Martin Braun ist Gründer und Geschäftsführer der CyberSecurity manufaktur GmbH. Er verfügt über mehr als 20 Jahre Erfahrung in IT, IT-Sicherheit und IT-Risikomanagement, unter anderem als externer CISO / ISB in verschiedenen Kliniken und Krankenhäusern.
m.braun@cybersecurity-manufaktur.com,
cybersecurity-manufaktur.com

Wie Klinik-CIOs mit dem KHZG die IT-Sicherheit strategisch verbessern

von Martin Braun und Michael Watzl - Geschäftsführer der CyberSecurity manufaktur GmbH

Im September dieses Jahres ist das Krankenhauszukunftsgesetz[1] (kurz "KHZG") vom Deutschen Bundestag beschlossen worden. Es stellt ein Förderprogramm für Krankenhäuser in Höhe von 3 Mrd. Euro mit Fokus auf Digitalisierung und IT-Sicherheit dar. Doch wie nutzt man diesen Topf optimal, um die Cyber-Sicherheit nachhaltig zu verbessern?

Digitalisierung ist der Schlüssel zu Innovation, höherer Effizienz und zu besserem Service. Auf der anderen Seite vergrößert sich die Angriffsfläche für Cyber-Attacken. Dass dies für Krankenhäuser kein theoretisches Risiko ist, zeigen Fürth[2], Neuss[3] und zuletzt Düsseldorf[4]. Solche Cyber-Attacken können sich massiv auf essentielle Patientenversorgungsprozesse auswirken. Dadurch entsteht nicht nur finanzieller Schaden, sondern eine reale Gefahr für Patienten. Damit ist klar, dass der Umgang mit Cyber-Risiken nicht einfach an die IT-Abteilung delegiert werden darf.

Neue IT-Infrastruktur macht alles sicher?

Das KHZG will Krankenhäuser bei Digitalisierung und IT-Sicherheit gezielt unterstützen. So sind 15% des Fördervolumens allein für IT-Sicherheit einzuplanen. Den Aussagen einiger Cyber-Security-Experten zufolge, genügt ein ausreichendes Investment in die Modernisierung der IT-Infrastruktur und die entsprechende IT-Sicherheit wird sozusagen automatisch realisiert. Gerade das im KHZG-Kontext häufig diskutierte Reifegrad-Modell INFRAM[5] der HIMSS unterstützen diese These wie der Name "Infrastructure Adoption Model" bereits nahelegt. Prinzipiell bieten Reifegrad-Modelle durchaus den Vorteil, dass Fortschritte messbar werden. Das macht sich das KHZG zunutze und sieht eine zweimalige Messung vor (jeweils Ende Juni 2021 und 2023) anhand eines noch zu entwickelnden Reifegrad-Modells.

IT-Infrastruktur allein - sei sie auch noch so modern - schützt aber nicht ganzheitlich gegen Cyber-Angriffe. Es sind daneben noch Strukturen, Prozesse und Mitarbeiter einzubeziehen. Entscheidendes Manko bei reiner IT-Sicht ist aber das völlige Fehlen einer Schutzziel- und Risiko-Betrachtung: Welche Auswirkung hat die fehlende Verfügbarkeit eines Teilprozesses der Patientenversorgung, der unautorisierte Zugriff auf die Labor-Daten oder eine Manipulation digital vorliegender Akten? Damit sind drei wesentliche Schutzziele aus der Informationssicherheit aufgeführt: Verfügbarkeit, Vertraulichkeit und Integrität. Nur durch die Analyse der individuellen Schutzbedürfnisse der kritischen Prozesse werden Schwachstellen und Handlungsbedarfe sichtbar. Der oben dargestellte Infrastrukturansatz erschöpft sich im Gegensatz dazu mit Investitionen in Security-Technologie. Das Ergebnis ist ein Basis-Schutz, der den ohne Bezug auf die Prozesse und Risiken nur eingeschränkten Mehrwert bietet.

Wie sieht also der Ansatz zu verbesserter IT-Sicherheit im Schulterschluss mit dem KHZG und der eigenen Digitalisierungsstrategie aus? Und wie passt das mit den branchenspezifischen Sicherheitsstandards (B3S) für kritische Infrastrukturen (KRITIS) zusammen? Gerade dieser Punkt ist besonders relevant, da a) mit der Neuauflage des IT-Sicherheitsgesetzes mehr Häuser unter KRITIS fallen werden und b) das Patientendatenschutzgesetz (PDSG) explizit auf den B3S-Standard - unabhängig vom KRITIS-Status des Krankenhauses - Bezug nimmt.

Blindflug ohne Betrachtung der spezifischen IT-Risiken

Eine ausgewogene Cyber-Sicherheits-Strategie basiert auf Menschen, Prozessen und Technologie und ein praxisorientiertes Cyber-Risiko-Management verbindet diese drei Säulen. Den Einstieg in ein solches Managementsystem findet man typischerweise mit einer unabhängigen Cyber-Security-Reifegrad-Analyse, die branchenspezifische Anforderungen umfasst, z.B. Personengruppen (Ärzte, Pflegepersonal, Patienten, Verwaltungspersonal, etc.), medizinisch-technische Geräte oder auch besonders sensible Gesundheitsdaten.

Erfolgsfaktor branchenspezifische Praxiserfahrung

Vor allem Erfahrung und Praxisbezug sind bei der Bewertung von aktuellen technischen und organisatorischen Maßnahmen entscheidende Faktoren: Funktionieren die Notfall-Prozesse in realistischen IT-Ausfall-Szenarien? Sind die organisatorischen Strukturen intern und darüberhinaus (LKA, Katastrophenschutz, BSI) dokumentiert, etabliert, erprobt? Decken die eingesetzten Technologien die identifizierten Risiken tatsächlich auch ab? Die Beantwortung dieser Fragen ist definitiv nicht trivial, wie bspw. die "Stabsrahmenübung Cybersicherheitsvorfall" des Vivantes Klinikums in Berlin zeigt [6]: Diese Übung wurde ganze sechs Monate vorbereitet unter Einbeziehung der IT, unterschiedlicher Medizinbereiche, des LKA und sogar des Katastrophenschutzes. In der Realität eines Cyber-Notfalls steht deutlich weniger Vorbereitungszeit zur Verfügung!

Fazit

Eine fundierte Cyber-Security Reifegrad-Analyse bietet durch den Bezugspunkt "Krankenhausprozesse" sowohl eine valide Einschätzung der aktuellen Cyber-Risiko-Situation, als auch eine ideale Planungsgrundlage für Investitionen und Förderprojekte im Kontext des KHZG. Legt man hierbei einschägige Standards zugrunde, ist man bestens auf die Reifegrad-Prüfungen des KHZG vorbereitet. Eine Orientierung an ISO 27001 in Kombination mit dem branchenspezifischen B3S-Standard bietet eine optimale Ausgangsbasis - gerade in Hinblick auf KRITIS und PDSG.

Mithilfe dieser Standards lässt sich eine priorisierte Cyber-Strategie- und Investitionsplanung ableiten und optimal in förderfähige KHZG-Projekte einpassen. Ersteres ist sowieso auch ohne KHZG ein absolutes Muss für alle Krankenhäuser! Lücken bei einer Fokussierung auf IT-Infrastruktur bspw. auf Basis des Reifegradmodells INFRAM würden sich spätestens bei echten Cyber-Attacken - oder auch bei neuen Compliance-Anforderungen aus KritisV und PDSG - zeigen. Durch einen risikobasierten Reifegrad-Ansatz lässt sich dies vermeiden.

Quellen

[1] hwww.bundesgesundheitsministerium.de/krankenhauszukunftsgesetz.html

[2] www.nordbayern.de/region/fuerth/experte-erklart-das-steckt-hinter-cyber-attacke-auf-klinikum-1.9670400

[3] www.sueddeutsche.de/digital/hacker-angriff-computervirus-legt-klinik-in-neuss-lahm-1.2861656

[4] www.handelsblatt.com/technik/sicherheit-im-netz/cyberkriminalitaet-todesfall-nach-hackerangriff-auf-uni-klinik-duesseldorf/26198688.html

[5] www.himssanalytics.org/infram

[6] www.krankenhaus-it.de/modules/publisher/index.php/item.360

Michael Watzl ist Geschäftsführer der CyberSecurity manufaktur mit ebenso langjähriger Cyber-Security-Erfahrung, bspw. zu Security-Awareness, IT-Security-Technologien und strategischer Cyber-Security-Planung.
m.watzl@cybersecurity-manufaktur.com , cybersecurity-manufaktur.com