IT-SICHERHEIT
Magazin für Management und Technik

Krankenhaus-IT JOURNAL
Fakten und Perspektiven der IT im Gesundheitswesen

SPECIAL

IT-Sicherheit im Krankenhaus

Das Wichtigste zuerst

Christian Schreiner von SWS erklärt, was Krankenhäuser für mehr Cybersicherheit tun können

DATAKONTEXT

Kurzinterview mit
Christian Schreiner, SWS

Top-down: Das Wichtigste zuerst

KHZG, RIS, PACS, KIS und Telematik-Infrastruktur sind für die SWS AG keine Fremdworte. Das Unternehmen hat einen jahrzehntelangen Erfahrungsschatz aus zahlreichen Klinikprojekten aufgebaut. An oberster Stelle steht immer ein ganzheitlicher Security-Ansatz zum Schutz der hochsensiblen Patientendaten. Im Interview mit IT-SICHERHEIT verrät Christian Schreiner, Verstandsvorsitzender der SWS, was Krankenhäuser für mehr Cybersicherheit tun können.

ITS: Warum ist die ständige Verfügbarkeit der IT besonders in einem Krankenhaus so essenziell?

Christian Schreiner: Selbstverständlich ist in jeder Art von Unternehmen die Verfügbarkeit der IT unabdingbar. Bei einem Ausfall der IT entstehen beispielsweise in einem Produktionsbetrieb jedoch meist „nur" materielle Schäden, was durchaus tragisch ist und sogar zur Insolvenz des Unternehmens führen kann. In einem Krankenhaus steht bei einem solchen Ausfall jedoch viel mehr auf dem Spiel. So kann zum Beispiel nicht mehr auf Patientenakten zugegriffen werden und unter Umständen müssen lebenswichtige Operationen verschoben werden. So berichteten die Medien von einem Vorfall aus dem Jahr 2020, bei dem die Uniklinik Düsseldorf durch einen zufälligen Hackerangriff vier Wochen lang lahmgelegt war. Abmeldung von der Notfallversorgung, Rettungswagen fuhren sie tagelang nicht an und sogar der Tod einer Frau durch zu späte Behandlung waren die Folge.

ITS: Es sind zahlreiche Maßnahmen notwendig, um die IT-Sicherheit zu gewährleisten. Eine Umsetzung solcher Maßnahmen in einem kurzen Zeitraum ist schon aus personeller Hinsicht oft nicht möglich. Wie würden Sie hier vorgehen?

Christian Schreiner: Es sind sicherlich schon einige Sicherheitsmaßnahmen umgesetzt. Zunächst einmal ist aufzulisten, welche Sicherheitsmaßnahmen heute bereits existieren, um zu prüfen, inwieweit diese noch den aktuellen Anforderungen entsprechen. Sind sie nicht mehr auf dem aktuellen technischen Stand, muss das unbedingt nachgeholt werden. Das ist normalerweise mit überschaubarem Aufwand möglich.

ITS: Ist das erledigt, wie würden Sie dann die nächsten Punkte angehen?

Christian Schreiner: Danach ist zu prüfen welche Maßnahmen fehlen, um einen sicheren IT-Betrieb zu gewährleisten. Ich empfehle hier eine Top-Down-Vorgehensweise: Die Maßnahmen mit dem größten Sicherheitseffekt würde ich hier zuerst umsetzen.

ITS: Können Sie hier Beispiele nennen?

Christian Schreiner: Es hilft nichts, wenn die Endgeräte einen Virenscanner haben, die Server jedoch ungeschützt im Netzwerk stehen. Ich würde hier versuchen meine „Kronjuwelen", nämlich die Server und SAN-Systeme als erstes zu schützen. Das funktioniert am besten mit einer Microsegmentierung des zentralen Datacenter-Netzwerkes. Als nächstes gilt es, die Systeme zu überwachen und automatisiert Anomalien zu erkennen. Gerade in Zeiten von Fachkräftemangel ist es in einem komplexen Krankenhaus-IT-System schier unmöglich ständig alle Systeme manuell zu überwachen. Deshalb ist hier ein Security-Information-and-Event-Management-(SIEM)-System empfehlenswert. Es prüft permanent Istzustände gegen Sollzustände aller relevanten Systeme, erkennt Anomalien und warnt die IT-Administratoren proaktiv. Das sind jedoch nur zwei Beispiele von vielen.

ITS: Wie ist die Vorgehensweise, wenn ein Krankhaus trotz aller Schutzmaßnahmen Opfer eines Hacker-Angriffs wird?

Christian Schreiner: Eine 100-prozentige Absicherung der IT ist leider nie möglich. Unser Ziel ist es jedoch, mit den Maßnahmen die Angriffsfläche zu minimieren und den Schaden so gering wie möglich zu halten. In so einem Fall analysiert unser Security-Operation-Center-(SOC)-Team zusammen mit der Klinik den Vorfall und leitet Maßnahmen zur Datenwiederherstellung und Verhinderung der weiteren Ausbreitung der Ransomware ein. Zudem werden forensisch der Einfallspunkt sowie die kompromittierten Systeme ermittelt, um weitere Angriffe und eine Ausbreitung zu verhindern. Wir stehen dabei selbstverständlich bis zur vollständigen Rehabilitation an der Seite der Klinik. ■

Prävention und Transparenz

Mit wenigen Maßnahmen Angriffsflächen verringern

Viele Entscheider im Gesundheitswesen stehen heute vor der Frage, wie man in einer modernen Krankenhaus-Umgebung den digitalen Blackout vermeidet und mit vorhandenen Ressourcen den Spagat zwischen Sicherheit, Verfügbarkeit und Nutzerfreundlichkeit schafft. Unser Beitrag gibt Antworten.

Christian Schreiner ist Vorstandsvorsitzender der SWS Computersysteme AG und berät in Sachen Cybersicherheit viele Krankenhäusern. „Natürlich war man in den vergangenen Jahren auch mit Cyberangriffen einzelner Häuser konfrontiert", so Schreiner „mitentscheidend, dass versuchte Ransomware-Attacken bei verschiedenen Krankenhäusern ohne größere Schäden oder gar erfolglos blieben, war dabei das frühzeitige Verringern der Angriffsflächen durch Maßnahmen wie Segmentierung beziehungsweise Mikrosegmentierung der Krankenhausnetze, professionelle Sicherheitswerkzeuge, Werkzeuge zur Anomalie-Erkennung wie auch gute Backupkonzepte."

Generell sollten die Verantwortlichen in den Krankenhäusern in ihrem Netzwerk Transparenz schaffen, zum Beispiel durch eine dedizierte Analyse des Kommunikationsverhaltens von IT-Komponenten. Dazu gibt es sehr gute Werkzeuge mit hohen Automatismen. Ziel ist es, nicht gewünschte oder erforderliche Verbindungen einzuschränken beziehungsweise zu verhindern. Ein Dopplersonografiegerät muss in der Regel keine Verbindung zum MRT oder Autoklaven haben oder ein Drucker keine Verbindung zu einer Videokamera. „Bei unseren zahlreichen IT-Projekten in Kliniken im Krankenhaus-Pflegeumfeld sehen wir bei einem Haus mit 1000 Betten momentan im Durchschnitt circa 4000 vernetzte medizinische Geräte im Einsatz", so Schreiner. „Speziell die Internet-of-Medical-Things-(IoMT)-Geräte werden zunehmend als Brückenköpfe für Cyberangriffe auf die digitale Infrastruktur genutzt."

Problem Fachkräftemangel

Auch der IT-Fachkräftemangel trifft die Verantwortlichen und stellt eine weitere Schwachstelle in Bezug auf die IT-Sicherheit dar. Daher greifen viele Kliniken zunehmend auf die Unterstützung von professionellen IT-Dienstleistern zurück. „Wichtig ist, dass der Dienstleister die grundsätzlichen Abläufe in der Klinik kennt und Erfahrungen aus anderen Projekten zur Verfügung stellt. Nur dann er kann einen echten Mehrwert liefern", meint Schreiner von der SWS AG.

Mithilfe des Dienstleisters kann die Organisation dann geeignete Schutzmaßnahmen umsetzen, wobei man dabei nicht vergessen darf, dass Aspekte wie Verfügbarkeit und Patientennutzen eine ebenso wichtige Rolle wie die Sicherheit spielen. Fragen, die immer wieder auftauchen, sind zum Beispiel:

- Wie integriert man IT-basierte Kameras sicher?
- Wie installiert man ein sicheres und flächendeckendes Patienten-WLAN?
- Wie setzt man sicheres digitales Patientenmonitoring um?
- Wie schützt man die Anbindung und Integration von Belegärzten und Zuweisern?
- Wie können Daten nach außen geschickt werden, zum Beispiel von Radiologien?
- Wie findet die Integration von Haus- und Patiententechnik statt?
- Ist ein Eigenbetrieb denkbar oder sollte man Managed-Service-Partner nutzen?

Weitere Maßnahmen sind zum Beispiel eine abgestimmte Sicherheitsrichtlinie, der Aufbau eines Informationssicherheitsmanagementsystems (ISMS), die Implementierung von Sicherheitsprozessen (Notfallplanung, Umgang mit Sicherheitsvorfällen etc.) sowie die Durchführung von Awareness-Trainings.

Besonders elementar in einer Sicherheitsstrategie sind regelmäßige Schulungen durch Awareness-Trainings. Das bedeutet die wiederkehrende Sensibilisierung der Mitarbeiter, Lieferanten und Dienstleister (Stakeholder) hinsichtlich von Fehlverhalten sowie der Gefährdung durch und im Umgang mit Cyber-Attacken.

Zudem gibt es technische Mittel, die alle organisatorischen Aspekte integrieren beziehungsweise berücksichtigen und für ein bestmögliches Sicherheitsniveau sorgen können. Alle genannten Maßnahmen bedürfen der Rückendeckung der Geschäftsführung.

Netzwerksegmentierung

Viele Kliniken haben ihre Segmentierungsvorhaben bereits begonnen oder befinden sich im laufenden Prozess. Bevor allerdings eine geplante Segmentierungsstrategie umgesetzt werden kann, stehen Punkte wie Verfügbarkeit, Sicherheit und ein strukturiertes Vorgehen, idealerweise mit einer entsprechenden Risikoanalyse untermauert, auf der Tagesordnung.

Ein grobes Zonenkonzept basiert auf der Trennung der Krankenhausinfrastruktur in einzelne Netze. Die Kernstücke der Segmentierung haben weitere Unterteilungen in Sub-Netze und Zonen bis hin zu einer Mikrosegmentierung.

Innerhalb der Netze (Zonen) werden entsprechende Kommunikationsverbindungen ermittelt, hinterfragt und in einer Kommunikationsmatrix festgehalten und bewertet. Voraussetzung für Transparenz und Visibilität ist, dass die beteiligten Komponenten bekannt und entsprechend inventarisiert sind. Außerdem müssen die Systemstände erfasst sein.

„Die Entwicklung von flachen Netzen in ein Netzwerk mit segmentierten Enklaven ist als Prozess zu verstehen, der im strukturierten Ablauf und mit der notwendigen Unterstützung erfolgreich umgesetzt werden kann", lautet das Fazit von Schreiner.

IT-Sicherheitsgesetz 2.0 und NIS 2

Aber auch der Gesetzgeber stellt Krankenhäuser vor neue Herausforderungen: Gerade Betreiber kritischer Infrastrukturen sind in den folgenden Monaten mit der Umsetzung des IT-Sicherheitsgesetzes und der NIS-2-Richtlinie gefordert. Hierzu gehören unter anderem:

- Risiko- und Notfallmanagementkonzept
- Verfahren zur Meldung von Vorfällen
- Betrachtung von Cyber-Sicherheitsrisiken in Lieferketten
- Audits und Methoden zur Verbesserung der Informationssicherheit

Analog der Datenschutzgrundverordnung (DSGVO) gilt auch bei NIS 2, dass bei signifikanten Sicherheitsvorfälle binnen 24 Stunden eine Frühwarnung und innerhalb von 72 Stunden eine Einschätzung an die Behörde erfolgen muss. Bei Nichterfüllung drohen teils drastische Sanktionen.

Allerdings kann nur melden, wer über eine konforme Angriffs- und Anomalie-Erkennung verfügt. Auch bei der Umsetzung dieser Systeme setzen viele Unternehmen auf Wissen von außerhalb und binden unter dem Stichwort Managed-Detection and -Response (MDR) externe Security-Spezialisten mit in die Cyberabwehr ein.

Grundlegende Maßnahmen

Die vorangestellten Punkte nützen aber wenig, wenn grundlegende Bedingungen nicht erfüllt werden und in der IT die Mindestanforderungen nicht umgesetzt sind. Folgend eine nicht abschließende Übersicht:

- **E-Mail-Sicherheit und Endpoint-Protection:** Neben einem segmentierten Netz (einschließlich Firewall-Konzept) zählen weitere wichtige Instrumente zum Portfolio einer Sicherheitsstrategie. Die Überwachung von zentralen Diensten beispielsweise. So sind E-Mails nach wie vor eines der häufigsten Einfallstore und stehen wie ein entsprechender Endpunktschutz im besonderen Fokus der Angriffserkennung.

- **Zugriffssteuerung:** Multi-Faktor-Authentifizierung für alle Mitarbeiter, sichere Passwörter und getrennte sowie persönlich zugeordnete Accounts sind unumgänglich. Ferner auch die Sicherstellung, dass jeder nur auf die Daten zugreifen darf, die er auch wirklich für seine Arbeit benötigt – ein Hausmeister muss keine Röntgenbilder sehen, nur Ärzte haben Zugriff auf Klinik-Applikationen. Die Nutzung von Cloud-Applikationen sollte im Blickpunkt der aktuellen Sicherheitsbetrachtungen stehen.

- **Backup:** Zur Wiederherstellung der Betriebsfähigkeit im Falle einer Kompromittierung, bei Fehlkonfigurationen sowie bei Hard- und Softwaredefekten ist ein funktionierendes Backup-Konzept obligatorisch. Die Lauffähigkeit der auf unterschiedlichen Medien gespeicherten Datensicherungen sind in regelmäßigen Abständen zu überprüfen und stellen eine einfache Maßnahme für Krankenhäuser dar, um bei einer Ransomware-Attacke den Betrieb aufrecht zu erhalten. ■

Hans-Martin Kuhn
ist T.I.S.P.-zertifizierter Security-Experte und Consultant bei der SWS Computer AG.