Bild: iStock.com/Morsa Images

Was sagen die gesetzlichen Vorgaben zur IT-Sicherheit im Gesundheitsbereich in Deutschland aktuell? Hier tut sich tatsächlich gerade einiges.

Sicherheit der Verarbeitung

IT-Sicherheit in Krankenhäusern und Arztpraxen

Großes oder kleines Krankenhaus, große oder kleine Arztpraxis? Je nachdem gelten andere gesetzliche Vorgaben für die IT-Sicherheit. Die Richtlinien, Muster und Priorisierungen sind auch für weitere schweigepflichtige Berufe und kleine Unternehmen interessant.

Durch die Festlegungen der BSI-Kritisverordnung (BSI-KritisV) vom 22. April 2016 (BGBL I, 598; geändert BGBl I, 1903) fallen Kliniken mit mehr als 30.000 stationären Aufnahmen pro Jahr unter die KRITIS-Regeln im BSI-Gesetz (BSIG).

Große Krankenhäuser

Danach müssen diese Kliniken mindestens alle zwei Jahre durch Sicherheitsaudits, Prüfungen oder Zertifizierungen nachweisen, dass sie angemessene organisatorische und technische Vorkehrungen treffen, um Störungen zu vermeiden bei der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit der Kritischen Infrastrukturen maßgeblich sind, die sie betreiben.

Die Ergebnisse einschließlich der aufgedeckten Sicherheitsmängel müssen sie an das BSI übermitteln (§ 8a BSIG).

Darüber hinaus hat die deutsche Krankenhausgesellschaft einen branchenspezifischen Sicherheitsstandard (B3S) für die Informationssicherheit im Krankenhaus erstellt und mit dem BSI abgestimmt. Er ist gemäß Feststellungsbescheid des BSI vom 22.10.2019 geeignet, um die Anforderungen nach § 8a Abs. 1 BSIG in Krankenhäusern zu gewährleisten. Damit ist ein Sicherheitsstandard für die großen Krankenhäuser verfügbar (abrufbar unter https://ogy.de/downloads-b3s; Orientierungshilfe des BSI zu den Nachweisen nach § 8a Abs. 1 BSIG siehe https://ogy.de/oh-nachweise-bsig).

Kleine Krankenhäuser

Das Patientendaten-Schutz-Gesetz vom 14. Oktober 2020 (BGBl. I, 2115) hat mit § 75c Anforderungen an die IT-Sicherheit in Krankenhäusern, die keine kritische Infrastruktur sind, in das Sozialgesetzbuch (SGB) V aufgenommen. Diese Regelungen sind ab 1. Januar 2022 anzuwenden.

Krankenhäuser müssen nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen treffen, um Störungen zu vermeiden bezüglich der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind. Dies kann insbesondere durch die Anwendung des B3S für Krankenhäuser erfolgen. Anpassungen an den Stand der Technik müssen mindestens alle zwei Jahre erfolgen.

Praxen

Das Digitale-Versorgung-Gesetz (DVG) vom 9. Dezember 2019 hat § 75b in das SGB V eingefügt. Danach mussten die Kassenärztlichen Bundesvereinigungen (Kassenärztliche Bundesvereinigung = KBV und Kassenzahnärztliche Bundesvereinigung = KZBV) bis zum 30. Juni 2020 in einer Richtlinie die Anforderungen zur Gewährleistung der IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung festlegen.

Die Richtlinien sind, wenn auch verspätet, Anfang 2021 in Kraft getreten (abrufbar unter https://hub.kbv.de/site/its und www.kzbv.de/it-sicherheitsrichtlinie.1475.de.html).

Die beiden wörtlich identischen Richtlinien sind mit dem BSI abgestimmt. Sie

<table>
<tr><td colspan="2"></td><td>Kleine Krankenhäuser
Bis zu 30.000
stationäre Fälle/Jahr</td><td>Große Krankenhäuser
Mehr als 30.000
stationäre Fälle/Jahr</td></tr>
<tr><td colspan="2"></td><td>angemessene Vorkehrungen
nach § 75c SGB V
insb. auch B3S Krankenhaus
(Umsetzung ab 1.1.2022)</td><td>§ 8a Abs. 1 BSIG oder
B3S Krankenhaus oder
ISO 27001
(erstmalig bis zum 30.6.2019)</td></tr>
<tr><td>Kleine Praxis
Bis zu 5 Personen ständig mit Datenverarbeitung betraut</td><td>Mittlere Praxis
6 bis 20 Personen ständig mit Datenverarbeitung betraut</td><td>Große Praxis
Mehr als 20 Personen ständig mit Datenverarbeitung betraut oder sehr umfangreiche DV</td><td></td></tr>
<tr><td colspan="3">Anlagen 1, 5 und, falls entsprechende Großgeräte vorhanden, Anlage 4 der RL nach § 75b SGB V</td><td></td></tr>
<tr><td></td><td colspan="2">Zusätzlich Anlage 2 der RL</td><td></td></tr>
<tr><td colspan="2"></td><td>Zusätzlich Anlage 3 der RL</td><td></td></tr>
<tr><td colspan="3">Umsetzung je nach Vorgabe ab 1.4.2021, 1.7.2021, 1.1.2022 oder 1.7.2022</td><td></td></tr>
<tr><td colspan="3">Alternativ: Vorkehrungen nach § 8a Abs. 1 BSIG oder B3S Krankenhaus</td><td></td></tr>
</table>

Übersicht über die Vorgaben für Krankenhäuser und Praxen zur Umsetzung angemessener organisatorischer und technischer Vorkehrungen, um die IT-Sicherheit zu gewährleisten

müssen jährlich in Zusammenarbeit mit dem BSI an den Stand der Technik und an das Gefährdungspotenzial angepasst werden. Darüber hinaus müssen der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, die Bundesärztekammer, die Bundeszahnärztekammer, die Deutsche Krankenhausgesellschaft und die für die Wahrnehmung der Interessen der Industrie maßgeblichen Bundesverbände aus dem Bereich der Informationstechnologie im Gesundheitswesen bei der Erstellung und Anpassung angehört werden.

Modulare IT-Sicherheitsmaßnahmen

Die IT-Sicherheitsmaßnahmen sind modular nach Praxisgröße und Ausstattung der Praxis (Großgeräte) gruppiert. Sie gliedern sich in die Gruppen

- Software und Internet,
- Hardware inkl. Netz sowie
- Großgeräte & Telematik (Konnektoren).

Die Maßnahmen geben abstrakt vor, was die Praxen bedenken müssen. Während eine „Regelmäßige Datensicherung" (A1.14 = Anlage 1 Nr. 14) für alle Praxisgrößen Pflicht ist, empfehlen die Richtlinien eine „Datenträgerverschlüsselung" (A3.10) nur für Wechseldatenträger in Großpraxen. Eine Verschlüsselung von Patientendaten müsste für alle Praxen Pflicht sein. Eine Verschlüsselung in der Cloud ist für alle Pflicht (A1.10). Die Hälfte der zusätzlichen Maßnahmen für die Großpraxen beziehen sich auf Mobile Device Management.

Für zwei Bereiche fordern die Maßnahmen, Richtlinien zu erstellen: für den Einsatz mobiler Geräte (A2.6, A2.8 und A3.1) und für die Nutzung von Wechseldatenträgern (A2.10). Für beide Bereiche gibt es Musterrichtlinien auf der Themenseite der KBV. Für die Erstellung eines Netzwerkplans (A1.33) findet sich ebenfalls ein Muster, allerdings nur als PDF-Datei. Außerdem seien die jeweiligen FAQ auf den Informationsseiten der KBV und der KZBV dringend empfohlen (https://ogy.de/kbv-faq, https://ogy.de/kzbv-faq).

Zertifizierung

Eine dritte Richtlinie regelt die Zertifizierung von Personen, die im Rahmen von Dienstleistungen die Praxen bei der Umsetzung der Richtlinie sowie bei zukünftigen Anpassungen unterstützen oder die die Geräte zur Verbindung mit der Telematikinfrastruktur installieren oder warten. Die Richtlinie beschreibt die fachlichen Voraussetzungen, die Prüfung und eine Anerkennung von anderen Zertifizierungen (z.B. BSI Grundschutz-Auditor).

Optimierungen

Die Formulierungen in den Erläuterungen unterteilen die Maßnahmen für Praxen in „muss"- und „sollte"-Regeln. Hier ist eine sprachliche Überarbeitung sinnvoll. Denn „sollte" ist immer vorhanden, „muss" fehlt manchmal (z.B. A1.1).

Es wäre generell sicherlich sinnvoll, die Regelungen für Krankenhäuser und Praxen zu vereinheitlichen. Denn die Praxen müssen ebenfalls die technisch-organisatorischen Aspekte des Datenschutzes berücksichtigen. So geben die Richtlinien für Praxen z.B. keinen Schutz der Vertraulichkeit durch Verschlüsselung bei der Dateiablage vor. Auch müssten die Vorgaben datenschutzkonforme Begriffe (z.B. schreibt A1.18 „persönliche Daten") verwenden.

Prof. Dr. Rainer W. Gerling ist Autor und Referent sowie stellvertretender Vorsitzender des Vorstands der GDD e.V. Er lehrt IT-Sicherheit an der Hochschule München.