

Inhaltsverzeichnis

Vorwort	VII
Abkürzungsverzeichnis	XIV
1 Einleitung	1
1.1 Prolog	1
1.2 Definitionen und Bedeutungen	2
1.3 Aktuelle (Cyber-)Bedrohungen und ihre Auswirkungen	3
1.4 Warum Ihre Apotheke vorangehen muss	5
1.5 IT- und Cybersicherheit sind „Chefsache“	6
1.6 Über dieses Buch	7
2 Rechtsgrundlagen und Haftung.....	9
2.1 Einführung.....	9
2.2 Strafrecht (Schweigepflicht, § 203 StGB)	9
2.3 Berufsrecht	11
2.3.1 Integrität und Vertrauen	12
2.3.2 Schweigepflicht	12
2.3.3 Berufshaftpflicht gleich Cyberversicherung?	14
2.4 Datenschutzrecht	14
2.5 Telemediengesetz	16
2.6 BSI-Gesetz (IT-Sicherheitsgesetz)	17
2.7 NIS-2-Richtlinie und BSI-Gesetz (neu)	19
2.8 Digital-Gesetze	21
2.9 Apothekenrecht	22
2.10 Haftung	23
3 Grundlagen der Cybersicherheit	24
3.1 Einführung.....	24
3.2 Abgrenzung und Definition von grundlegenden Begriffen	24
3.2.1 Definition von IT-System, Information und Datenobjekt	25
3.2.2 Abgrenzung der Begriffe Informationssicherheit, Cybersicherheit, IT-Sicherheit, Datensicherheit und Datenschutz	25
3.2.3 Informationssicherheits-Managementsystem (ISMS)	26
3.2.4 Abgrenzung von Identifizierung, Authentifizierung und Autorisierung	26
3.2.5 Definition von Bedrohung und Schwachstelle	27

3.3 Schutzziele in der Informationssicherheit.....	28
3.3.1 Vertraulichkeit	29
3.3.2 Integrität	29
3.3.3 Verfügbarkeit	30
3.3.4 Authentizität	31
3.3.5 Nichtabstreichbarkeit	32
3.3.6 Exkurs: Schutzziele des Datenschutzes	32
3.4 Grundlegende Sicherheitstechniken in der Informations-sicherheit.....	34
3.4.1 Sicherheitsprinzipien und -modelle	34
3.4.2 Zugriffssteuerung	37
3.4.3 Kryptografische Mittel	37
3.4.4 Netzwerksicherheit	39
3.4.5 Datensicherung und Wiederherstellung	41
3.4.6 Redundanz und Ausfallsicherung	42
3.4.7 Endpunktsicherheit	43
3.4.8 Penetration Testing	45
3.5 Wichtige Cybersicherheitsprozesse	47
3.5.1 Änderungsmanagement in IT-Systemen	47
3.5.2 Die integrierte Cybersicherheitslösung	48
3.6 Risikomanagement	49
3.6.1 Risikoidentifikation	50
3.6.2 Risikoermittlung	51
3.6.3 Risikoanalyse und -bewertung.....	52
3.6.4 Priorisierung und Behandlung von Risiken	53
3.6.5 Dokumentation von Risiken und Maßnahmen	54
3.7 Business-Continuity-Management	55
4 Bedrohungsvektoren in einer Apotheke	57
4.1 Einführung	57
4.2 Die Angreifer	58
4.3 Physische Sicherheit	58
4.3.1 Unbefugter Zutritt bzw. Zugriff	59
4.3.2 Diebstahl von Geräten oder Datenträgern	60
4.3.3 Weitere physische Sicherheitsrisiken	61
4.4 Digitale Sicherheit	61
4.4.1 Netzwerkangriffe	61
4.4.2 Malware, Viren und Co.	63
4.4.3 Hacking	65
4.4.4 Schwachstellen in Software und Systemen	66

4.5 Faktor Mensch	66
4.5.1 Social Engineering	67
4.5.2 Phishing-Angriffe	68
4.5.3 Mitarbeiterfehler und -nachlässigkeit	69
4.6 Interne Bedrohungen	70
4.6.1 Risiken durch Mitarbeiter	71
4.6.2 Bedrohungen durch ehemalige Angestellte	72
4.7 Lieferkette und Drittanbieter	73
4.7.1 Lieferanten	73
4.7.2 Software- und Dienstleistungsanbieter	74
4.8 IT-Geräte	76
4.8.1 Standard-PC	76
4.8.2 Mobile Geräte	76
4.8.3 Internet der Dinge (IoT) und medizinische Geräte	78
4.8.4 USB-Sticks (Datenträger)	79
4.9 Komplexe Systeme und Netzwerke	80
4.10 Künstliche Intelligenz	81
4.10.1 Stärkung der Angreifer	81
4.10.2 Risiken durch die Anwendung von KI	82
4.11 Zusammenfassung	83
5 Implementierung von IT-Sicherheit	84
5.1 Einführung	84
5.2 Fast-Track – Top Ten der wichtigsten IT-Sicherheitsmaßnahmen	85
5.2.1 Top 1 – Verantwortung tragen und definieren	85
5.2.2 Top 2 – Physische Absicherung	86
5.2.3 Top 3 – Regelmäßige Back-ups	88
5.2.4 Top 4 – Sichere Passwörter	90
5.2.5 Top 5 – Immer up to date	92
5.2.6 Top 6 – Notfallkonzept und Prozesse definieren	92
5.2.7 Top 7 – Nutzerkreise und Netzwerkbereiche definieren	93
5.2.8 Top 8 – Wissen und Awareness des Teams steigern	94
5.2.9 Top 9 – IT-Werkzeuge nicht nur kaufen, sondern richtig einsetzen	95
5.2.10 Top 10 – Lassen Sie sich helfen	96
5.3 Masterclass ISMS – Schritt für Schritt	97
5.3.1 ISMS ist Chefsache – geben Sie den Startschuss	98
5.3.2 Leitlinie zur Informationssicherheit	99
5.3.3 Sicherheitskonzept	107
5.3.4 Risikoanalyse	117
5.3.5 Sicherheitsmaßnahmen	124

5.3.6	Überwachung und Verbesserung	128
5.3.7	Zusammenfassung und Empfehlungen	130
6	Notfallplanung und -management	132
6.1	Einführung	132
6.2	Sofort- und Erstmaßnahmen	133
6.2.1	Bevor etwas passiert	133
6.2.2	Wenn etwas passiert	134
6.2.3	Nachdem etwas passiert ist	136
6.3	Grundlagen des Notfallmanagements	136
6.3.1	Definition eines Notfalls	136
6.3.2	Rolle des Apothekenpersonals in Notfällen	137
6.3.3	Vorteile effektiver Notfallplanung	137
6.3.4	Bestandteile des Notfallmanagements	138
6.3.5	Phasen des Notfallmanagements	138
6.4	Schritte zur Erstellung Ihres Notfallkonzepts	138
6.4.1	Leitlinie zum Notfallmanagement	140
6.4.2	Business-Impact-Analyse	144
6.4.3	Risikoanalyse	150
6.4.4	Kontinuitätsstrategie	151
6.4.5	Notfallvorsorgekonzept	152
6.4.6	Notfallbewältigung	153
6.4.7	Notfallübungen	159
6.4.8	Notfallmanagement verbessern	159
7	Schulung und Sensibilisierung der Mitarbeiter	160
7.1	Einführung	160
7.2	Empfehlungen	160
7.2.1	Adressaten – wer und wie?	161
7.2.2	Sensibilisierung und Motivation	161
7.2.3	Schulungsformen	161
7.2.4	Vorbereitung der Schulungen	162
7.2.5	Schulungsinhalte und -umfang	162
7.2.6	Schulungsintervalle und -regelmäßigkeit	162
7.2.7	Fortlaufende Bewertung und Anpassung	164
7.3	Resilienz-Test und Praxistraining	164
8	Weitere Hilfestellungen	165
8.1	Nützliches vom Bundesamt für Sicherheit in der Informations-technik (BSI)	165
8.1.1	Informationen zum Nachlesen und Vertiefen	166
8.1.2	Nach BSI-Standards erstellte Muster und Beispiele	167
8.1.3	Nach BSI-Standards erstellte Vorlagen	167

8.2 Checklisten	168
8.2.1 Checkliste Cybersicherheit: Organisatorisches, physische Sicherheit, Weiteres	168
8.2.2 Checkliste: Datensicherung	169
8.2.3 Checkliste: Deboarding	169
8.2.4 Checkliste: IT-Dienstleister	170
8.2.5 Checkliste: Netzwerk	170
8.2.6 Checkliste: Updates	170
8.2.7 Checkliste: Verschlüsselung	171
8.2.8 Checkliste: Virenschutz	171
8.3 Weitere Empfehlungen	171
8.3.1 So finden Sie ein geeignetes IT-Sicherheitsunternehmen	171
8.3.2 Cyberversicherung: sinnvoll oder nicht?	172
8.3.3 Was tun bei Lösegeldforderungen?	174
8.3.4 Einbindung der Polizei: ja oder nein?	175
8.4 Fördermöglichkeiten	177
Schlusswort	178
Glossar	179
Literatur	196
Bildnachweis	198
Sachregister	199
Die Autoren	201