



# Auf einen Blick

<b>Über die Autoren</b> .....	<b>7</b>
<b>Einleitung</b> .....	<b>19</b>
<b>Teil I: Informationssicherheit, IT-Sicherheit und Datenschutz</b> .....	<b>25</b>
<b>Kapitel 1:</b> Irrtümer und häufige Fehler .....	27
<b>Kapitel 2:</b> Grundlagen der Informationssicherheit .....	35
<b>Kapitel 3:</b> Bausteine der Informationssicherheit .....	47
<b>Kapitel 4:</b> Datenschutz und technisch-organisatorische Maßnahmen .....	59
<b>Teil II: Rechtliche Anforderungen</b> .....	<b>63</b>
<b>Kapitel 5:</b> Die DS-GVO und das BDSG .....	65
<b>Kapitel 6:</b> Gesetze zur IT-Sicherheit .....	75
<b>Kapitel 7:</b> ISO-Normen .....	95
<b>Kapitel 8:</b> BSI und Grundschutz .....	105
<b>Kapitel 9:</b> Weitere Standards .....	119
<b>Kapitel 10:</b> Technisch-organisatorische Maßnahmen (TOM) .....	131
<b>Teil III: Organisation der Informationssicherheit</b> .....	<b>153</b>
<b>Kapitel 11:</b> Organisation im Unternehmen .....	155
<b>Kapitel 12:</b> Der Deming-Kreis (PDCA) und die ständige Verbesserung .....	163
<b>Kapitel 13:</b> Risikoanalyse und Kronjuwelen .....	165
<b>Kapitel 14:</b> Grundlegende Dokumentation .....	171
<b>Kapitel 15:</b> Meldepflichten und Vorfallsmanagement .....	185
<b>Kapitel 16:</b> Awareness und Beschäftigte .....	197
<b>Teil IV: Bausteine der technischen IT-Sicherheit</b> .....	<b>201</b>
<b>Kapitel 17:</b> Grundlagen der Verschlüsselung .....	203
<b>Kapitel 18:</b> Biometrie .....	243
<b>Kapitel 19:</b> Chipkarten und Secure Hardware Token .....	249
<b>Teil V: Lösungen und Umsetzungen</b> .....	<b>255</b>
<b>Kapitel 20:</b> Backup & Co. ....	257
<b>Kapitel 21:</b> Netzwerksicherheit .....	267
<b>Kapitel 22:</b> Firewalls .....	291
<b>Kapitel 23:</b> Verschlüsselung im Einsatz .....	301
<b>Kapitel 24:</b> Monitoring .....	319
<b>Kapitel 25:</b> Patch Management .....	331
<b>Kapitel 26:</b> Zugangssicherung und Authentisierung .....	335
<b>Kapitel 27:</b> Anwendungssicherheit .....	343





## 10 Auf einen Blick

<b>Teil VI: Der Top-Ten-Teil</b> .....	<b>359</b>
<b>Kapitel 28:</b> Zehn Maßnahmen für den technischen Basisschutz.....	361
<b>Kapitel 29:</b> Zehn Maßnahmen für den organisatorischen Überbau.....	365
<b>Literaturverzeichnis</b> .....	<b>369</b>
<b>Abbildungsverzeichnis</b> .....	<b>373</b>
<b>Stichwortverzeichnis</b> .....	<b>379</b>





# Inhaltsverzeichnis

<b>Über die Autoren .....</b>	<b>7</b>
<b>Einleitung.....</b>	<b>19</b>
Über dieses Buch .....	19
Törichte Annahmen über den Leser .....	19
Was Sie nicht lesen müssen .....	20
Wie dieses Buch aufgebaut ist.....	20
Teil I: Informationssicherheit, IT-Sicherheit und Datenschutz .....	20
Teil II: Rechtliche Anforderungen.....	21
Teil III: Organisation der Informationssicherheit.....	21
Teil IV: Bausteine der technischen IT-Sicherheit.....	22
Teil V: Lösungen und Umsetzungen .....	22
Teil VI: Der Top-Ten-Teil.....	22
Symbole, die in diesem Buch verwendet werden.....	23
Konventionen in diesem Buch.....	23
Wie es weitergeht.....	24
<b>TEIL I</b>	
<b>INFORMATIONSSICHERHEIT, IT-SICHERHEIT</b>	
<b>UND DATENSCHUTZ.....</b>	<b>25</b>
<b>Kapitel 1</b>	
<b>Irrtümer und häufige Fehler.....</b>	<b>27</b>
Internet-Sicherheit.....	27
Mobile und Cloud-Sicherheit.....	29
Endgerätesicherheit .....	31
E-Mail-Sicherheit .....	32
<b>Kapitel 2</b>	
<b>Grundlagen der Informationssicherheit.....</b>	<b>35</b>
Was ist Informationssicherheit?.....	35
Was ist IT-Sicherheit? .....	35
Was ist Cybersicherheit? .....	38
Klassische Schutzziele der Informationssicherheit.....	39
Verfügbarkeit.....	39
Integrität.....	41
Vertraulichkeit .....	42
Authentizität .....	42
Verantwortlichkeit.....	42
Benutzbarkeit.....	43
Weitere Schutzziele.....	44





## 12 Inhaltsverzeichnis

<b>Kapitel 3</b>	
<b>Bausteine der Informationssicherheit</b> .....	<b>47</b>
Risikomanagement.....	48
Meldepflichten bei Vorfällen.....	51
Einhaltung von Sicherheitsstandards.....	54
Nachweis der Einhaltung durch Audits.....	55
<b>Kapitel 4</b>	
<b>Datenschutz und technisch-organisatorische Maßnahmen</b> .....	<b>59</b>
<b>TEIL II</b>	
<b>RECHTLICHE ANFORDERUNGEN</b> .....	<b>63</b>
<b>Kapitel 5</b>	
<b>Die DS-GVO und das BDSG</b> .....	<b>65</b>
Die acht Gebote des Datenschutzes (BDSG a. F.).....	65
Stand der Technik.....	67
Implementierungskosten.....	70
Gewährleistungsziele des Datenschutzes.....	73
<b>Kapitel 6</b>	
<b>Gesetze zur IT-Sicherheit</b> .....	<b>75</b>
NIS-Richtlinie (EU).....	75
Rechtsakt zur Cybersicherheit (EU).....	77
eIDAS-Verordnung (EU).....	79
Single-Digital-Gateway-(SDG-)Verordnung (EU).....	81
BSI-Gesetz (D).....	81
BSI-Kritisverordnung (D).....	85
Geschäftsgeheimnisgesetz (D).....	86
Onlinezugangsgesetz (D).....	87
Sozialgesetzbuch V (D).....	88
TKG, TMG und TTDSG (D).....	92
<b>Kapitel 7</b>	
<b>ISO-Normen</b> .....	<b>95</b>
ISO/IEC 270xx Informationssicherheit.....	96
Anforderungsnormen.....	98
Leitfäden.....	100
ISO/IEC 27701 Datenschutz.....	102
<b>Kapitel 8</b>	
<b>BSI und Grundschutz</b> .....	<b>105</b>
IT-Grundschutz.....	105
BSI-Standards.....	106
IT-Grundschutz-Kompodium.....	108
Standard-Datenschutzmodell und IT-Grundschutz.....	113
Technische Richtlinien des BSI.....	115



## Inhaltsverzeichnis 13

<b>Kapitel 9</b>	
<b>Weitere Standards</b> .....	<b>119</b>
Prozessorientierte Standards .....	119
VdS 10000: ISMS für KMU.....	120
ISIS12 wird CISIS12.....	122
TISAX.....	122
Finanzstandards.....	123
Vorgaben für die öffentliche Verwaltung.....	124
Technikorientierte Standards.....	125
Common Criteria.....	125
PCI-DSS.....	127
FIPS.....	129
ITIL.....	130
<b>Kapitel 10</b>	
<b>Technisch-organisatorische Maßnahmen (TOM)</b> .....	<b>131</b>
Vertraulichkeit.....	131
Zutrittskontrolle, physische und umgebungsbezogene Sicherheit.....	132
Zugangskontrolle, Zugangssteuerung.....	133
Zugriffskontrolle.....	134
[Trennungskontrolle], Nichtverkettbarkeit.....	135
Pseudonymisierung.....	137
Verschlüsselung, Kryptografie.....	139
Integrität.....	141
Eingabekontrolle.....	141
Digitale Signatur, Hashfunktionen.....	142
Weitergabekontrolle, Kommunikationssicherheit.....	143
Löschkontrolle (»Recht auf Vergessen werden«).....	144
Verfügbarkeit und Belastbarkeit.....	145
Verfügbarkeitskontrolle und Informationssicherheitsaspekte beim Business Continuity Management.....	146
Auftragskontrolle, Lieferantenbeziehungen.....	147
Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM.....	149
<b>TEIL III</b>	
<b>ORGANISATION DER INFORMATIONSSICHERHEIT</b> .....	<b>153</b>
<b>Kapitel 11</b>	
<b>Organisation im Unternehmen</b> .....	<b>155</b>
Verantwortung für die Informationssicherheit.....	155
Organisatorische Strukturen.....	155
Geschäftsleitung.....	156
Chief Information Officer/Chief Digital Officer.....	156
Informationssicherheitsbeauftragter.....	156
IT-Leitung.....	157
Computer Emergency Response Team (CERT).....	158
Informationssicherheitsausschuss.....	159
Richtlinien und Regeln.....	159



## 14 Inhaltsverzeichnis

<b>Kapitel 12</b>	
<b>Der Deming-Kreis (PDCA) und die ständige Verbesserung.....</b>	<b>163</b>
<b>Kapitel 13</b>	
<b>Risikoanalyse und Kronjuwelen .....</b>	<b>165</b>
Klassifizierung der Daten .....	165
Klassifizierung der Systeme.....	166
Bedrohungsanalyse.....	168
Metriken und Bewertung.....	169
<b>Kapitel 14</b>	
<b>Grundlegende Dokumentation.....</b>	<b>171</b>
Asset- und Konfigurationsmanagement.....	174
Nutzermanagement und Zugriffskontrolle .....	180
<b>Kapitel 15</b>	
<b>Meldepflichten und Vorfallsmanagement.....</b>	<b>185</b>
Datenschutzvorfälle.....	185
IT-Sicherheitsvorfälle .....	187
Angriffserkennung.....	189
Security Information and Event Management (SIEM).....	190
Dokumentation von Vorfällen und Forensik.....	191
Sharing von Threat-Informationen.....	192
<b>Kapitel 16</b>	
<b>Awareness und Beschäftigte .....</b>	<b>197</b>
<b>TEIL IV</b>	
<b>BAUSTEINE DER TECHNISCHEN IT-SICHERHEIT .....</b>	<b>201</b>
<b>Kapitel 17</b>	
<b>Grundlagen der Verschlüsselung.....</b>	<b>203</b>
Symmetrische Verschlüsselung.....	208
Betriebsarten der Blockverschlüsselung .....	210
Asymmetrische Verschlüsselung .....	214
Diffie-Hellman-Merkle-Schlüsselaustausch.....	214
Das RSA-Verfahren.....	215
Hybride Verschlüsselung.....	220
Hashfunktionen .....	221
Digitale und elektronische Signaturen.....	225





## Inhaltsverzeichnis 15

Elliptische-Kurven-Kryptografie .....	227
DLIES und ECIES .....	229
Vertrauensmodelle .....	229
Persönlicher Kontakt .....	232
Zertifizierungsstellen .....	233
Web of Trust .....	235
Trust on First Use .....	237
Kryptographische Forschung .....	237
Homomorphe Verschlüsselung .....	238
Post-Quantenkryptografie .....	240

<b>Kapitel 18</b>	
<b>Biometrie .....</b>	<b>243</b>
Hautleisten .....	246
Venenmuster .....	247
Iris-Scan .....	247
Gesichtserkennung .....	247

<b>Kapitel 19</b>	
<b>Chipkarten und Secure Hardware Token .....</b>	<b>249</b>
Einmalpasswort-Token .....	252

<b>TEIL V</b>	
<b>LÖSUNGEN UND UMSETZUNGEN .....</b>	<b>255</b>

<b>Kapitel 20</b>	
<b>Backup &amp; Co. ....</b>	<b>257</b>
Datensicherung .....	258
Kontrollfragen .....	261
Aufbewahrungspflichten .....	262
Archivierung .....	263
Redundanz .....	264

<b>Kapitel 21</b>	
<b>Netzwerksicherheit .....</b>	<b>267</b>
Grundlagen .....	269
Sicherheitserweiterungen von Netzwerkprotokollen .....	270
DNS, Anwendungsschicht .....	270
HTTPS, SMTPS, Anwendungsschicht .....	272
TCP und UDP, Transportschicht .....	272
IP und IPsec, Netzwerkschicht .....	276
ARP und 802.1X, Verbindungsschicht .....	277
Netzwerkzugang .....	278
Netzwerksegmentierung .....	280





## 16 Inhaltsverzeichnis

Denial-of-Service-Angriffe .....	281
Anonymisierung in Netzwerken.....	283
Funknetze .....	284
WLAN.....	284
Bluetooth.....	286
NFC, RFID.....	288
Das sichere Internet der Zukunft.....	290

### Kapitel 22

<b>Firewalls .....</b>	<b>291</b>
Grundlagen von Firewalls.....	291
Packet Filter .....	294
Stateful Inspection Firewall.....	294
Network Address Translation (NAT).....	295
Proxy-Server und Application Layer Firewall.....	296
NG Firewall und Deep Packet Inspection.....	297
Firewall in der Cloud.....	298

### Kapitel 23

<b>Verschlüsselung im Einsatz .....</b>	<b>301</b>
Daten in Ruhe .....	301
Datenträgerverschlüsselung.....	304
Partitionsverschlüsselung.....	307
Containerverschlüsselung.....	307
Dateiverschlüsselung.....	308
Daten in Bewegung .....	309
Transportverschlüsselung.....	309
E-Mail-Verschlüsselung.....	311
Virtuelle private Netzwerke (VPN).....	311

### Kapitel 24

<b>Monitoring .....</b>	<b>319</b>
Metriken der IT-Sicherheit.....	319
Angriffserkennungssysteme.....	322
Angriffserkennungssysteme (netzwerkbasiert).....	323
Angriffserkennungssysteme (hostbasiert).....	324
Managed Security.....	325
Schadsoftware.....	326
Abwehrstrategien.....	327
Analyse von Schadsoftware.....	328

### Kapitel 25

<b>Patch Management.....</b>	<b>331</b>
------------------------------	------------





## Inhaltsverzeichnis 17

<b>Kapitel 26</b>	
<b>Zugangssicherung und Authentisierung.....</b>	<b>335</b>
Passwörter im Unternehmen.....	335
Zwei-Faktor-Authentisierung.....	338
Biometrie.....	339
Single Sign-on .....	340
<b>Kapitel 27</b>	
<b>Anwendungssicherheit.....</b>	<b>343</b>
Chat.....	343
E-Mail.....	344
Verschlüsselung.....	345
Allgemeine Sicherheit .....	346
Videokonferenzen .....	347
Multipoint Control Unit.....	347
Selective Forwarding Unit.....	348
Peer to Peer .....	348
Webanwendungen .....	349
Datenbanken .....	351
Cloud.....	352
Speichern in der Cloud.....	353
Verarbeiten in der Cloud .....	353
Blockchain.....	354
Künstliche Intelligenz.....	356
<b>TEIL VI</b>	
<b>DER TOP-TEN-TEIL.....</b>	<b>359</b>
<b>Kapitel 28</b>	
<b>Zehn Maßnahmen für den technischen Basisschutz.....</b>	<b>361</b>
Backup .....	361
Schutz vor Schadsoftware.....	361
Netzwerkschutz.....	361
Firewall.....	362
Patch-Management.....	362
Verschlüsselt speichern .....	362
Verschlüsselt kommunizieren.....	362
Passwort-Management.....	362
Biometrie und Zwei-Faktor-Authentifikation.....	362
Spam-Abwehr.....	363
<b>Kapitel 29</b>	
<b>Zehn Maßnahmen für den organisatorischen Überbau.....</b>	<b>365</b>
Übernahme der Verantwortung.....	365
Leitlinie zur Informationssicherheit .....	365
Richtlinien zur Informationssicherheit.....	365



## 18 Inhaltsverzeichnis

Definition und Besetzung der Rollen.....	366
Definition der fundamentalen Prozesse.....	366
Risikobetrachtung.....	366
Klassifizierung der Daten und Systeme.....	366
Awareness.....	366
Krisenmanagement.....	366
Regelmäßige Überprüfung.....	367
<b>Literaturverzeichnis.....</b>	<b>369</b>
<b>Abbildungsverzeichnis.....</b>	<b>373</b>
<b>Stichwortverzeichnis.....</b>	<b>379</b>

