Bevor Sie beginnen … 4

1 Was ist Sicherheit? 6

1.1 Grundforderungen an Sicherheit 6
1.2 Datensicherheit = Datenschutz? 6
1.3 Sicherheitsziele 7
1.4 Ursachen von Sicherheitsproblemen 9
1.5 Sensibilisierung der Mitarbeiter (Awareness) 10

2 Rechtsgrundlagen 11

2.1 Gesetzliche Grundlagen der Informationssicherheit 11
2.2 „Hackerparagraf“ §§ 202a–c StGB 11
2.3 IT-Sicherheitsgesetz (IT-SiG) 12
2.4 IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) 14
2.5 KRITIS-Dachgesetz (KRITIS-Dach-G) 16
2.6 EU-NIS2 Umsetzungsgesetz zur Stärkung der Cybersicherheit (NIS2UmsuCG) 17
2.7 Besondere Vertragsbedingungen für die Beschaffung von DV-Leistungen (BVB) 17

3 Risikolage für Unternehmen 18

3.1 Warum ist das Internet nicht „sicher“? 18
3.2 Schadensmöglichkeiten 20

4 Angriffsvorbereitung 21

4.1 Hacker und Cracker 21
4.2 „Staatliche“ Hacker 22
4.3 Elektronische Kriegsführung 24
4.4 Informationsbeschaffung vor dem Angriff 24
4.5 Wardriving 30
4.6 Social Engineering 31

5 Angriffsarten 34

5.1 Exploits 34
5.2 Rootkits 40
5.3 DoS/DDoS/DRDoS 42
5.4 Sniffer 43
5.5 Replay-Attacken 45
5.6 TCP/IP Session-Hijacking 45

6 Sicherheitsprobleme durch Mitarbeiter 47

6.1 Ausfall/Krankheit 47
6.2 Unrechtmäßige Systemzugänge 48
6.3 Spionage 49
6.4 Mangelnde Kompetenz 50

7 Viren und ihre Verbreitung 54

7.1 Grundkonzepte von Viren 54
7.2 Virenarten 56
7.3 Tarnmechanismen von Viren 62
7.4 Würmer 68
7.5 Trojaner 69
7.6 Adware und PUA 72
7.7 Tendenzen und Ausblick 72

8 Spyware, Phishing und Browser-Hijacking 74

8.1 Geld verdienen im Internet 74
8.2 Spyware 77
8.3 Browser-Hijacking 79
8.4 Was ist Phishing? 80
8.5 Anti-Spyware einsetzen 83

9 Stand-alone-Virenschutz 88

9.1 Einfache Virenprävention 88
9.2 Gängige Anti-Malware-Applikationen 94
9.3 Computer scannen 97
9.4 Viren entfernen 99

10 IT-Sicherheitsstandards 101

10.1 Planung und Umsetzung der Informationssicherheit durch Kriterienwerke 101
10.2 Die wichtigsten Sicherheitsstandards 101
10.3 Zielgruppenmatrix 104
10.4 DIN EN 50600-Reihe 105
10.5 Security Policy 106
10.6 Der IT-Sicherheitsbeauftragte 107

11 Kryptografie 108

11.1 Was ist Kryptografie? 108
11.2 Klassische Verschlüsselungsmethoden 111
11.3 Symmetrische Verschlüsselung 117
11.4 Asymmetrische Kryptografie 127
11.5 Schlüsselerzeugung und -austausch 132
11.6 Public Key Infrastructure 139
11.7 Digitale Signatur 141
11.8 Hash-Algorithmen 143
11.9 Hybride Verschlüsselung 146

12 Kryptografische Protokolle und deren Anwendung 148

12.1 SSL/TLS 148
12.2 SSH 154
12.3 IPsec 155

13 Sichere E-Mail-Verfahren 157

13.1 Grundlagen der E-Mail-Verschlüsselung 157
13.2 E-Mail-Verschlüsselung mit Gpg4win (GnuPG) einrichten 159
13.3 E-Mail mit Outlook signieren und verschlüsseln 165

14 Firewalls 168

14.1 Wie Firewalls arbeiten 168
14.2 Paketfilter-Firewall 170
14.3 Stateful Inspection Firewall 172
14.4 Proxy Level / Application Level Firewall 174
14.5 NAT 175
14.6 Personal Firewall 177
14.7 Sicherheitskonzept Firewall 178
14.8 Erweiterte Funktionen der Firewall 178

15 Intrusion-Detection-/Prevention-Systeme 180

15.1 Notwendigkeit von Intrusion-Detection-Systemen 180
15.2 Arbeitsweise eines IDS 181
15.3 Auf erkannte Angriffe reagieren 183
15.4 Intrusion-Prevention-Systeme (IPS) 184
15.5 Snort 185
15.6 Honeypot-Netzwerke 186

16 Virtual Private Network (VPN) 189

16.1 Zielsetzung 189
16.2 PPTP 191
16.3 L2TP/IPsec 192
16.4 OpenVPN 197
16.5 WireGuard 197
16.6 ExpressVPN 198
16.7 Abgrenzung zu anderen VPN-Arten 198

17 WLAN und Sicherheit 199

17.1 WLAN-Arbeitsweise 199
17.2 Access-Points (AP) 203
17.3 Verschlüsselungsprotokolle 204
17.4 Weitere Authentifizierung- und Verschlüsselungsmethoden im WLAN 206
17.5 Funkausleuchtung 209

18 Alternative Software 211

18.1 Warum Nicht-Standardsoftware sinnvoll sein kann 211
18.2 Alternative Webbrowser 213
18.3 Alternative E-Mail-Clients 216

19 Authentifizierungssysteme 219

19.1 Kerberos 219
19.2 PAP, CHAP, EAP, RADIUS und Diameter 223
19.3 Smartcards und Token-Systeme 225
19.4 Biometrie 227

20 Proaktive Sicherheit 231

20.1 Defensive Programmierung 231
20.2 Gehärtete Betriebssysteme 233
20.3 Isolierte Umgebungen (Sandbox) 234
20.4 Patches 234
20.5 Vulnerability Assessment 236
20.6 Sicherheit der IT-Infrastruktur 241
20.7 Sensibilisierung der Mitarbeiter (Awareness) 243

21 KI – Künstliche Intelligenz als neue Herausforderung an die IT-Sicherheit 244

21.1 Was ist KI? 244
21.2 Sicherheitsrisiken in der IT durch KI: Herausforderungen und Lösungsansätze 245
21.3 Denkbare IT-Angriffe durch KI 246
21.4 Fazit 249

Stichwortverzeichnis 250