Bevor Sie beginnen … 4

1 Was ist Sicherheit? 6
1.1 Grundforderungen an Sicherheit 6
1.2 Sicherheitsziel Vertraulichkeit 6
1.3 Sicherheitsziel Integrität 7
1.4 Sicherheitsziel Verfügbarkeit 8
1.5 Rechtliche Aspekte 9

2 Risikolage für Unternehmen 14
2.1 Warum ist das Internet nicht „sicher“? 14
2.2 Schadensmöglichkeiten 15
2.3 Wie abhängig sind Firmen vom IT-Einsatz? 16

3 Angriffsvorbereitung 18
3.1 Hacker und Cracker 18
3.2 „Staatliche“ Hacker 19
3.3 Elektronische Kriegsführung 21
3.4 Netzwerkscans 21
3.5 Wardriving 27
3.6 Social Engineering 27

4 Angriffe auf Serverdienste 31
4.1 Exploits 31
4.2 Rootkits 37
4.3 DoS/DDoS/DRDoS 39
4.4 Sniffer 40
4.5 Replay-Attacken 42
4.6 TCP/IP Session-Hijacking 42
4.7 Übung 44

5 Sicherheitsprobleme durch Mitarbeiter 45
5.1 Ausfall/Krankheit 45
5.2 Unrechtmäßige Systemzugänge 46
5.3 Spionage 47
5.4 Mangelnde Kompetenz 49
5.5 Übung 51

6 Virenarten und ihre Verbreitung 52
6.1 Grundkonzepte von Viren 52
6.2 Virenarten 54
6.3 Tarnmechanismen von Viren 59
6.4 Würmer 66
6.5 Trojaner 67
6.6 Adware und PUA 69
6.7 Tendenzen und Ausblick 69
6.8 Übung 70

7 Spyware, Phishing und Browser Hijacking 71
7.1 Geld verdienen im Internet 71
7.2 Spyware 73
7.3 Browser Hijacking 76
7.4 Was ist Phishing? 77
7.5 Anti-Spyware einsetzen 80
7.6 Übung 84

8 Stand-Alone-Virenschutz 85
8.1 Einfache Virenprävention 85
8.2 Gängige Antivirensoftware 91
8.3 Computer scannen 95
8.4 Viren entfernen 97
8.5 Übung 98

9 IT-Sicherheitsstandard 99
9.1 Standards im Bereich Informationssicherheit 99
9.2 IT-Grundschutz-Kompendium 99
9.3 Weitere Kriterienwerke zur IT-Sicherheit 100
9.4 DIN EN 50600 103
9.5 Security Policy 104
9.6 Aufgaben eines IT-Sicherheitsbeauftragten 105
9.7 Übung 106

10 Symmetrische Kryptografie 107
10.1 Das Problem von Alice und Bob 107
10.2 Einfache Verschlüsselungsmethoden 109
10.3 Symmetrische Verfahren 116
10.4 Übung 125

11 Asymmetrische Kryptografie 126
11.1 Nachteile symmetrischer Verfahren 126
11.2 Einwegfunktion 127
11.3 Diffie-Hellman-Schlüsseltausch 131
11.4 El-Gamal 132
11.5 RSA 133
11.6 Digitale Signatur 136
11.7 Hashfunktionen 137
11.8 Schwachstellen in RSA 138
11.9 Public Key Infrastructure 141
11.10 Übung 144

12 Kryptografische Protokolle und ihre Anwendung 145
12.1 SSL/TLS 145
12.2 SSH 150
12.3 IPsec 151
12.4 Übung 152

© HERDT-Verlag

13 Sichere E-Mail-Verfahren 153
13.1 Grundlagen der E-Mail-Verschlüsselung 153
13.2 Schlüssel generieren 155
13.3 Schlüsselexport und -import 157
13.4 Signieren von Schlüsseln 160
13.5 E-Mail signieren und verschlüsseln 161
13.6 Dateien signieren und verschlüsseln 162
13.7 Übung 162

14 Firewalls 163
14.1 Wie Firewalls arbeiten 163
14.2 Paketfilter-Firewall 165
14.3 Stateful Inspection Firewall 167
14.4 Proxy Level/Application Level Firewall 168
14.5 NAT 169
14.6 Personal Firewall 170
14.7 Sicherheitskonzept Firewall 172
14.8 Erweiterte Funktionen der Firewall 172
14.9 Übung 173

15 Intrusion-Detection/Prevention-Systeme 174
15.1 Notwendigkeit von Intrusion-Detection-Systemen 174
15.2 Arbeitsweise eines IDS 175
15.3 Auf erkannte Angriffe reagieren 177
15.4 Intrusion-Prevention-Systeme (IPS) 178
15.5 Snort 179
15.6 Honeypot-Netzwerke 180
15.7 Übung 182

16 Virtual Private Network 183
16.1 Zielsetzung 183
16.2 PPTP 184
16.3 L2TP/IPsec 185
16.4 OpenVPN 190
16.5 Abgrenzung zu anderen VPN-Arten 190
16.6 Übung 190

17 WLAN und Sicherheit 191
17.1 WLAN-Arbeitsweise 191
17.2 Access-Points 195
17.3 WEP – Wired Equivalency Protocol 196
17.4 WPA – Wi-Fi Protected Access 197
17.5 WPA2 – Wi-Fi Protected Access 2 198
17.6 WPA3 – Wi-Fi Protected Access 3 198
17.7 Weitere Authentifizierung und Verschlüsselung im WLAN 199
17.8 Funkausleuchtung 200
17.9 Übung 202

18 Alternative Software 204
18.1 Warum Nicht-Standard-Software sinnvoll sein kann 204
18.2 Alternative Webbrowser 206
18.3 Alternative E-Mail-Clients 208

19 Authentifizierungssysteme 211
19.1 Kerberos 211
19.2 PAP, CHAP, EAP und RADIUS 214
19.3 Smartcards und Tokensysteme 217
19.4 Biometrie 218

20 Proaktive Sicherheit 222
20.1 Defensive Programmierung 222
20.2 Gehärtete Betriebssysteme 223
20.3 Patches 225
20.4 Vulnerability Assessment 226

Stichwortverzeichnis 232

© HERDT-Verlag