www.krankenhaus-it.de ISSN 1619-0629 Preis: 17,50 Euro

Ausgabe 4&5 / 2024

Krankenhaus-IT JOURNAL

Fakten und Perspektiven der IT im Gesundheitswesen

KH-IT Herbsttagung 2024: Patientenportal, Ambulantisierung und Wertbeitrag

Bundesverband der Krankenhaus IT-Leiterinnen / Leiter e. V.

ENTSCHEIDERFABRIK

IHE DEUTSCHLAND Integrating the Healthcare Enterprise

KRITISCher Stammtisch IT-Sicherheit im Sektor Gesundheitswesen

NIS-2-Richtlinie und ISMS: Optimierung der IT-Sicherheit in Krankenhäusern

Die fortschreitende digitale Transformation erhöht die Risiken für Datensicherheit und Systemintegrität. Besonders in Krankenhäusern spielt IT-Sicherheit eine zentrale Rolle, da hier hochsensible Gesundheitsdaten verarbeitet werden: die Patientendaten müssen geschützt, die Systemausfälle vermieden, Cyberangriffe abgewehrt und Datenverluste verhindert werden. Dies deutet darauf hin, dass im Zuge der Digitalisierung und der zunehmenden Informationsflut Krankenhäuser stärker denn je auf zuverlässige IT-Sicherheit angewiesen sind.

Von Dr. Timo Braun, Senior Berater, Curacon GmbH Wirtschaftsprüfungsgesellschaft und Sanovis GmbH, und Natalia Ermanis, Senior Beraterin, Curacon GmbH Wirtschaftsprüfungsgesellschaft

Stand der IT-Sicherheit in deutschen Krankenhäusern

Laut den Ergebnissen des Digital Radar Krankenhaus 2022, der den Digitalisierungsgrad der deutschen Krankenhäuser abbildet und bei dem IT- und Informationssicherheit eine von vier bewerteten Dimensionen darstellt, erfüllten 67 % der Krankenhäuser mehr als 50 % der Anforderungen in dieser Dimension. Dennoch erreichten lediglich 4 Einrichtungen von insgesamt 1.624 Häusern den Reifegrad 5 des EMRAM-Referenzmodells. Dies deutet auf eine Diskrepanz zwischen dem allgemeinen Digitalisierungsgrad und der Erfüllung der IT- und Informationssicherheitsanforderungen hin. Auch Krankenhäuser mit hohem Digitalisierungsreifegrad könnten daher trotz fortschrittlicher Digitalisierung Sicherheitslücken aufweisen.

Des Weiteren wird deutlich, dass IT-Sicherheit ein fortlaufender Prozess und kein einmaliges Projekt ist. Regelmäßige Überwachung und kontinuierliche Verbesserung sind unerlässlich, um Sicherheitslücken zu identifizieren und zu schließen. Daher sollten sich alle Krankenhäuser, unabhängig von ihrem Digitalisierungsgrad, intensiv mit IT-Sicherheit auseinandersetzen, um möglichen Sicherheitsrisiken auch bei fortschrittlicher Digitalisierung proaktiv zu begegnen. Ein geregelter Sicherheitsprozess muss etabliert werden, der auf Leitungsebene initiiert und gesteuert wird.

Gewährleistung eines Rechtsrahmens für ein hohes gemeinsames Sicherheitsniveau

Von regulatorischer Seite kommt außerdem eine weitere Vorgabe zur Netzwerk- und Informationssicherheit, die die Bedeutung der IT-Sicherheit auf ein neues Niveau hebt. Die seit Januar 2023 geltende NIS-2-Richtlinie, die bis Oktober 2024 in nationales Recht umgesetzt werden muss, ersetzt die NIS-1-Richtlinie und legt die Anforderungen an die Informationssicherheit unter anderem für Krankenhäuser fest. In Deutschland wird sie durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) umgesetzt.

Die NIS2-Richtlinie und das NIS2UmsuCG stellt den überarbeiteten Rahmen der Europäischen Union zur Gewährleistung der Sicherheit von Netz- und Informationssystemen dar. Es wird darauf abgezielt, die Abwehr der EU gegen Cyber-Bedrohungen zu stärken und ein hohes gemeinsames Niveau der Cybersicherheit in den Mitgliedstaaten sicherzustellen. Die Schlüsselanforderungen der NIS-2-Richtlinie in Krankenhäusern lassen sich im folgenden Überblick kurz zusammenfassen:

Schlüsselanforderungen	Beschreibung
Erhöhung der Risikomanagement-maßnahmen	Es sind technische und organisatorische Maßnahmen zu erfüllen. Gesundheitseinrichtungen, die B3S noch nicht eingeführt haben, müssen die in der NIS-2-Richtlinie vorgeschriebenen Maßnahmen umsetzen.
Gewährleistung der Geschäftskontinuität	NIS-2 legt den Schwerpunkt auf die Widerstandsfähigkeit kritischer Infrastrukturen und Dienste, wodurch das Business Continuity Management nicht nur auf die Vorbereitung und Reaktion auf Vorfälle abzielt, sondern auch die Fähigkeit zur Bewältigung von Cyberangriffen stärkt.
Verantwortung der Geschäftsleitung	Die Geschäftsleitung trägt die volle Verantwortung für Cyber-Security-Maßnahmen und muss künftig verpflichtend an Cyber-Security-Schulungen teilnehmen.
Dreistufige Meldepflicht	Mit der Umsetzung der NIS-2-Richtlinie ist eine dreistufige Meldepflicht gegenüber dem BSI erforderlich. Die Angaben hinsichtlich des erheblichen Sicherheitsvorfalls variieren je nach Einrichtung.
Nachweispflicht	Betreiber von kritischen Anlagen müssen nach Inkrafttreten des NIS2UmsuCG alle drei Jahre die Einhaltung der Risikomanagementmaßnahmen vor dem BSI nachweisen.
Sanktionen und persönliche Haftung	Je nach Einrichtung drohen bei Nichteinhaltung der Pflichten Geldbußen von bis zu zehn Millionen Euro. Anders als bei Datenschutzvorfällen, wird nach dem NIS2UmsuCG die Geschäftsleitung persönlich in Anspruch genommen.

Abbildung 1 Die Anforderungen der NIS-2-Richtlinie auf einen Blick

Besonders hervorzuheben ist die persönliche Haftung der Geschäftsführung, die im aktuellen Entwurf des Bundesinnenministeriums vorgesehen ist. So sind die Geschäftsführungen zur Genehmigung und Überwachung der Durchführung von Maßnahmen zum Risikomanagement im Bereich der Informationssicherheit verpflichtet. Kommen sie dieser Verantwortung nicht nach und ist ein IT-Sicherheitsvorfall auf die Nichteinhaltung der Sicherheitsanforder-ungen zurückzuführen, können sie hierfür haftbar gemacht werden.

In Deutschland übernimmt das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine zentrale, kooperative Rolle und agiert als integraler Bestandteil der Cybersicherheitsarchitektur auf staatlicher Ebene. Das BSI legt u. a. die gesetzlich verankerten Sicherheitsstandards fest. Die Sicherheitsanforderungen sowie der erforderliche „Stand der Technik" für informa-tionstechnische Systeme in den Krankenhäusern werden im Branchenspezifischen Sicherheitsstandard (B3S) erfasst. Der B3S beinhaltet die gesetzlich geforderten Maßnahmen zur Informationssicherheit und spiegelt u. a. alle organisatorischen und technischen Maßnahmen ab, die die NIS-2-Richtlinie vorgibt.

Hilfsmittel zum technischen und organisatorischen Aufbau eines Informationssicherheitssystems

Ein prozessorientiertes Informationssicherheitssystem (ISMS) nach der Sicherheitskonzeption des B3S ermöglicht einem Krankenhaus die Einführung einer systematischen Vorgehensweise zur Erreichung des erforderlichen Sicherheitsniveaus, der Beobachtung und der kontinuierlichen Verbesserung der IT-Sicherheitsprozesse.

Fazit

Mit der Einführung von NIS-2 gewinnt die Implementierung eines ISMS zunehmend an Bedeutung. Das BSI stellt dafür geeignete Mechanismen als Grundlage zur Verfügung. Dazu zählen unter anderem branchenspezifische Sicherheitsstandards (B3S), das Business Continuity

Management (BSI-Standard 200-4), Anforderungs- und Maßnahmenkataloge sowie weitere Hilfsmittel wie Dokumentenvorlagen und Auswertungsbögen, die dazu beitragen, ein robustes IT-Sicherheitssystem zu etablieren, das Unternehmensprozesse vor Cyberangriffen schützt. Dabei ist besonders hervorzuheben, dass IT-Sicherheit als fortlaufender Prozess verstanden wird, der kontinuierlich überwacht und optimiert werden muss. Die Verantwortung hierfür liegt durch die NIS-2 Richtline direkt bei der Geschäftsführung.

Natalia Ermanis, Senior Beraterin, Curacon GmbH Wirtschaftsprüfungsgesellschaft und

Dr. Timo Braun, Senior Berater, Curacon GmbH Wirtschaftsprüfungsgesellschaft und Sanovis GmbH