

Inhaltsverzeichnis

Geleitwort	5
Vorwort	7
Verzeichnis der Autorinnen und Autoren	13
1 Krisenresilienz als Aufgabe und Herausforderung für Krankenhäuser und MVZ-Strukturen	17
1.1 Einleitung	17
1.2 Die Entwicklungen der Gefahrenbereiche	19
1.2.1 Schadenszenario Brandereignis	19
1.2.2 Schadensrisiko Hygiene	20
1.2.3 Schadenszenario Cybervorfall	21
1.2.4 Schadenszenario Lieferkette	22
1.2.5 Schadenszenario Umweltkatastrophe	23
1.2.6 Szenario Pandemie	24
1.3 Die Verantwortung der Krankenhäuser	24
1.4 Die Einbindung in die Krankenhaus-Compliance	26
1.5 Die Verantwortung der MVZ	28
1.6 Rechtsfolgen einer mangelhaften Krisenresilienz unter Berücksichtigung der Abrechnung	29
1.6.1 Rechtsfolgen im Normalfall	29
1.6.2 Rechtsfolgen im Notfall	29
1.6.3 Krisenresilienz und Abrechnungsbetrug	30
1.7 Fördermöglichkeiten und gesetzgeberisches Handeln	31
2 Rechtsgrundlagen des BCM und Compliance	33
2.1 Unionsrechtliche Vorgaben und ihre Umsetzung in nationales Recht	33
2.1.1 Entwicklungen auf der Ebene der Europäischen Union	33
2.1.2 IT-Sicherheit nach dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, dem IT-Sicherheitsgesetz und nach § 391 SGB V	36
2.1.3 Zwischenergebnis	43

2.2	Rechtspflicht zur Einführung eines BCM	43
2.2.1	Rechtspflicht zur Einführung eines BCM nach § 91 Abs. 2 AktG	43
2.2.2	Rechtspflicht zur Einführung eines BCM nach §§ 76, 93 AktG bzw. § 43 GmbHG	44
2.2.3	Krisenfrüherkennung nach § 1 StaRUG	48
2.2.4	Fazit	50
2.3	BCM als Gegenstand der bilanzrechtlichen Berichterstattung	50
2.3.1	Vorgaben des HGB	51
2.3.2	Strafbarkeit nach § 331 HGB	51
2.4	Verrechtlichungstendenzen infolge strafrechtlicher und ordnungswidrigkeitenrechtlicher Vorgaben	52
2.4.1	Strafbarkeit wegen Untreue nach § 266 StGB	52
2.4.2	Weitere Strafbarkeitsrisiken	55
2.5	Compliance und ihr Verhältnis zum BCM	61
2.5.1	Compliance – Bedeutung und Rechtsgrundlagen	61
2.5.2	Folgen mangelhafter Compliance	69
2.5.3	Anforderungen an eine effektive Compliance	70
2.5.4	Parallelen und Schnittmengen von Compliance und BCM	79
2.5.5	Betriebskontinuität als Compliance-Pflicht?	82
2.6	Standardisierte Empfehlungen zum BCM	83
2.7	Fazit	84
3	Spezielle Bereiche des BCM im Krankenhaus und in MVZ-Strukturen	86
3.1	Cybersicherheit	86
3.1.1	Begrifflichkeiten beim Thema Cybersicherheit	86
3.1.2	Angriffsarten, das Big Game Hunting und Cybercrime-as-a-Service	87
3.1.3	Auswirkungen von Cybervorfällen auf Krankenhäuser und MVZ-Strukturen	89
3.1.4	Praxisbeispiele von Cyberangriffen im Gesundheitswesen	90
3.2	Cybersicherheit in Krankenhäusern	92
3.2.1	Verfassungsrechtliche Grundlagen der Cybersicherheit im Gesundheitswesen	92
3.2.2	Unionsrechtliche Regelungen zur Cybersicherheit	93
3.2.3	Krankenhäuser im Anwendungsbereich des BSIG	95
3.2.4	Krankenhäuser nach § 391 SGB V	106
3.2.5	Anforderungen der DS-GVO an Krankenhäuser	109
3.2.6	Künstliche Intelligenz im Krankenhaus: Bedrohungen und Potenziale	113
3.2.7	Personenschäden durch Cybervorfälle in Krankenhäusern	117
3.2.8	Cyberversicherungen aus rechtlicher Sicht	119

3.2.9	Lösegeldzahlungen als Strafbarkeitsrisiko?	120
3.2.10	Cybervorfall und der Kontakt mit Behörden	121
3.2.11	Fazit	121
3.3	Cybersicherheit in MVZ-Strukturen	122
3.3.1	Regelungsgeschichte des § 390 SGB V	123
3.3.2	Personeller Anwendungsbereich des § 390 SGB V	123
3.3.3	Regelungsinhalt des § 390 SGB V	124
3.3.4	Anforderungen der KBV-Richtlinie	125
3.3.5	Zertifizierte Dienstleister nach § 390 SGB V	128
3.3.6	Datensicherheit in MVZ-Strukturen	129
3.3.7	Sanktionen gegen MVZ-Strukturen im Bereich Cybersicherheit	131
3.3.8	Praxishinweise für MVZ-Strukturen	132
3.3.9	Auswirkungen des Digitalgesetzes	132
3.4	KRITIS-Dachgesetz	134
3.4.1	Einleitung zum KRITIS-Dachgesetz	134
3.4.2	Referentenentwurf des KRITIS-Dachgesetzes	135
3.4.3	Folgen für die Zukunft	138
3.5	Krankenhausalarm- und -einsatzplanung	139
3.5.1	Rechtsgrundlagen der KAEP	140
3.5.2	Inhalt des Handbuchs/Etablierung KAEP	141
3.5.3	Rechtsfolgen einer ineffektiven KAEP und der Blick in die Zukunft	146
3.6	Brandschutz im Krankenhaus	147
3.6.1	Einführung zum Brandschutz	147
3.6.2	Besondere Rechtsgrundlagen für den Brandschutz ...	149
3.6.3	Vorschriften für Leitungsorgane	150
3.6.4	Brandschutzleitfäden ohne Normcharakter	151
3.6.5	Umsetzung des Brandschutzes im Krankenhaus	151
3.7	Priorisierungssituationen im Krankenhaus	153
3.7.1	Einführung	153
3.7.2	Strafrechtliche Bewertung von Triage-Entscheidungen	154
3.7.3	Triage in der Pandemie	155
3.7.4	Folgen für das Krankenhaus	156
4	Der Cyberangriff aus Sicht der Staatsanwaltschaft	157
4.1	Erscheinungsformen aktueller Ransomware-Gruppierungen	157
4.2	Ermittlungen bei Ransomware-Angriffen – Art, Umfang und Zuständigkeiten	159
4.3	Warum sich Strafanzeigen lohnen	161
5	Versicherungslösungen für Krankenhäuser	165
5.1	Risiken durch Cyber-Angriffe steigen	165
5.2	Große Risiken durch Datenschutzverletzungen	168
5.3	Die Cyberversicherung als »Allheilmittel«?	168

5.4	Welche Voraussetzungen müssen für eine Cyberversicherung erfüllt sein?	171
5.5	Voraussetzungen für den Leistungsfall	172
5.6	Ersetzt eine D&O-Versicherung die Cyberversicherung?	173
5.7	Benötigt ein Krankenhaus eine eigenständige Vertrauensschadenversicherung?	174
5.8	Fazit	175
6	BCM in der Praxis	176
6.1	Einleitende Ausführungen zu BCM aus praktischer Sicht	176
6.1.1	Ziel der Implementierung eines BCMS	177
6.1.2	Funktionsweise des BCM	178
6.2	Organisationsstruktur im BCM	178
6.2.1	Strategische Ebene	178
6.2.2	Taktische Ebene	180
6.2.3	Operative Ebene	181
6.3	BCM-Programm	181
6.3.1	Initiierung	183
6.3.2	Analysephase	184
6.3.3	BC-Lösungskonzept	189
6.3.4	Implementierung risikomindernder Maßnahmen	195
6.3.5	Planung	197
6.3.6	Validierung	199
6.3.7	Schulung und Awareness	200
6.4	Fazit	202
7	Fazit – kurz gefasst	203
Verzeichnisse		205
Abkürzungsverzeichnis	205	
Literaturverzeichnis	209	
Stichwortverzeichnis	214	