

Bevor Sie beginnen ...	4	7 Spyware, Phishing und Browser-Hijacking	72
		7.1 Geld verdienen im Internet	72
		7.2 Spyware	74
		7.3 Browser-Hijacking	77
		7.4 Was ist Phishing?	78
		7.5 Anti-Spyware einsetzen	81
		7.6 Übung	85
1 Was ist Sicherheit?	6	8 Stand-alone-Virenschutz	86
1.1 Grundforderungen an Sicherheit	6	8.1 Einfache Virenprävention	86
1.2 Sicherheitsziel Vertraulichkeit	6	8.2 Gängige Antimalware-Applikationen	91
1.3 Sicherheitsziel Integrität	7	8.3 Computer scannen	95
1.4 Sicherheitsziel Verfügbarkeit	8	8.4 Viren entfernen	97
1.5 Rechtliche Aspekte	9	8.5 Übung	98
2 Risikolage für Unternehmen	15	9 IT-Sicherheitsstandard	99
2.1 Warum ist das Internet nicht „sicher“?	15	9.1 Standards im Bereich Informationssicherheit	99
2.2 Schadensmöglichkeiten	17	9.2 IT-Grundschutz-Kompendium	99
3 Angriffsvorbereitung	18	9.3 Weitere Kriterienwerke zur IT-Sicherheit	100
3.1 Hacker und Cracker	18	9.4 DIN EN 50600	104
3.2 „Staatliche“ Hacker	19	9.5 Security Policy	104
3.3 Elektronische Kriegsführung	21	9.6 Aufgaben eines IT-Sicherheitsbeauftragten	106
3.4 Netzwerkscans	21	9.7 Übung	106
3.5 Wardriving	26	10 Symmetrische Kryptografie	107
3.6 Social Engineering	27	10.1 Das Problem von Alice und Bob	107
4 Angriffe auf Dienste/Protokolle	30	10.2 Einfache Verschlüsselungsmethoden	109
4.1 Exploits	30	10.3 Symmetrische Verfahren	116
4.2 Rootkits	36	10.4 Übung	126
4.3 DoS/DDoS/DRDoS	38	11 Asymmetrische Kryptografie	127
4.4 Sniffer	40	11.1 Nachteile symmetrischer Verfahren	127
4.5 Replay-Attacken	42	11.2 Einwegfunktion	128
4.6 TCP/IP Session-Hijacking	42	11.3 Diffie-Hellman-Schlüsseltausch	132
4.7 Übung	44	11.4 El-Gamal	133
5 Sicherheitsprobleme durch Mitarbeiter	45	11.5 RSA	134
5.1 Ausfall/Krankheit	45	11.6 Digitale Signatur	137
5.2 Unrechtmäßige Systemzugänge	46	11.7 Hashfunktionen	137
5.3 Spionage	47	11.8 Schwachstellen in RSA	141
5.4 Mangelnde Kompetenz	48	11.9 Public Key Infrastructure	143
5.5 Übung	51	11.10 Übung	146
6 Viren und ihre Verbreitung	52	12 Kryptografische Protokolle und ihre Anwendung	147
6.1 Grundkonzepte von Viren	52	12.1 SSL/TLS	147
6.2 Virenarten	54	12.2 SSH	153
6.3 Tarnmechanismen von Viren	60	12.3 IPsec	155
6.4 Würmer	66	12.4 Übung	156
6.5 Trojaner	67		
6.6 Adware und PUA	70		
6.7 Tendenzen und Ausblick	70		
6.8 Übung	71		

13 Sichere E-Mail-Verfahren	157	17 WLAN und Sicherheit	194
13.1 Grundlagen der E-Mail-Verschlüsselung	157	17.1 WLAN-Arbeitsweise	194
13.2 Schlüssel generieren	159	17.2 Access-Points	198
13.3 Schlüsselexport und -import	161	17.3 WEP – Wired Equivalency Protocol	199
13.4 E-Mail signieren und verschlüsseln	163	17.4 WPA – Wi-Fi Protected Access	200
13.5 Dateien signieren und verschlüsseln	164	17.5 WPA2 – Wi-Fi Protected Access 2	201
13.6 Übung	164	17.6 WPA3 – Wi-Fi Protected Access 3	201
		17.7 Weitere Authentifizierung und Verschlüsselung im WLAN	201
14 Firewalls	165	17.8 Funkausleuchtung	203
14.1 Wie Firewalls arbeiten	165	17.9 Übung	204
14.2 Paketfilter-Firewall	167		
14.3 Stateful Inspection Firewall	169	18 Alternative Software	206
14.4 Proxy Level/Application Level Firewall	170	18.1 Warum Nicht-Standard-Software sinnvoll sein kann	206
14.5 NAT	171	18.2 Alternative Webbrowser	208
14.6 Personal Firewall	172	18.3 Alternative E-Mail-Clients	210
14.7 Sicherheitskonzept Firewall	174		
14.8 Erweiterte Funktionen der Firewall	174	19 Authentifizierungssysteme	213
14.9 Übung	175	19.1 Kerberos	213
		19.2 PAP, CHAP, EAP und RADIUS	217
15 Intrusion-Detection/Prevention-Systeme	176	19.3 Smartcards und Tokensysteme	219
15.1 Notwendigkeit von Intrusion-Detection-Systemen	176	19.4 Biometrie	221
15.2 Arbeitsweise eines IDS	177		
15.3 Auf erkannte Angriffe reagieren	179	20 Proaktive Sicherheit	224
15.4 Intrusion-Prevention-Systeme (IPS)	180	20.1 Defensive Programmierung	224
15.5 Snort	181	20.2 Gehärtete Betriebssysteme	225
15.6 Honeypot-Netzwerke	182	20.3 Patches	227
15.7 Übung	184	20.4 Vulnerability Assessment	229
16 Virtual Private Network	185	Stichwortverzeichnis	236
16.1 Zielsetzung	185		
16.2 PPTP	187		
16.3 L2TP/IPsec	187		
16.4 OpenVPN	192		
16.5 WireGuard	192		
16.6 Abgrenzung zu anderen VPN-Arten	193		
16.7 Übung	193		