

Auf einen Blick

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

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

Inhaltsverzeichnis

Über die Autoren	7
Einleitung.....	19
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
TEIL I	
INFORMATIONSSICHERHEIT, IT-SICHERHEIT	
UND DATENSCHUTZ.....	25
Kapitel 1	
Irrtümer und häufige Fehler.....	27
Internet-Sicherheit.....	27
Mobile und Cloud-Sicherheit.....	29
Endgerätesicherheit	31
E-Mail-Sicherheit	32
Kapitel 2	
Grundlagen der Informationssicherheit.....	35
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

Kapitel 3	
Bausteine der Informationssicherheit	47
Risikomanagement.....	48
Meldepflichten bei Vorfällen.....	51
Einhaltung von Sicherheitsstandards.....	54
Nachweis der Einhaltung durch Audits.....	55
Kapitel 4	
Datenschutz und technisch-organisatorische Maßnahmen	59
TEIL II	
RECHTLICHE ANFORDERUNGEN	63
Kapitel 5	
Die DS-GVO und das BDSG	65
Die acht Gebote des Datenschutzes (BDSG a. F.).....	65
Stand der Technik.....	67
Implementierungskosten.....	70
Gewährleistungsziele des Datenschutzes.....	73
Kapitel 6	
Gesetze zur IT-Sicherheit	75
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
Kapitel 7	
ISO-Normen	95
ISO/IEC 270xx Informationssicherheit.....	96
Anforderungsnormen.....	98
Leitfäden.....	100
ISO/IEC 27701 Datenschutz.....	102
Kapitel 8	
BSI und Grundschutz	105
IT-Grundschutz.....	105
BSI-Standards.....	106
IT-Grundschutz-Kompodium.....	108
Standard-Datenschutzmodell und IT-Grundschutz.....	113
Technische Richtlinien des BSI.....	115

Kapitel 9

Weitere Standards **119**

- 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

Kapitel 10

Technisch-organisatorische Maßnahmen (TOM)..... **131**

- 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

TEIL III

ORGANISATION DER INFORMATIONSSICHERHEIT **153**

Kapitel 11

Organisation im Unternehmen..... **155**

- 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

Kapitel 12	
Der Deming-Kreis (PDCA) und die ständige Verbesserung	163
Kapitel 13	
Risikoanalyse und Kronjuwelen	165
Klassifizierung der Daten.....	165
Klassifizierung der Systeme.....	166
Bedrohungsanalyse.....	168
Metriken und Bewertung.....	169
Kapitel 14	
Grundlegende Dokumentation	171
Asset- und Konfigurationsmanagement.....	174
Nutzermanagement und Zugriffskontrolle.....	180
Kapitel 15	
Meldepflichten und Vorfallsmanagement	185
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
Kapitel 16	
Awareness und Beschäftigte	197
TEIL IV	
BAUSTEINE DER TECHNISCHEN IT-SICHERHEIT	201
Kapitel 17	
Grundlagen der Verschlüsselung	203
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

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
Kapitel 18	
Biometrie	243
Hautleisten	246
Venenmuster	247
Iris-Scan	247
Gesichtserkennung	247
Kapitel 19	
Chipkarten und Secure Hardware Token	249
Einmalpasswort-Token	252
TEIL V	
LÖSUNGEN UND UMSETZUNGEN	255
Kapitel 20	
Backup & Co.	257
Datensicherung	258
Kontrollfragen	261
Aufbewahrungspflichten	262
Archivierung	263
Redundanz	264
Kapitel 21	
Netzwerksicherheit	267
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

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	
Firewalls	291
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	
Verschlüsselung im Einsatz	301
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	
Monitoring	319
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	
Patch Management	331

Kapitel 26
Zugangssicherung und Authentisierung..... 335
 Passwörter im Unternehmen..... 335
 Zwei-Faktor-Authentisierung..... 338
 Biometrie..... 339
 Single Sign-on 340

Kapitel 27
Anwendungssicherheit..... 343
 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


TEIL VI
DER TOP-TEN-TEIL..... 359

Kapitel 28
Zehn Maßnahmen für den technischen Basisschutz..... 361
 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

Kapitel 29
Zehn Maßnahmen für den organisatorischen Überbau..... 365
 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
Literaturverzeichnis.....	369
Abbildungsverzeichnis.....	373
Stichwortverzeichnis.....	379

Diese Leseprobe haben Sie beim
 **edv-buchversand.de** heruntergeladen.
Das Buch können Sie online in unserem
Shop bestellen.

[Hier zum Shop](#)