Branchenspezifischer Sicherheitsstandard (B3S)

IT-Sicherheit umsetzen

Der Stellenwert der Informationstechnologie (IT) nimmt in allen Branchen und Lebensbereichen kontinuierlich zu. Auch in Krankenhäusern ist die IT elementar für die Unternehmensprozesse. Jedoch ist die IT-Ausstattung in den Häusern oft nicht auf dem aktuellsten Stand und die Bedeutung der IT wird häufig noch unterschätzt oder nicht erkannt.

Neben der Einbindung der IT in die täglichen Prozesse der Krankenhäuser, ist auch der Faktor der IT-Sicherheit in deutschen Krankenhäusern von Nachholbedarf gekennzeichnet.

Diese Defizite wurden durch den Gesetzgeber in Deutschland erkannt und mit dem IT-Sicherheitsgesetz im Jahr 2015 bedacht. Das IT-Sicherheitsgesetz definiert Verpflichtungen zur Verbesserung der IT-Sicherheit für kritische Einrichtungen (KRITIS) in Deutschland. Neben Einrichtungen der Energieversorgung, der Telekommunikation oder Ernährungsindustrie gehört der Gesundheitssektor zu KRITIS-Betreibern, die eine kritische Dienstleistung zur Versorgung der Bevölkerung erbringen. Zusätzlich zu Krankenhäusern als medizinische Versorger zählen Labore sowie arzneimittel- und impfstoffherstellende Bereiche zum Sektor Gesundheit. Krankenhäuser, die einen festgelegten Schwellenwert von 30.000 vollstationären Behandlungsfällen überschreiten, sind verpflichtet, die IT-Sicherheitsanforderungen zu erfüllen.

Mit Hilfe des B3S ist es für Kliniken möglich, ihre IT-Sicherheit zu erhöhen und damit den Anforderungen des IT-Sicherheitsgesetzes zu entsprechen.

Corona-Krise und ihre Folgen

Gerade in der Corona-Krise wurde die Bedeutung der kritischen Dienstleistungen an vielen Stellen im Gesundheitssektor stärker sichtbar. Neben der engen und an vielen Stellen unabdingbaren Verknüpfung der IT mit medizinischen Versorgungsprozessen wurde dies auch in Prozessen der Unterstützungsbereiche deutlich. So beschleunigte die Corona-Krise im Gesundheitswesen in vielen Bereichen die Digitalisierung. Es wurde u.a. vermehrt auf virtuelle Meetings und Homeoffice statt auf Besprechungen und Präsenzpflichten gesetzt. Vielerorts wurden hierfür schnelle Lösungen für Videokonferenzsysteme gesucht und oft auf cloudbasierte Lösungen, die wenig physische Komponenten in den Rechenzentren der Organisationen benötigen, zurückgegriffen. Dies bot Kriminellen eine Vielzahl an potenziellen Einfallstoren. Mancherorts fielen z.B. notwendige sicherheitstechnische Anpassungen von VPN-Zugängen und Rollen-/Rechtekonfigurationen etwa der Remote-Arbeitsplätze der Zeitknappheit bei der Umstellung zum Opfer. Durch die vermehrt angestoßenen Digitalisierungsprozesse wurden in Kliniken bereits bekannte, als auch neue Defizite in der IT-Ausstattung und IT-Sicherheit an vielen Stellen deutlich.

Die Corona-Krise zeigt sowohl, wie wichtig eine funktionierende und sichere IT-Landschaft im Krankenhaus ist und welche Chancen durch die Digitalisierung Gesundheitssektor entstehen, als auch, welche hohe Bedeutung die IT-Sicherheit, nicht nur für kritische Einrichtungen, hat.

Das IT-Sicherheitsgesetz

Die zu etablierenden Maßnahmen des IT-Sicherheitsgesetzes führen zu einer Verbesserung der IT-Sicherheit in den jeweiligen Einrichtungen. Diese Maßnahmen haben das Ziel, die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse sicherzustellen. KRITIS-Betreiber sind daher gesetzlich verpflichtet, ein Mindestmaß an IT-Sicherheit in Form angemessener organisatorischer und technischer Vorkehrungen nach dem Stand der Technik zu gewährleisten. Sie sind auch ver-

Bild: BRN-Pixel (stock.adobe.com)

pflichtet, ein Informationssicherheitsmanagement sowie eine zugehörige Informationssicherheitsorganisation einzuführen und zu betreiben.

Branchenspezifischer Sicherheitsstandard (B3S)

Da die Anforderungen und Gefahren für die IT-Sicherheit in den jeweiligen Sektoren unterschiedlich sind, existieren branchenspezifische Sicherheitsstandards (B3S). Sie helfen dabei, den jeweiligen „Stand der Technik" umzusetzen. Für Krankenhäuser in Deutschland steht der „Branchenspezifische Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus" zur Verfügung.

Mit Hilfe des B3S ist es Krankenhäusern möglich, ihre IT-Sicherheit zu erhöhen und damit den Anforderungen des IT-Sicherheitsgesetzes zu entsprechen. Die Methodik des B3S orientiert sich an etablierten Normen zur IT-Sicherheit (ISO 27001, ISO 27002, ISO 27799), am Risikomanagement (ISO 27005) und Best-Practice-Methoden wie ITIL und COBIT. Grundlage und Ziel des B3S ist die Einführung eines Informationssicherheitsmanagementsystems (ISMS) zur Planung, Umsetzung und Überwachung der technischen und organisatorischen Maßnahmen zur IT-Sicherheit. Hierfür liefert der B3S eine Umsetzungsempfehlung. Zur Einführung eines ISMS ist es zunächst erforderlich, die strategischen Ziele der IT-Sicherheit und den Geltungsbereich des ISMS zu definieren und die kritischen Dienstleistungen des Hauses einzuschließen. Maßgeblich zum Erfolg der ISMS-Einführung ist die Etablierung der erforderlichen Managementstrukturen. In diesem Rahmen müssen bereits Kriterien zur Bewertung und Klassifizierung von Informationen definiert und grundlegende Richtlinien erarbeitet werden.

Eine Hauptaufgabe im Rahmen des ISMS stellt die Risikoanalyse dar. Hierfür benennt der B3S erneut branchenspezifische Risiken, Bedrohungsszenarien und Gefährdungen zur Verfügung. Dies ist gerade im hochspezialisierten Krankenhausumfeld unabdingbar. Neben der Informationstechnik, Kommunikationstechnik und Versorgungstechnik werden Medizintechnik/-produkte gelistet, die für die kritischen Dienstleistungen betrachtet werden müssen. Nach erfolgreicher Risikoanalyse können darauf aufbauend die ersten technischen und organisatorischen Sicherheitsmaßnahmen umgesetzt werden. Neben diesen technischen und organisatorischen Maßnahmen zur Erhöhung der IT-Sicherheit ist die Schulung und Sensibilisierung der Krankenhausmitarbeiter eine nicht zu vernachlässigende Maßnahme. Oft führen gerade Unachtsamkeit oder fehlende Kenntnisse ungeschulter Mitarbeiter zu Verletzungen der IT-Sicherheit und Sicherheitsvorfällen in den kritischen Dienstleistungen. So helfen bereits einfache Awareness-Kampagnen z.B. das Risiko von Phishing-Attacken zu reduzieren. Gerade durch die aktuellen Wechsel auf Homeoffice-Lösungen und die allgemeine Verunsicherung durch die Corona-Krise konnte ein Anstieg an Phishing-Attacken registriert werden.

Nach erfolgreicher Einführung des ISMS steht das Monitoring und Überwachen der Maßnahmen im Fokus. Parallel ist die Planung von Audits voranzutreiben, um dem vom Gesetzgeber geforderten zweijährigen Nachweis gegenüber dem BSI zu entsprechen.

Nach Einführung des IT-Sicherheitsgesetztes kam es anfänglich zu Unsicherheiten, da eine Zertifizierung nach ISO 27011 für den Nachweis gegenüber dem BSI als erforderlich angesehen wurde. Hierbei konnte der B3S ebenfalls Klarheit schaffen. Zum Nachweis gemäß § 8a (3) IT-Sicherheitsgesetz beauftragt das Krankenhaus als KRITIS-Betreiber eine „prüfende Stelle", deren Prüfbericht das Krankenhaus an das BSI übermittelt.

Die Gewährleistung der IT-Sicherheit im Krankenhaus wird mit Hilfe des „Branchenspezifischen Sicherheitsstandards für die Gesundheitsversorgung im Krankenhaus" deutlich erleichtert. Dennoch ist der Projektumfang der Einführung eines Informationssicherheitsmanagementsystems (ISMS) sehr umfangreich und sollte so frühzeitig wie möglich angegangen werden. Vom BSI in Auftrag gegebene Studien zur IT-Sicherheit in Kritischen Infrastrukturen zeigen, dass, auch wenn die Kliniken ihre kritischen Dienstleistungen durch technische Schutzmaßnahmen schützen, gerade ihre organisatorischen IT-Sicherheitsmaßnahmen starke Lücken aufweisen. Diese Defizite können durch den strukturierten Aufbau eines ISMS vermieden werden.

Auch für Häuser, die unter dem Schwellenwert von 30.000 vollstationären Behandlungsfällen liegen und somit noch keinen gesetzlichen Verpflichtungen nachkommen müssen, ist der B3S relevant. Unabhängig von der eigenen Größe kann kein Haus ausschließen, nicht selbst Opfer eines IT-Sicherheitsvorfalls, sei er mutwillig oder versehentlich herbeigeführt, zu werden. Keine Einrichtung kann es sich daher erlauben, seine IT-Sicherheit zu vernachlässigen. Gerade wenn durch die Corona-Krise Defizite in der IT-Sicherheit sichtbar wurden, sollten diese nun bewusst in den Fokus gestellt und systematisch nach und nach behoben werden. Letzten Endes sollte jedoch die Devise „Agieren statt Reagieren" gelten, wobei der B3S eine sehr gute Unterstützung für Krankenhäuser in Deutschland darstellt.

Dr. Timo Braun

Master of Science, Projektleiter bei Curacon, **Kontakt: timo.braun@curacon.de**

Bild: Curacon