Inhalt

Die Autoren **9**

Vorwort **13**

1 Zum Umgang mit dem Leitfaden **15**

2 Lerninhalte der NIS-2-Schulungspflicht **17**

3 Einführung in das NIS-2-Umsetzungsgesetz **20**

3.1 Geschäftsleitungspflichten 21
3.2 Risikomanagement 22
3.3 Registrierungspflicht 23
3.4 Meldemechanismen inkl. Unterrichtungspflicht 24
3.5 Nachweispflicht 24

4 Gefährdungslage im Gesundheitswesen **25**

4.1 Allgemeine Risikofaktoren 25
4.2 Typische Angriffe 28
4.3 Beispiele 29

5 Betroffenheit nach dem NIS-2-Umsetzungsgesetz **32**

5.1 Anwendungsbereich des BSIG unter der alten EU NIS-Richtlinie 32
5.2 Betroffenheitsbereich nach EU NIS-2 33

5.3	Betroffene Teilsektoren im Gesundheitswesen	34
5.3.1	Einrichtungen aus dem Sektor Gesundheit in Anlage I	34
5.3.2	Weitere betroffene Einrichtungen aus dem Gesundheitswesen	37
5.4	Sondervorschriften bei der Betroffenheitsprüfung	37
6	**Risikomanagement nach dem NIS-2-Umsetzungsgesetz und B3S Krankenhaus**	**39**
6.1	Allgemeines	39
6.1.1	Gesetzliche Anforderungen: NIS-2 und das neue BSIG	39
6.1.2	Bezug zu § 8a und § 39 BSIG	42
6.1.3	Verzahnung mit dem B3S Krankenhaus	43
6.1.4	Risikobasierter Ansatz statt formaler Compliance	44
6.1.5	Die Rolle des ISMS	45
6.1.6	Verzahnung mit dem klinischen Risikomanagement	46
6.2	Identifikation, Analyse und Bewertung von Informationssicherheitsrisiken	47
6.2.1	Asset-basierter vs. prozessbasierter Ansatz	47
6.2.2	Schutzbedarfsfeststellung	48
6.2.3	Kritische Versorgungsprozesse im Krankenhaus	49
6.2.4	Abhängigkeiten zwischen IT, Medizintechnik und Gebäudetechnik	50
6.2.5	Dokumentation: Risikoregister und Maßnahmenplan	51
6.2.6	Management-Reporting	51
6.2.7	Mögliche Werkzeuge	52

6.3	Praktische Übungen und Fallbeispiele	52
6.3.1	Szenario 1: Ransomware im Krankenhausinformationssystem (KIS)	53
6.3.2	Szenario 2: Stromausfall mit teilweisem Systemversagen im Notstrombetrieb	54
6.3.3	Szenario 3: Fehlkonfiguration im Identity- und Berechtigungsmanagement	54
6.3.4	Szenario 4: Ausfall eines externen IT-Dienstleisters bzw. Cloud-Anbieters	55
6.3.5	Szenario 5: Technisch bedingter Ausfall einer zentralen medizinischen Fachanwendung	56
6.3.6	Szenario 6: Störung der Telematikinfrastruktur und ihrer Dienste	57
6.3.7	Szenario 7: Innentäter	59
7	**Melde- und Unterrichtungspflicht nach dem neuen BSIG**	**61**
8	**Weitere Rechtspflichten im neuen BSIG**	**64**
9	**Pflichten und Haftung der Geschäftsleitung**	**65**
9.1	Geschäftsleitungsverantwortung	66
9.2	Regresspflicht der Geschäftsleitung	68
9.3	Schulungspflicht der Geschäftsleitung	68
9.4	Compliance-Verantwortung des Aufsichtsorgans	69
10	**Aufsichtsmaßnahmen nach dem neuen BSIG**	**70**
11	**Sanktionen nach dem NIS-2-Umsetzungsgesetz**	**71**
12	**Zusammenspiel mit dem KRITIS-Dachgesetz**	**73**
12.1	Risikoanalyse & Bewertung	74

12.2 Resilienzplanung & Maßnahmen 74
12.3 Durchführung von Schulungen und Übungen 75
12.4 Krisenmanagement & Kommunikation 75

13 BSIG und SGB V 77

14 Wechselwirkung zur Krankenhausalarm- und Einsatzplanung 79

15 Patientenschäden aufgrund eines Cybersicherheitsvorfalls 81

16 EU NIS-2-Richtlinie und Datenschutz 84

17 Cyberversicherung unter NIS-2 88

18 Rechtliche Bewertung von Lösegeldzahlungen 92

19 Best Practices zum Umgang mit einer Krise 94

19.1 Der Incident-Response-Plan als Grundlage 94
19.2 Der Krisenstab: Zusammensetzung und Aktivierung 95
19.3 Rollen und Verantwortlichkeiten 96
19.4 Kontaktlisten und Alarmierung 97
19.5 Übungen: Tabletop und darüber hinaus 98
19.6 Weitere proaktive Vorbereitungsmaßnahmen 99