootkits.....	28	12.3 Symmetrische Verfahren	102
5.3 DoS/DDoS.....	29	13 Asymmetrische Kryptografie	110
5.4 Sniffer	29	13.1 Nachteile von symmetrischen	
5.5 Replay-Attacken	30	Verfahren.....	110
5.6 Hijacking	31	13.2 Einwegfunktion.....	111
6 Sicherheitsprobleme durch		13.3 Diffie-Hellman-Schlüsseltausch	114
Mitarbeiter	32	13.4 El-Gamal.....	115
6.1 Ausfall/Krankheit.....	32	13.5 RSA.....	116
6.2 Hintertürchen	33	13.6 Digitale Signatur	118
6.3 Spionage	34	13.7 Hashfunktionen.....	119
6.4 Mangelnde Kompetenz.....	34	13.8 Schwachstellen in RSA.....	120
7 Virenarten und ihre Verbreitung	36	13.9 Public Key Infrastructure.....	122
7.1 Grundkonzepte von Viren.....	36	14 Kryptografische Protokolle und	
7.2 Virenarten.....	37	deren Anwendung.....	124
7.3 Tarnmechanismen von Viren	43	14.1 SSL/TLS	124
7.4 Würmer.....	49	14.2 SSH	126
7.5 Trojanische Pferde.....	50	14.3 IPSec	127
7.6 Hoaxes.....	51	14.4 SET/HBCI.....	127
7.7 Tendenzen und Ausblick.....	52	15 Sichere E-Mail mit PGP/GnuPG	130
8 Spyware, Phishing und Browser		15.1 Installation.....	130
Hijacking	54	15.2 Schlüssel generieren.....	132
8.1 Geld verdienen im Internet.....	54	15.3 Schlüsselexport und -import	134
8.2 Spyware.....	56	15.4 Signieren von Schlüsseln	137
8.3 Browser Hijacking.....	58	15.5 Revocation Certificates	138
8.4 Was ist Phishing?	60	15.6 E-Mail signieren und verschlüsseln	140
8.5 Anti-Spyware einsetzen.....	62		

16 Firewalls	142	19.3 WEP	172
16.1 Wie Firewalls arbeiten	142	19.4 WPA, WPA2 und 802.11i	174
16.2 Paketfilter-Firewall.....	145	19.5 Funkausleuchtung.....	175
16.3 Stateful Inspection	145	20 Alternative Software	176
16.4 Proxy Level/Application Level	147	20.1 Warum andere Software sinnvoll sein kann	176
16.5 NAT Firewall	148	20.2 Alternative Webbrowser	177
16.6 Personal Firewall	149	20.3 Alternative E-Mail-Clients.....	179
17 Intrusion-Detection-Systeme.....	152	21 Zugangskontrollsysteme.....	182
17.1 Notwendigkeit von Intrusion- Detection-Systemen	152	21.1 NT-LM und Kerberos.....	182
17.2 Arbeitsweise eines IDS	153	21.2 PAP, CHAP, EAP und RADIUS.....	186
17.3 Intrusion-Reaction-System	154	21.3 Smartcards und Tokensysteme	187
17.4 Snort	155	21.4 Biometrie.....	188
17.5 Honeypot-Netzwerke.....	158	22 Proaktive Sicherheit.....	190
18 Virtual Private Network	160	22.1 Defensive Programmierung.....	190
18.1 Zielsetzung	160	22.2 Gehärtete Betriebssysteme.....	191
18.2 PPTP	162	22.3 Patches	192
18.3 L2TP/IPSEC.....	163	22.4 Vulnerability Assessment.....	193
19 WLAN und Sicherheit.....	168	Stichwortverzeichnis	196
19.1 WLAN-Arbeitsweise	168		
19.2 Access-Points	172		