Anforderungen an IT-Sicherheit steigen

Das Thema IT-Sicherheit betrifft schon lange nicht mehr nur Technologieunternehmen, Geheimdienste oder Regierungsorganisationen. Gerade für Krankenhäuser ist die IT-Sicherheit von enormer Bedeutung. Mit Gesundheitsdaten verarbeiten Krankenhäuser die denkbar sensibelsten personenbezogenen Daten und sind im Rahmen der Digitalisierung und steigender Informationsintensität mehr denn je auf eine verlässliche IT-Sicherheit angewiesen. Gleichzeitig ist der Mehrwert einer ausgereiften IT-Sicherheit innerhalb einer Organisation nicht immer auf dem ersten Blick ersichtlich. Diese Einschätzung ändert sich jedoch schlagartig, wenn deren Abwesenheit dazu führt oder dazu beiträgt, dass die IT einer Organisation und insbesondere die dazugehörigen Informationen kompromittiert werden. So berichtet der IT-Branchenverband bitkom, dass der deutschen Wirtschaft im Jahr 2020 ein Gesamtschaden von 223 Mrd. € durch Cyberangriffe entstanden ist. Dies ist ein sprunghafter Anstieg zu einem Schaden von je 103 Mrd. € in den Vorjahren 2018 und 2019. Neun von zehn Unternehmen in Deutschland waren 2020/2021 Opfer von Cyberangriffen. Welche Auswirkungen – neben finanziellen Schäden – derartige Angriffe in der Gesundheitswirtschaft erzeugen können, lässt sich an zwei Beispielen der letzten Jahre anschaulich erkennen:

Am Donnerstag, dem 10. September 2020, verschafften sich Hacker unter Ausnutzung einer Sicherheitslücke in der Virtualisierungssoftware Citrix, welche später unter dem Spitznamen „Shitrix“ bekannt wurde, Zugang zu 30 Servern der Uniklinik Düsseldorf. In der Hoffnung auf die Zahlung von Lösegeld in Bitcoins wurden die angegriffenen Server verschlüsselt. Obwohl die Täter, nachdem ihnen klar wurde, dass sie fälschlicherweise ein Krankenhaus und nicht wie geplant die Universität getroffen hatten, einen Schlüssel zur Entschlüsselung der Server bereitstellten, war die Patientenversorgung für längere Zeit stark beeinträchtigt. So musste sich die Uniklinik unter anderem von der Notfallversorgung abmelden und Patienten mussten in umliegende Krankenhäuser umgeleitet werden. Noch Wochen nach dem Cyberangriff war die IT der Uniklinik nicht voll einsatzfähig.

Auch zum Jahresbeginn 2022 wurde ein deutscher Klinikverbund bereits Opfer eines Hackerangriffs. Am Donnerstag, dem 13. Januar 2022, traf es die Kliniken Medizin Campus Bodensee. Als Folge des Cyberangriffs kam es zeitweise zu einem vollständigen Ausfall der IT, woraufhin sich die betroffenen Häuser auch hier von der Notfallversorgung abmelden mussten. Auch die ambulante Behandlung in angeschlossenen MVZs war nicht mehr möglich und es kam zu Absagen von Operationen.

Es wird also deutlich, dass im heutigen Zeitalter Krankenhäuser ohne IT beinahe handlungsunfähig sind und gleichzeitig – beabsichtigt oder zufällig – immer öfter als Ziele von Hackerangriffen ausgewählt werden.

Schutzbedarf geht über kritische Infrastrukturen hinaus

Die Bedrohungen, die von derartigen Angriffen ausgehen können, hat auch der Gesetzgeber erkannt. Aufbauend auf dem im Juli 2015 in Kraft getretenen Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) wurden zum 30. Juni 2017 mit der BSI-KRITIS-Verordnung Krankenhäuser mit mehr als 30 000 vollstationären Fällen pro Jahr dazu verpflichtet, *„angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen“* (§ 8a BSIG). Diese Krankenhäuser sind Teil der kritischen Infrastruktur (KRITIS) Deutschlands und gehören zu *„Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden“* (KRITIS-Definition der Bundesressorts).

Mit der zunehmenden Digitalisierung und kontinuierlich steigenden Vernetzung in der Gesundheitswirtschaft, nicht zuletzt durch das Krankenhauszukunftsgesetz (KHZG), steigt auch das Schadens- und Ausfallrisiko für Krankenhäuser unter dem KRITIS-Schwellenwert. Im Oktober 2020 wurden daraufhin mit dem Patientendaten-Schutz-Gesetz erneut Anpassungen in Bezug auf die IT-Sicherheit vorgenommen, die im § 75c SGB V konkretisiert wurden. In der Folge sind seit dem 1. Januar 2022 nunmehr alle Krankenhäuser verpflichtet, die IT-Sicherheit nach dem Stand der Technik zu gewährleisten. Der „Stand der Technik“ wurde mit dem „Branchenspezifischen Sicherheitsstandard (B3S) für die Gesundheitsversorgung im Krankenhaus“ im Sinne des BSI-Gesetzes erstmals im Oktober 2019 freigegeben und dient seitdem allen Krankenhäusern als anerkannte Leitlinie zur Erhöhung ihrer IT-Sicherheit. Dieser von der Deutschen Krankenhausgesellschaft in Arbeitsgruppen erarbeitete Katalog definiert eine Aufstellung an Anforderungen, welche entsprechend umzusetzen sind, um dem „Stand der Technik“ zu genügen und der Pflicht im Sinne des § 75c SGB V nachzukommen. Als Grundlage orientiert sich der B3S am internationalen Standard ISO 27001.

Der B3S zielt dabei darauf ab, die vier Schutzziele

- Verfügbarkeit (Bereitstehen von Systemen im benötigten Maß)

- Integrität (Verhinderung unautorisierter Modifikation von Informationen)
- Authentizität (Verlässlichkeit von Informationen, insbesondere bezüglich deren Autorenschaft)
- Vertraulichkeit (Schutz vor unbefugter Preisgabe von Informationen)

zu gewährleisten.

Dafür deklariert der B3S Anforderungen an das Risikomanagement und an das Management der Informationssicherheit.

ISMS in Organisationsstruktur integrieren

Kern der Umsetzung des B3S ist die Einführung eines Informationssicherheitsmanagementsystems (ISMS). Hierbei handelt es sich um eine Aufstellung von Verfahren und Regeln einer Organisation, die die Informationssicherheit betreffen. Es geht also nicht originär um ein System im Sinne von reiner Soft- und Hardware, sondern um ein organisatorisches Gebilde, das verschiedene Komponenten beinhaltet, um die Informationssicherheits-Schutzziele zu erreichen. Nichtsdestotrotz kann eine entsprechende Software dabei unterstützen, ein ISMS aufzubauen und zu pflegen.

Der erste Schritt zur Einführung eines ISMS ist das Commitment der Geschäftsführung zu ebendieser, denn einer der größten Erfolgsfaktoren für eine Steigerung der Informationssicherheit ist die Übernahme der Verantwortung für den Themenkomplex durch die oberste Managementebene.

Sobald die Entscheidung gefallen ist, kann mit der Einführung eines ISMS begonnen werden. Dies kann mit externer Unterstützung und/oder insbesondere durch einen bestellten Informationssicherheitsbeauftragten (ISB) geschehen: Hierbei handelt es sich um eine intern definierte Person, deren Aufgabe es ist, die Schutzziele zu gewährleisten. Der Informationssicherheitsbeauftragte ist deshalb organisatorisch direkt der Geschäftsführung zu unterstellen und sollte auch direkt an diese berichten. Dabei ist es möglich, diese Position auch mit externen Personen zu besetzen, also nicht mit Mitarbeitenden des Unternehmens, sondern mit entsprechend qualifizierten Experten, die diese Leistung am Markt anbieten.

Sobald die Organisationsstruktur zur Erarbeitung eines ISMS geklärt ist, ist im nächsten Schritt der Geltungsbereich des individuellen ISMS zu definieren: Welche Bereiche, Prozesse oder Systeme sollen berücksichtigt werden, welche explizit nicht? Kern des Geltungsbereichs müssen die Systeme und Prozesse sein, die zur Erbringung kritischer Dienstleistungen zwingend erforderlich sind. Dafür ist es zunächst erforderlich, die internen (kritischen) Prozesse zu erkennen und zu dokumentieren, um eine bewusste Entscheidung über die Definition des Geltungsbereichs zu treffen.

Weiterhin müssen bestehende, die Informationssicherheit betreffende Risiken identifiziert, bewertet und gewichtet werden. Dafür sind mögliche Bedrohungsszenarien zu skizzieren und deren Eintrittswahrscheinlichkeit und Folgenschwere abzuschätzen. Hierbei liefert der B3S spezifische Risiken und Bedrohungslagen für die Gesundheitsversorgung im Krankenhaus, die über Gefährdungskataloge des BSI (Bundesamt für Sicherheit in der Informationstechnik) hinausgehen.

Eine ausformulierte Leitlinie zur Informationssicherheit unterstützt dabei, den Stellenwert von Informationssicherheit im eigenen Haus zu kommunizieren und den Prozess zur Steigerung ebendieser festzuhalten. Hier kann auf das etablierte Konzept des PDCA-Zyklus aufgebaut werden (Plan – Do – Check – Act, zu Deutsch Planen – Umsetzen – Überprüfen – Handeln). Mithilfe eines solchen Vorgehens kann eine stetige Verbesserung sichergestellt werden, ohne das Ziel aus den Augen zu verlieren. Die Leitlinie ist Bestandteil des Informationssicherheit-Kommunikationskonzeptes, welches insbesondere um Sensibilisierungsmaßnahmen der Mitarbeitenden ergänzt werden sollte (sogenannte Awareness-Maßnahmen).

Sobald Risiken bewertet wurden und der Verbesserungsprozess definiert wurde, kann mit der Bestandsaufnahme der aktuellen Informationssicherheitslage begonnen werden. Hierfür sollten alle rele-

vanten Dokumente gesichtet und Workshops durchgeführt werden, in welchen Vertreter aller Fachbereiche und Abteilungen zur Darstellung der Ausgangslage beitragen können und sollten.

Im Rahmen einer Gap-Analyse kann darauffolgend festgestellt werden, wo die erhobene Ist-Situation noch stark von der zu erreichenden Soll-Situation abweicht. Dadurch lassen sich konkrete Maßnahmen ableiten, die anschließend, beispielsweise in Bezug auf das dahinterstehende Risiko, zu priorisieren und umzusetzen sind. Die Umsetzung der Maßnahmen ist dann gemeinschaftlich sicherzustellen. Dies ist keine alleinige Aufgabe des ISB und/oder der IT-Abteilung, sondern betrifft weitere Fachbereiche und Abteilungen des Krankenhauses gleichermaßen. Im Rahmen des ISMS wird die Umsetzung der Maßnahmen kontinuierlich nachgehalten.

Insgesamt lässt sich feststellen, dass die Einführung eines ISMS einen enormen Mehrwert für Organisationen im Gesundheitswesen darstellt, auch wenn dieser unter Umständen nicht direkt ersichtlich ist, da das Maß für die Effektivität die Vermeidung oder Mitigation von negativen, die Informationssicherheit betreffenden Ereignissen ist. Mit dem Patientendaten-Schutz-Gesetz und den hieraus entstehenden gestiegenen Anforderungen an die IT-Sicherheit müssen deutsche Krankenhäuser das Thema IT-Sicherheit mit hoher Priorität auf ihre Agenda setzen.

IT-Sicherheitsanalyse als sinnvoller erster Schritt

Gerade für Krankenhäuser, die sich nun erstmalig intensiver dem Thema IT-Sicherheit zuwenden, ist es hilfreich, sich zunächst einen Überblick über den aktuellen Status quo der IT-Sicherheit in ihrem Haus zu verschaffen. Hierbei können IT-Sicherheitsanalysen auf Basis des B3S helfen. Im Rahmen derartiger IT-Sicherheitsanalysen wird die bestehende Informationssicherheit anhand von Dokumentenanalyse und Interviews erhoben. Ergänzt werden kann eine Analyse durch einen Penetrationstest. Dieser technische Scan der bestehenden IT-Landschaft zeigt offene Schwachstellen auf und ermöglicht es, direkt umsetzbare Maßnahmen zu generieren. Mithilfe derartiger IT-Sicherheitsanalysen lässt sich eine priorisierte Maßnahmenliste zur Gewährleistung der IT-Sicherheit erarbeiten, die erste Anknüpfungspunkte für den folgenden Aufbau eines ISMS liefert.

Fazit

Eine organisatorische Auseinandersetzung mit der IT-Sicherheit lässt sich in der heutigen Gesetzes- und Bedrohungslage, unabhängig von den bereits geschaffenen technischen Gegebenheiten, nicht länger vor sich herschieben. Trotz des wahrgenommenen damit verbundenen Aufwands überwiegt der Mehrwert klar erkennbar und eine Vernachlässigung des Themas ist von keiner Krankenhausgeschäftsführung mehr vertretbar.

Anschrift der Verfasser

Dr. Timo Braun, Patrick Winter, Sanovis GmbH, Riedenburger Str. 7, 81677 München, Tel.: 089/992757-90

Bücher

Budgetvereinbarung und Finanzierung von Psych-Einrichtungen

Stefan Günther, Ramon Krüger, Stefan Thewes (Hrsg.): Budgetvereinbarung und Finanzierung von Psych-Einrichtungen. medhochzwei GmbH, April 2022, 320 Seiten, kartoniert, ISBN: 978-3-86216-901-6, 89,00 €.

Das Buch „Budgetverhandlung und Finanzierung von Psych-Einrichtungen“ widmet sich ausschließlich der Finanzierung von psychiatrischen und psychosomatischen Kliniken. PEPP, PPP-RL, AEB-Psych und leistungsbezogener Vergleich sind neue Schlagwörter, die den Alltag der Einrichtungen bestimmen und die das Sammelwerk aufgreift. Zentraler Bestandteil des Werkes, ist die umfassende Darstellung der Erstellung einer Budgetforderung von der Leistungsplanung bis zur Ermittlung des Entgeltwertes. Schritt für Schritt wird die Erstellung einer Budgetforderung erklärt und mit zahlreichen Hintergrundinformationen ergänzt.

Nach der allgemeinen Einführung werden verschiedene Spezialfragen zu Schiedsstelle, Leistungsbezogener Vergleich, Erlösplanung, Modellvorhaben und Nachweisführung aufgegriffen, in denen der Leser die Themen weiter vertiefen kann. Darüber hinaus enthält das Buch Listen und Tabellen wie beispielsweise Checklisten zur Vorbereitung auf Budget- und Pflegesatzverhandlungen und dient somit als praxisorientierter und nützlicher Ratgeber für alle, die sich einen Überblick über das System der Finanzierung psychiatrischer und psychosomatischer verschaffen wollen. Die Praktiker aus Krankenhausmanagement und Controlling bekommen Hilfestellungen für die Vorbereitung von Budgetverhandlungen. Aber auch Leser, die bisher wenig Einblick in das Finanzierungssystem haben, gewinnen Verständnis für das System. Das Buch ist damit eine sehr hilfreiche Kombination aus Lehrbuch, Nachschlagewerk und Praktikerhandbuch.

Dr. Hanns-Diethard Voigt, Geschäftsführer Evangelisches Krankenhaus Bethanien gGmbH, 17489 Greifswald