

---

## Praxistipps IT

# Cybersecurity in der Praxis

Gefahren, Präventionsmaßnahmen,  
Krisenmanagement

Krüger/Simon/Trappe



IDW VERLAG GMBH

# Inhaltsverzeichnis

<b>1 Einleitung .....</b>	<b>9</b>
<b>2 Akteure, Gefahren und Grundlagen .....</b>	<b>13</b>
2.1 Der Cyberraum (Cyberspace) .....	13
2.2 Cybersecurity .....	15
2.3 Akteure des Cyberraums .....	15
2.3.1 Anwender .....	16
2.3.2 Angreifer .....	17
2.3.3 Wirtschaftsprüfer und Steuerberater als Zielgruppen .....	32
2.4 Sensible Daten wandern in die Cloud .....	34
2.5 Crime as a Service .....	35
<b>3 Schutz- und Verteidigungskonzepte .....</b>	<b>36</b>
3.1 Entwicklung einer Informationssicherheitsleitlinie .....	37
3.1.1 Aller Anfang ist schwer .....	39
3.1.2 Der Schutzbedarf von Informationen .....	40
3.1.3 Der Informationssicherheitsbeauftragte .....	41
3.1.4 Die Wahl der Vorgehensweise .....	43
3.2 Layered Security und Defense in Depth .....	43
3.2.1 Layered Security und Defense in Depth im schematischen Ansatz .....	44
3.2.2 Typische Sicherheitsmaßnahmen im Layered-Security-Konzept .....	45
3.2.3 Von der Schwachstelle bis zur Ausnutzung .....	47
3.2.4 Consumer vs. Enterprise Layered Security Strategy .....	47
3.2.5 Realisierung von Multifaktor-Authentifizierung .....	48
3.2.6 Beseitigung des Weakest Link .....	49
3.2.7 Das Prinzip des Least Privilege .....	50
3.2.8 Integration vs. Best of Breed .....	50
3.2.9 Kategorisierung der Sicherheitsmaßnahmen .....	51
3.3 DMZ/Architekturen .....	52

<b>4 Standards, Leitlinien und Qualifikationen .....</b>	<b>54</b>
4.1 ISO 27000/27001.....	54
4.2 IT-Grundschutz nach BSI mit Erweiterung KRITIS .....	56
4.2.1 IT-Grundschutz nach BSI 100 (2005).....	58
4.2.2 IT-Grundschutz nach BSI 200 (2017).....	59
4.2.3 BSI-KRITIS-Verordnung.....	63
4.3 BSI-C5-Testat.....	64
4.4 CISSP .....	68
4.5 T.I.S.P.....	70
<b>5 Absicherungsmaßnahmen .....</b>	<b>72</b>
5.1 Schlüsseltechnologien der Cybersecurity-Industrie.....	73
5.1.1 Firewall und Proxy.....	73
5.1.2 Intrusion Prevention Systems (IPS)/Intrusion Detection Systems (IDS).....	75
5.1.3 Anti-Malware .....	76
5.2 Das Zonenmodell .....	77
5.2.1 Digitaler Arbeitsplatz.....	78
5.2.2 DMZ/Eigene Dienste .....	83
5.2.3 Netzwerk (LAN) .....	86
5.2.4 Perimeter.....	90
5.2.5 Physische Umgebung .....	92
5.2.6 Querschnittliche Maßnahmen.....	96
5.2.7 Erweiterte Maßnahmen.....	104
<b>6 Cloud .....</b>	<b>106</b>
6.1 Definition von unterschiedlichen Cloud-Typen .....	106
6.2 Risiken von Cloud-Diensten.....	111
6.2.1 Schatten-IT.....	111
6.2.2 Datensicherheit und Datenschutz.....	112
6.2.3 Schnittstellenproblematik .....	112
6.2.4 Angriffe auf Cloud-Dienste.....	114
6.3 Zertifizierung von Cloud-Diensten.....	115

6.4 SaaS-Sicherheit .....	116
6.5 SOaaS.....	117
6.6 Best Practices.....	119
<b>7 Mobile Device Security .....</b>	<b>121</b>
7.1 Herausforderungen.....	121
7.2 Mobile Device Management.....	124
7.3 Sicherheit bei mobilen Geräten.....	126
<b>8 Internet of Things .....</b>	<b>129</b>
8.1 Definition vom Internet der Dinge.....	129
8.2 Herausforderungen bei der Nutzung von IoT.....	130
8.3 Chancen für IoT.....	131
<b>9 Maßnahmenevaluation .....</b>	<b>132</b>
9.1 Grundbegriffe der Maßnahmenevaluation .....	132
9.1.1 Testobjekt (Scope) und Tester .....	132
9.1.2 White/Blue/Red Team .....	132
9.1.3 White/Black/Grey Box.....	134
9.1.4 Double-Blind/Blind/Targeted .....	135
9.1.5 Methodik/Angreifermodell.....	136
9.2 Audits.....	139
9.3 Technische Prüfungen.....	140
9.3.1 Technische Schwachstellenanalyse.....	141
9.3.2 Penetrationstest .....	143
9.3.3 Red Teaming .....	144
9.4 Zusammenfassung: Maßnahmenevaluation .....	146
<b>10 Open Source Security Software .....</b>	<b>147</b>
10.1 Definition von Open Source .....	148
10.2 Open vs. Closed .....	150
10.3 Open-Source-Projekte.....	150
10.3.1 pfSense.....	151

10.3.2 Snort.....	151
10.3.3 Graylog.....	152
10.3.4 OpenVAS.....	153
10.3.5 OnlyOffice.....	154
<b>11 Business Continuity Management.....</b>	<b>155</b>
11.1 Definitionen und Einordnung.....	156
11.2 Potenziell relevante Risiken und Szenarien.....	161
11.2.1 Krisenfälle und Unternehmensfolgen .....	161
11.2.2 Mögliche Szenarien.....	161
11.3 Krisenvorsorge .....	165
11.3.1 Aufbau eines BCMS.....	166
11.3.2 Business-Impact-Analyse .....	167
11.3.3 Bewertung der Risiken für die Geschäftsprozesse.....	168
11.3.4 Kontinuitätsstrategie und Notfalldokumentation .....	171
11.3.5 Ablauf eines Notfalls und Notfallhandbuch .....	171
11.3.6 Risikotransfer durch Outsourcing von Risiken .....	174
11.3.7 Durchführung von Notfallübungen.....	176
11.4 Krisenbewältigung.....	177
11.4.1 Ablauf eines Notfalls.....	177
11.4.2 Besonderheiten bei Cyberangriffen.....	179
<b>12 Thinking outside the Box.....</b>	<b>180</b>
12.1 Capture The Flag (CTF) Events.....	180
12.2 Humble Bundle .....	182
12.3 Video-on-Demand-Plattformen und Youtube .....	182
12.4 Konferenzen/LiveHacking-Veranstaltungen.....	183
12.5 Lock Picking.....	183
12.6 Schulungen/Trainings/Workshops.....	184
12.7 Try it yourself!.....	184
<b>13 Fazit.....</b>	<b>186</b>
<b>Stichwortverzeichnis.....</b>	<b>188</b>