Krankenhauszukunftsgesetz fordert Maßnahmen für IT-Sicherheit:

WORAUF KRANKENHÄUSER BEI DER BEDARFSANMELDUNG ACHTEN MÜSSEN

Während der Fördertatbestand 10 sich ausschließlich mit der IT- und Cybersicherheit befasst, müssen bei den Fördertatbeständen 1 bis 9 und 11 mindestens 15 Prozent der beantragten Leistungen aus dem Krankenhauszukunftsgesetz (kurz KHZG) in Maßnahmen der IT- und Cybersicherheit fließen – so will es der Gesetzgeber (gemäß Nr. 5.2 in der Förderrichtlinie nach § 21 Abs. 2 KHSFV). Für Krankenhäuser heißt das, dass sie konkrete Maßnahmen einplanen müssen, wenn sie von den vom Bund für die Krankenhausinfrastruktur bereitgestellten Mitteln in Höhe von insgesamt 4,3 Milliarden Euro profitieren wollen. Die Krux: „Wenn Krankenhäuser beispielsweise planen, ein neues Patientenportal durch die Förderung zu implementieren, haben sie dabei oft die IT-Sicherheit gar nicht auf dem Schirm und riskieren damit die Ablehnung der Bedarfsanmeldung", sagt Thomas Althammer, Geschäftsführer der Althammer & Kill GmbH & Co. KG. „Die Investitionen in die Sicherheit der Systeme sind aber extrem wichtig. Anders als beim Krankenhausstrukturfonds werden hierbei auch kleinere Häuser berücksichtigt, denn gerade die Corona-Pandemie hat gezeigt, dass sie eine enorme Rolle bei der Abwehr nationaler Bedrohungslagen spielen. Aber gerade diese Krankenhäuser sind in Sachen IT-Sicherheit oft nicht gut aufgestellt." Laut einer Umfrage der Unternehmensberatung Roland Berger vom Mai 2017 wurden bereits zwei Drittel aller Krankenhäuser Opfer eines Hackerangriffs, welche nicht nur hochsensible Patientendaten gefährden, sondern bei Komplettausfall der IT-Systeme auch eine Gefahr für Leib und Leben darstellen können.

Wie können die Projektvorhaben in den verschiedenen Fördertatbeständen konkret um IT-Sicherheitsmaßnahmen ergänzt werden?

Krankenhäuser müssen den Status quo der IT-Systeme bewerten und mit gezielten Maßnahmen die Sicherheit erhöhen. Vorhaben zur Prävention und Detektion von Informationssicherheitsvorfällen, die Steigerung und Aufrechterhaltung des Bewusstseins gegenüber IT-Vorfällen sowie die Bedeutung von IT- und Cybersicherheit und der Aufbau eines Informationssicherheitsmanagementsystems (nach ISO 27001/BSI IT-Grundschutz[1] und weiterer Sicherheitsstandards (B3S)) stehen dabei besonders im Fokus. Folgende konkrete Maßnahmen sollten bei der Förderung nach dem KHZG Berücksichtigung finden:

1. Erstellung von Berechtigungs- und IT-Sicherheitskonzepten
2. Risikomanagement und Datenschutz-Folgenabschätzungen
3. Security-Awareness und Penetrationstests
4. Einführung Informationssicherheitsmanagementsysteme nach ISO 27001 und B3S

Die Prävention muss Hand-in-Hand gehen mit konkreten Handlungsplänen für den Fall von Cyberangriffen. Insbesondere im Krankenhausumfeld muss der reibungslose Ablauf aller Systeme Tag und Nacht gewährleistet sein. Ein stichhaltiges und wirksames IT-Notfallmanagement nach BSI 200-4 aufzubauen und zu etablieren ist dabei essenziell.

Fazit

Krankenhäuser müssen schon bei den Bedarfsanmeldungen für Fördermittel nach dem KHZG konkrete Maßnahmen zur Erhöhung der IT- und Cybersicherheit mit einbeziehen. Denn Ziel ist es, die Verfügbarkeit, die Integrität und die Vertraulichkeit für alle informationstechnischen Systeme, Komponenten und Prozesse im Krankenhaus sicherzustellen. ■

[1] *https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Managementsystemzertifizierung/Zertifizierung27001/GS_Zertifizierung_node.html*

Weitere Details unter:
www.althammer-kill.de/khzg

Leistungen, die Althammer & Kill zu den Fördertatbeständen 10, 1 bis 9 und 11 anbietet. (Quelle: Althammer & Kill GmbH & Co. KG)