Pressemitteilung

IT-Sicherheit ist Patientensicherheit 14. Dezember 2020

TÜV SÜD: Krankenhäuser jetzt fit für das Patientendaten-Schutz-Gesetz machen

München. Im Rahmen des Konjunkturpakets zur Bewältigung der Corona-Pandemie stellt die Bundesregierung mit dem Krankenhauszukunftsgesetz 3 Milliarden Euro bereit, um digitale Technologien an Krankenhäusern zu fördern – weitere 1,3 Milliarden Euro schießen die Länder und Klinikträger zu. Ein idealer Zeitpunkt, um auch die IT-Sicherheit in Krankenhäusern zu verbessern, erklärt Jens Linstädt, Product Compliance Manager Healthcare der TÜV SÜD Management GmbH – zumal ab 2022 angemessene Maßnahmen zur Datensicherheit für alle Krankenhäuser verpflichtend werden.

In Sachen Digitalisierung schneiden deutsche Krankenhäuser im internationalen Vergleich nicht gut ab. Der Digitalisierungsgrad liegt, laut Krankenhausreport 2019, bei 33 Prozent – in vielen anderen Ländern Europas laufen dagegen schon die Hälfte der Prozesse in Krankenhäusern digital ab. Krankenhäuser geraten zudem immer häufiger ins Visier von Cyberkriminellen. Ein damit verbundener IT-Ausfall kann gravierende Folgen haben, beispielsweise wenn lebensbedrohlich erkrankte Patienten erst später behandelt werden können oder Neuaufnahmen von Patienten nicht möglich sind. Sind die IT-Sicherheitsmaßnahmen immer auf dem neuesten Stand, können solche Risiken minimiert werden. Daher gilt ab 1. Januar 2022 auf Basis des Patientendaten-Schutz-Gesetzes, dass alle Krankenhäuser, egal welcher Größe, „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse“ treffen müssen.

Branchenspezifischer Sicherheitsstandard (B3S) für alle Kliniken

Bisher sind nur Kliniken mit mehr als 30.000 vollstationären Fällen pro Jahr dazu verpflichtet, geeignete IT-Sicherheitsmaßnahmen zu treffen, die § 8a des Gesetzes des Bundesamts für Sicherheit in der Informationstechnik (BSI) entsprechen. Diese Kliniken gehören zur „Kritischen Infrastruktur“ (KRITIS). Durch Gesetzesbeschluss von September 2020 müssen künftig auch kleinere Kliniken dem Stand der Technik angemessene, organisatorische und technische Vorkehrungen zur IT-Sicherheit treffen – dies regelt der neue Paragraf 75c Sozialgesetzbuch V (SGB V).

Der Paragraf empfiehlt ausdrücklich den branchenspezifischen Sicherheitsstandard (B3S) der Deutschen Krankenhausgesellschaft (DKG), der alle zwei Jahre revisioniert wird. In seiner nächsten Version soll er spezielle Regelungen für all jene Krankenhäuser enthalten, die unter dem Schwellenwert gemäß KRITIS-Verordnung liegen. Dies soll kleineren Kliniken helfen, die Maßnahmen zur Verbesserung ihrer IT-Sicherheit nach anerkanntem Standard umsetzen zu können.

Krankenhäuser sollten jetzt ihre IT-Sicherheitsmaßnahmen überprüfen

„Krankenhäuser sollten schnellstmöglich damit beginnen, angemessene IT-Security-Maßnahmen zu treffen oder diese zu aktualisieren, denn die gesetzte Frist bis zum 1. Januar 2022 klingt fern, ist aber knapp. Wir empfehlen dringend, sich am B3S zu orientieren“, sagt Jens Linstädt von der TÜV SÜD Management Service GmbH. Haben sie Maßnahmen zur IT-Sicherheit ergriffen, müssen Krankenhäuser diese spätestens alle zwei Jahre auf den aktuellen Stand der Technik prüfen. Zwar besteht für Nicht-KRITIS-Krankenhäuser keine Nachweis- oder Meldepflicht, trotzdem rät der Experte zu einer externen Prüfung, zum Beispiel durch TÜV SÜD: Im Schadensfall gilt sie als stichhaltiger Beleg für angemessene IT-Sicherheitsmaßnahmen und kann dadurch Haftungsrisiken für die Klinik minimieren.

Da sich der B3S inhaltlich am Informationssicherheits-Managementsystem ISO/IEC 27001 (ISMS) orientiert, ist es sinnvoll, bestehende Maßnahmen in ein solches Managementsystem einzubetten. Ein ISMS erleichtert außerdem die kontinuierliche Anpassung der IT-Sicherheitsmaßnahmen an geänderte Rahmenbedingungen. Für den Nachweis der Maßnahmen ist eine Zertifizierung nach ISO/IEC 27001 nicht erforderlich, aber sinnvoll und hilfreich.

Fördermöglichkeiten frühzeitig beantragen

Die anfangs erwähnten Fördermittel im Rahmen des Krankenhauszukunftsgesetzes beinhalten auch Unterstützung bei organisatorischen und technischen Maßnahmen im IT-Sicherheitsmanagement. Krankenhausträger sollten diese Fördermöglichkeiten frühzeitig beantragen, da die verfügbaren Mittel anteilig zugewiesen werden, bis sie ausgeschöpft sind. Informationen dazu finden sich auf den Websites des Bundesministeriums für Gesundheit und des Bundesministeriums der Justiz und für Verbraucherschutz. Anfang Dezember veröffentlichte das Bundesamt für Soziale Sicherung zudem neue Förderrichtlinien. Demzufolge müssen Krankenhäuser, wenn sie Fördermittel aus dem Krankenhauszukunftsfonds für Digitalisierungsprojekte beantragen, den Erfolg nachweisen. Belegbar ist dies beispielsweise durch eine Zertifizierung nach ISO 27001 oder eine Prüfung nach B3S.

Weitere Infos zur IT-Sicherheit nach §75C SGB V für Krankenhäuser: www.tuvsud.com/ghw-it-sicherheit.

Pressekontakt:

Sabine Krömer TÜV SÜD AG Unternehmenskommunikation Westendstr. 199, 80686 München	Tel. +49 (0) 89 / 57 91 – 29 35 Fax +49 (0) 89 / 57 91 – 22 69 E-Mail sabine.kroemer@tuvsud.com Internet www.tuvsud.com/de

Im Jahr 1866 als Dampfkesselrevisionsverein gegründet, ist TÜV SÜD heute ein weltweit tätiges Unternehmen. Mehr als 25.000 Mitarbeiter sorgen an über 1.000 Standorten in rund 50 Ländern für die Optimierung von Technik, Systemen und Know-how. Sie leisten einen wesentlichen Beitrag dazu, technische Innovationen wie Industrie 4.0, autonomes Fahren oder Erneuerbare Energien sicher und zuverlässig zu machen. www.tuvsud.com/de