TAGESSPIEGEL
BACKGROUND

Cybersecurity

„Viele Krankenhäuser unterschätzen die Bedrohungslage“

Jan Arfwedson, Geschäftsführer des Healthcare IT-Security-Spezialisten Aurasec im Nachgefragt. (Bild: Aurasec)

Heute treffen sich in Berlin IT-Sicherheitsexpert:innen aus der Gesundheitsbranche auf der Sitzung des E-Health-Hubs des Cyber-Sicherheitsrats Deutschland e.V. Jan Arfwedson, Geschäftsführer des Healthcare IT-Security-Spezialisten Aurasec und Leiter des Hubs, erklärt, welche Themen heute auf der Agenda stehen.

von **Redaktion** veröffentlicht am 07.04.2022

Die Warnungen vor einem Cyberkrieg haben viele Unternehmen verunsichert. Wie beurteilen Sie das Stimmungsbild unter Krankenhausbetreibenden?

Offen gesagt hat sich die Lage nur geringfügig verändert, weil viele Krankenhäuser ihre eigene Resilienz gegen Cyberattacken noch viel zu wenig – man könnte auch sagen viel zu wenig realistisch – einschätzen. Klar, das Bundesamt für Sicherheit in der Informationstechnik (BSI) versucht derzeit verstärkt mögliche Angriffsvektoren zu reduzieren und empfiehlt nicht zwingend notwendige

Vernetzung zeitweise zu deaktivieren oder zurückzufahren. Aber gerade Häuser, die nicht unter die KRITIS-Bestimmungen fallen, sind bei dem Thema häufig noch sehr rudimentär unterwegs. Dort ist man bestrebt die täglichen Herausforderungen zu meistern und den IT-Betrieb sicherzustellen und nicht die Frage danach, ob es aktuelle Warnungen des BSI gibt oder neue Schwachstellen entdeckt wurden – ganz zu schweigen von einem Bewusstsein für Spill-over-Effekte.

Woran liegt das?

Das Thema der Cybersecurity Awareness ist natürlich auch hier eine Herausforderung – generell beobachten wir, dass Verantwortliche häufig gar nicht einschätzen können, wie hoch die eigene IT-Kompetenz ist und dadurch den Security-Reifegrad ihrer Organisation überschätzen. Und es scheitert dann natürlich daran, dass IT- und Informationssicherheit bei den Führungskräften und Entscheider in den Krankenhäusern oft noch keine strategische Relevanz hat und man dadurch noch nicht verstanden hat, dass auch abseits von reinen Compliance-Anforderungen, wie beispielsweise dem *§ 75c SGB V (https://www.krankenhauszukunftsfonds.de/Redaktion/Glossareintraege/DE/S/sgb-v-paragraph-75c-kapitel-3-1.html)* etwas passieren muss und generell eine ernstzunehmende Bedrohungslage vorherrscht.

Wo erkennen Sie weitere Herausforderungen – abseits einer teilweise mangelhaften Lageeinschätzung?

Eine zentrale Herausforderung sind nicht ausreichende finanzielle Mittel und dann natürlich mangelndes Personal. Denn selbst wenn Krankenhäuser erkennen, dass sie etwas tun müssen, finden sie nicht die Fachkräfte, die das auch umsetzen können. Häufig gibt es nur eine Hand voll IT-Mitarbeiter und da macht jeder quasi alles, da gibt es keine IT-Security-Fachabteilung oder Stabstelle, wie beispielsweise in einem Universitätsklinikum. Derzeit kommen zum Tagesgeschäft dann noch zig Digitalisierungsprojekte aus dem *Krankenhauszukunftsgesetz (https://background.tagesspiegel.de/cybersecurity/was-das-khzg-den-kliniken-bringt)*(KHZG) dazu, die die IT zusätzlich stemmen muss.

Und dann kostet Sicherheit eben auch Geld. Mit dem KHZG fördern der Bund und die Länder Digitalisierungsmaßnahmen im Umfang von 4,3 Milliarden Euro. Dabei müssen fünfzehn Prozent auf IT-Sicherheitsmaßnahmen entfallen, denn der Staat hat erkannt: Keine digitale Transformation ohne entsprechende IT-Sicherheit. Aber die Rechnung geht nicht auf:

Die Deutsche Krankenhausgesellschaft hatte im Rahmen einer Studie ermitteln lassen, dass durch die Umsetzung des Branchenspezifischen

Sicherheitsstandards – wie es aktuell §75 c SGBV fordert – initiale Mehrkosten in Höhe von 1,5 bis zwei Millionen Euro sowie jährliche Folgekosten von 500 bis 600.000 Euro verursacht. Nimmt man das KHZG-Fördervolumen von 4,3 Milliarden Euro, teilt es durch die Anzahl der Krankenhäuser und multipliziert diesen Wert mit den fünfzehn Prozent, so kommt man auf rund 336.000 Euro welche jedem Krankenhaus im Schnitt im Kontext IT-Sicherheit zufließen.

Demnach deckt das KHZG bei weitem nicht den Finanzierungsbedarf der Krankenhäuser in Bezug auf Maßnahmen zur Erhöhung der IT-Sicherheit – unabhängig ob Krankenhäuser diesen Bedarf erkennen. Es fehlt zudem an der langfristigen Finanzierung der Betriebskosten inklusive Personal über 2024 hinaus.

Welche Themen stehen heute auf der Agenda?

Wir werden einen Überblick auf die aktuelle Bedrohungslage geben, um die Krankenhäuser abzuholen – Titelthema der Sitzung ist „Cyberangriffe auf Kritische Infrastrukturen: Herausforderungen für Informationssicherheitsbeauftragte (ISB) im Gesundheitswesen“. Als zentrales Thema wollen wir uns bei dieser Sitzung mit der Rolle des ISB in Krankenhäusern auseinandersetzen, denn häufig ist den Verantwortlichen nicht klar, welche Aufgaben und Befugnisse ein ISB hat und ob man beispielsweise einen ISB in Vollzeit benötigt. Wir werden hierzu eine Handreichung für Krankenhausleitungen und ISBs vorstellen, die wir mit Krankenhausvertretern und weiteren Experten erstellt haben. Diese enthält zudem Checklisten für die praktische Arbeit eines ISB in einem Krankenhaus; zudem wird es ein Kalkulationstool geben, mit welchem Verantwortliche abhängig von der Größe des Krankenhauses und der Anzahl der Standorte ermitteln können, welchen Bedarf sie an Unterstützungsleistungen durch einen ISB haben.

Die Fragen stellte Johannes Steger