Cybersicherheit im Herzen

Interview mit Dipl.-Inf. Andreas Lockau, Niels-Stensen-Kliniken und Bundesverband KH-IT

Andreas Lockau ist ein Mann vom Fach. Der studierte Diplominformatiker hat acht Jahre lang in IT-Unternehmen gearbeitet, bevor er 2001 ins St. Marien-Hospital Hamm gGmbH gewechselt ist und dort nach der Fusion mit der Kath. St. Johannes Gesellschaft Dortmund gGbmH die leitende Position in der IT ausgefüllt hat. Seit Anfang 2022 ist er Abteilungsleiter IT und Medizintechnik der Niels-Stensen-Kliniken in Osnabrück.
Am 23. September 2023 wurde er zum Vorsitzenden des Vorstandes des KH-IT, des Bundesverbands der Krankenhaus-IT-Leiterinnen und -Leiter, gewählt.

Herr Lockau, welche Themen wollen Sie im KH-IT besonders forcieren?
Andreas Lockau: Die ändern sich tatsächlich mit den Anforderungen. Aktuell treibt mich um, dass wir rein technisch sehr viele Möglichkeiten hätten, diese aber nicht ausreichend nutzen. Mit dem Krankenhauszukunftsgesetz können wir das ändern und Digitalisierung wie Vernetzung vorantreiben. Den Verband sehe ich als wichtige Plattform zum Austausch und zum Know-how-Transfer, ganz nach unserem Motto „Aus der Praxis für die Praxis“. Ich bin der Überzeugung, dass der Einzelne die Herausforderungen in der IT alleine nicht mehr bewältigen kann. Er braucht den Austausch und Best Practices. Dafür ist der KH-IT mit seinen knapp 600 Mitgliedern die perfekte Plattform. In diesem Rahmen kommen immer wieder Experten zu allen Fragen zu Wort, von der digitalisierten Anwendungsumgebung, den Projekten, der Infrastruktur bis zur IT-Sicherheit – besonders wichtig in Zeiten zunehmender Vernetzung.

Apropos Informationssicherheit: Ist es tatsächlich so, dass aktuell mehr Cyberangriffe auf Gesundheitseinrichtungen stattfinden?
A. Lockau: Ich denke, dass es grundsätzlich mehr Hackerangriffe gibt, und sich das auch entsprechend im Gesundheitswesen bemerkbar macht. Ich glaube zudem, dass nicht nur gezielt Gesundheitseinrichtungen angegriffen werden. Aufgrund der zunehmenden Offenheit durch Kommunikationskanäle wie Patienten- und Remote-Portale, sowie Wege der New Work für Mitarbeiter ergeben sich potenzielle Angriffsziele. Hacker stellen im Rahmen ihrer allgemeinen Bot-Aktivitäten fest, dass ein Haus unzureichend geschützt ist. Die Kriminellen scannen branchenübergreifend mittels Bots ständig IP-Ports, lassen ihre Programme ständig dagegen laufen. Das passiert in großem Stil automatisch, da sitzt ja niemand und tippt irgendetwas ein. Es gibt Datenbanken mit unzähligen Schlüsselwörtern, die gegen derartige Plattformen eingesetzt werden. Hat ein Hacker eine Lücke im Sicherheitsnetz entdeckt, verkauft er die Information an Dritte, die dann den Angriff starten. Da geht es dann in aller Regel um die Erpressung von Lösegeld für gesperrte Daten.

Was sind denn klassische Einfallstore für Hacker?
A. Lockau: Das sind die bereits beschriebenen Portale, aber auch VPN-Zugänge, Firewalls und Webseiten, die selbst gehostet werden. Gefahren bestehen überall dort, wo sich eigene Mitarbeiter oder Firmen, die Remoteservices anbieten, von außen einloggen können. Diese Plattformen und Zugänge gilt es, mit aktuellen Patches und den gegebenen Sicherheitsfeatures abzusichern. Der Schutz muss nicht immer dem Goldstandard entsprechen – auch wenn das maximal wünschenswert wäre –, er muss aber zwingend aktuell gehalten werden. Das ist das Minimum, was jede Einrichtung tun muss. Um das verlässlich gewährleisten zu können, braucht es auch

Hundertprozentige IT-Sicherheit gibt es nicht, es geht um Risikominimierung.

Dipl.-Inf. Andreas Lockau
Niels-Stensen-Kliniken und KH-IT

womöglich externes Know-how.
Da eine Klinik ein offenes Haus ist, besteht zudem die Gefahr, dass sich Unbefugte in den Räumen aufhalten, die dann einen Angriff von innen starten können. Dazu reichen häufig nicht gesperrte PCs aus, um mit einem USB-Stick Schadsoftware zu installieren oder mit einem simplen Webseitenaufruf einen Kontakt herzustellen. Hier sprechen wir dann über eine Mischung aus Informationssicherheit und Datenschutz. Darum sagen wir: Lasst keine Büros offen, loggt euch aus Anwendungen aus und sperrt die mobilen Endgeräte wie Visitenwagen oder Tablets.

Was sind weitere gängige Schutzmechanismen?

A. Lockau: Firewalls und Virenscanner gehören selbstverständlich zur Grundausstattung. Hilfreich sind auch eine spezielle Software, die Anomalien im Netzwerk erkennt, und sogenannte Log-Sammler, die alle Logs aus verschiedenen Systemen sammeln und analysieren. Dazu kommt dann noch ein Security-Operation-Center, das sieben Tage die Woche rund um die Uhr die Logs und Anomalien monitort und im Fall der Fälle Alarm schlägt. Zuerst einmal schützt man sich so gut wie möglich gegen Angriffe. Sind die aber passiert und geblockt, muss man sich die potenzielle Gefahrenstelle anschauen und handeln.
Ein weiteres wichtiges Instrument der Informationssicherheit ist eine Netzwerksegmentierung, gerne auch Microsegmentierung. Damit kann ich im Angriffsfall den Schaden so gering wie möglich halten. Natürlich müssen alle Strukturen mit jedem neuen Informationssystem, jedem der vielfältigen Programme, mit jedem neuen Medizingerät erneut überprüft werden.
Wichtig ist aber auch, sich stetig zu vergegenwärtigen, dass es keine hundertprozentige Sicherheit gibt. Jeder kann von einem Cyberangriff betroffen werden. Das schärft die Sinne. Hat ein Angriff stattgefunden, geht es darum, wie damit umgegangen wird. Das legt ein Haus im Informationssicherheitsmanagement und im Business-Continuity-Management mit Notfallhandbuch, Wiederanlaufplänen, klaren Prozessen und klassifizierten Services fest.

Wie schätzen Sie aktuell den Sicherheitsstandard der Krankenhäuser ein?

A. Lockau: Das kann man pauschal nicht sagen. Es gibt die bekannten Schutzmechanismen, die allen zur Verfügung stehen. Der eine nutzt sie stärker, der andere weniger stark. Es ist ja so, dass nicht alle Einrichtungen die gleichen finanziellen Mittel, das gleiche Know-how und die gleichen personellen Ressourcen haben. Deshalb halte ich es für einen guten Ansatz, dass das KHZG verbindlich vorschreibt, 15 Prozent der beantragten Geldmittel für Maßnahmen zur Optimierung der Informationssicherheit zu investieren. Das wird das allgemeine Sicherheitsniveau bereits deutlich heben. Allerdings mache ich mir Sorgen um die Nachhaltigkeit. Die Kosten – wir sprechen hier schnell von einer hohen sechsstelligen Summe pro Jahr – laufen ja auch nach dem Auslaufen der Förderung in drei Jahren weiter.

Wie können Kliniken die notwendigen Kosten denn dann schultern?

A. Lockau: Nicht aus Eigenmitteln, wir benötigen eine Anschlussfinanzierung. Ich halte es für sinnvoll, die Themen Digitalisierung und Informationssicherheit zu trennen. Digitalisierung ist notwendig, weil sie eine Vernetzung von Daten und Strukturen schafft, die zu einer effektiven, besseren Patientenversorgung führt. Aber das ist ohne die Informationssicherheit wenig wert. Das sollten die Verantwortlichen bei der Krankenhausfinanzierung bedenken, etwa mit einem separaten Abschlag. Bereits bei der Einführung von KRITIS hieß es, dass es kostenneutral für die Beteiligten sei. Das ist es natürlich mitnichten, weil allein der Informationssicherheitsbeauftragte Geld kostet – genau wie die geforderten Werkzeuge. Informationssicherheit bekomme ich nicht umsonst, aber sie muss ein funktionierendes Basiswerkzeug für alle Gesundheitseinrichtungen sein. Wenn wir an die Kosten denken, sollten wir aber nicht nach immer neuen Sicherheitstools verlangen, sondern auch an Mechanismen wie Security by Design denken.

Das wäre dann der Punkt, an dem IT-Anbieter die Krankenhäuser unterstützen und ihnen ein wenig den Druck abnehmen könnten?

A. Lockau: Ganz genau. Der angesprochene Punkt ist aber nur ein Aspekt; mir geht es um etwas Generelles. Bei den stetig steigenden Anforderungen können wir uns im Krankenhaus unmöglich um alle Themen selbst kümmern. Wir brauchen Unterstützung, wir brauchen externen Sachverstand, Unternehmen, die auf ein Thema spezialisiert sind. Das kostet aber Geld. Wir können es, wie bereits erwähnt, nicht mit den Mitteln finanzieren, die wir aus der Patientenbehandlung erlösen. Ich würde mir nun einen breiten Konsens wünschen, dass Informationssicherheit gewollt und als systemrelevant anerkannt ist. Und ich würde mir einen Informationssicherheitszuschlag als

Basisfinanzierung wünschen, der uns einen dauerhaft sicheren Betrieb der IT-Infrastruktur ermöglicht.

Ein interessanter Ansatz. Wie steht es eigentlich um das Spannungsfeld zwischen IT-Sicherheit und effektiver Patientenbehandlung?

A. Lockau: Klar ist, dass die Patientenbehandlung nicht unter den Vorgaben der Informationssicherheit leiden darf. In der Praxis ist es aber schon so, dass der eine oder andere Prozess vielleicht durch Passworteingaben oder Sicherheitsabfragen komplexer wird. Unsere Aufgabe ist es, das auf ein Minimum zu reduzieren und den Anwendern intelligente Lösungen an die Hand zu geben. Etwa ein Single-Sign-on oder automatische Datenaufbereitungen für ihre tägliche Arbeit.
Und wir müssen immer wieder sauber und nachvollziehbar erklären, warum die Schutzmaßnahmen wichtig und sinnvoll sind.

Sicherheit kostet Geld, haben Sie gesagt, Herr Lockau. Aber Tipps gibt es ja umsonst. Welche Verbände und Institutionen gibt es denn neben dem KH-IT, die Kliniken beim Thema IT-Security beraten können?

A. Lockau: Da ist zuvorderst das BSI zu nennen, das Bundesamt für Sicherheit in der Informationstechnik, das die Situation in Deutschland beobachtet. Auch die Landeskriminalämter haben mittlerweile sehr gutes Know-how aufgebaut, weil sie immer dann eingeschaltet werden, wenn es einen Angriff gegeben hat. Die Forensiker dort können bei der Analyse und Wiederherstellung der Systeme wertvolle Hilfe leisten. In einigen Bundesländern gibt es auch ein Landesamt für Sicherheit in der Informationstechnik.
Was die Verordnungen angeht, lohnt ein Blick in die EU NIS-2-Richtlinie und Technical Reports der einschlägigen Normen. Die geben auch Hilfestellung und konkrete Umsetzungsanweisungen, beispielsweise die DIN EN IEC 80001-1 zum Risikomanagement für medizinische IT-Netzwerke.

Wirkt sich der Fachkräftemangel eigentlich auf die IT-Sicherheit aus?

A. Lockau: Der Fachkräftemangel wird sich sicher auch in der Informationssicherheit niederschlagen, weil wir wahrscheinlich in allen Bereichen Personal verlieren werden. Da ist die Informationssicherheit genauso betroffen wie die Anwendungsbetreuung und der Helpdesk. Das wird uns insgesamt nicht guttun, weil alle diese Tätigkeiten auf die IT-Sicherheit einzahlen. Die Systeme müssen sauber konfiguriert, kontinuierlich gemonitort und regelmäßig gepatcht werden. Da greift ein Rad ins andere.

Welche Lösungen sehen Sie aus dem Dilemma?

A. Lockau: Die einfachste ist es, definierte Aufgaben outzusourcen, an spezialisierte Firmen oder an eigene IT-Partner, etwa über Managed Services. Da können Kliniken einzelne Teile der Infrastruktur und der damit verbundenen Aufgaben in fachkundige Hände übergeben. Gerade für die Informationssicherheit gibt es Experten, die uns sehr unterstützen können. Neben den Betreibermodellen sollten die IT-Anbieter uns natürlich weitere einfache Möglichkeiten bieten, etwa Dienste gesetzeskonform in die Cloud zu verlagern oder mit Webservices zu agieren – und das alles in sicheren Umgebungen.

Wenn Kliniken technologisch alle Register für die IT-Sicherheit gezogen haben, bleibt ja noch der Mensch. Wie sensibilisieren Sie Mitarbeiter für das wichtige Thema?

A. Lockau: Das ist tatsächlich enorm wichtig. Ich kann da allerdings nur für meine Einrichtungen mit fast 7.000 Mitarbeitern sprechen. Wir haben entsprechende Hinweise in die Bildschirmschoner der Arbeitsplätze integriert, lancieren Meldungen im Intranet und versenden bei akuten Gefahrensituationen zusätzlich E-Mails. Auch im Mitarbeitermagazin platzieren wir regelmäßig Beiträge zum Thema. Unsere Mitarbeiter sollen vor Ort aufmerksam sein. Sie sollen regelmäßig ihr Passwort ändern, es mit niemandem teilen, jedes Mal den PC sperren, wenn sie ihn verlassen, und reagieren, wenn sich Fremde auf dem Gelände bewegen. Es geht aber auch darum, dass sie sensibel für Veränderungen der eigentlichen Daten werden: dass sie sich fragen, ob die Daten noch valide und korrekt sind.
Am Ende sind wir für die Einhaltung der Schutzziele verantwortlich. Allgemein sind das Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit, für Gesundheitseinrichtungen kommen noch Patientensicherheit und Behandlungseffektivität dazu.

Vielen Dank für die hilfreichen Einblicke und Anregungen, Herr Lockau.

Interview: Ralf Buchholz

„Informationssicherheit bekomme ich nicht umsonst und ganz bequem.

Dipl.-Inf. Andreas Lockau
Niels-Stensen-Kliniken und KH-IT