Foto: Echelon IMG – Fotolia

Wie sicher ist die IT in unseren Krankenhäusern?

Interview mit Dr. Deniz Ulucay

Die Digitalisierung ermöglicht bahnbrechende Fortschritte in der Versorgung und Behandlung von Patienten. Doch wo viel Licht, da viel Schatten – denn dadurch wird das Thema IT-Sicherheit für Krankenhäuser und andere Gesundheitseinrichtungen immer wichtiger. Doch leider wird es oft noch nicht mit der Priorität behandelt, die ihm eigentlich zusteht. Sei es aus Kostengründen oder auch aus Mangel an ausreichend qualifiziertem Personal. Wir sprachen mit Dr. Deniz Ulucay, der als Berater für Informationssicherheit, Lead Auditor für ISO 27001, Datenschutzbeauftragter und auch als Prüfer für §8a-BSIG Prüfungen tätig ist, darüber, wo Krankenhäuser noch Nachholbedarf haben.

Keywords: *IT, Datenschutz, Strategie*

Dr. Deniz Ulucay
Senior Berater und Auditor für Informationssicherheit

Die fortschreitende Digitalisierung des Gesundheitssystems beinhaltet notwendigerweise auch eine konsequente Weiterentwicklung der IT-Sicherheit. Patientendaten, digitale Gebäudetechnik u. a. sind ein lohnendes Ziel für Cyberkriminelle und es müssen angemessene Sicherheitssystematiken institutionalisiert werden, um Daten und Infrastruktur entsprechend zu schützen.

KU Die Attacke mit der Ransomware Wannacry richtete im Jahr 2017 weltweit große Schäden an – u. a. im britischen National Health Service (NHS). Untersuchungen mussten verschoben, Operationen abgesagt werden, der finanzielle Schaden war immens. Wie groß ist das Risiko, dass sich dieses Szenario auch in Deutschland abspielt?

Dr. Deniz Ulucay: Wir hatten solche Fälle bereits in Deutschland. Insbesondere der Vorfall im Lukaskrankenhaus in Neuss ging Anfang 2016 durch die Presse. Ganz klar war dies kein Einzelfall. Sowohl weitere Krankenhäuser als auch diverse andere Branchen waren betroffen. Allgemein wird angenommen, dass die Dunkelziffer der nicht öffentlich gemeldeten Vorfälle in Krankenhäusern relativ hoch ist. Ich gehe davon aus, dass dies nicht der letzte Vorfall dieser Art war.

Wie gut sind Kliniken auf Cyberattacken vorbereitet?

Unterschiedlich, tendenziell aber nicht gut genug. Aus unseren Prüfungen aufgrund des IT-Sicherheitsgesetzes wissen wir, dass der Reifegrad der IT-Sicherheit in Kliniken sehr heterogen ist. Häufig sind die IT-Abteilungen aber derart unterbesetzt, dass es kaum für die Behebung der ganz akuten Probleme reicht. Wartungsarbeiten, Strategien zur Verbesserung oder Notfallübungen stehen dann immer hinten an. Meiner Meinung nach fehlt es vielerorts an einem Verständnis bzw. einer Sensibilisierung der Klinikleitungen für die Kritikalität und den Ressourcenbedarf dieses Themas.

Was sind die schlimmsten Fehler oder Nachlässigkeiten der Kliniken beim Thema IT-Sicherheit?

Eine pauschale Antwort ist natürlich sehr schwierig. Aus IT-technischer

Sicht sind Medizingeräte häufig „Altsysteme", d. h. nicht mit neuesten Betriebssystemen oder Updates ausgestattet. Entsprechend ist es sehr wichtig, dass diese Geräte innerhalb des IT-Netzes abgeschottet (Netzsegmentierung) und die Zugriffsrechte auf das wirklich notwendige Minimum eingeschränkt werden (Berechtigungsmanagement). Leider ist es häufig eher so, dass es in Kliniken ein großes Netzwerk gibt, in denen alle Geräte betrieben werden, vom Fahrstuhl über Kaffeemaschine, Patientenzugänge, Parkhaustechnik bis hin zu MRT, PACS und KIS. Zusätzlich existieren wenig geschützte Fernwartungszugänge mit nahezu direkter Internetanbindung. In solch einem Fall reicht dann eine einzige Sicherheitslücke, um den gesamten Betrieb lahmzulegen. Dabei muss es sich noch nicht einmal um einen gezielten Angriff handeln.

Sind uns andere Länder hier voraus?

Ich würde behaupten, dass die USA in Bezug auf die Sicherheit von Medizingeräten mit den Vorgaben der FDA (Pre- & Postmarket Management of Cybersecurity) und der Prüfung durch eine staatliche Stelle etwas besser aufgestellt sind als die EU. Nichtsdestotrotz sind aber auch amerikanische Medizinprodukte aufgrund ihrer teilweise gravierenden IT-Schwachstellen regelmäßig in den Schlagzeilen. Mit den Anforderungen des IT-Sicherheitsgesetzes nimmt Deutschland eine gewisse Vorreiterrolle ein und ist zumindest für die als kritisch eingestuften Kliniken auf einem guten Weg. Die stete Medienpräsenz sowie die regelmäßigen Prüfungen fördern das Managementverständnis sowie die sukzessive Verbesserung der IT-Sicherheit gleichermaßen. Offen ist dabei bislang jedoch, ob und wie die teilweise dringend notwendigen, aber auch teuren Maßnahmen von den Kliniken finanziert werden können.

Ist der Zustand der IT-Sicherheit hauptsächlich eine Frage des Budgets?

Der Kostendruck hat natürlich einen großen Einfluss auf die IT-Sicherheit. IT- und Informationssicherheit wird häufig – solange alles funktioniert – als ausschließlicher Kostenverursacher gesehen, sodass bei den Ressourcen gerne gespart wird. Richtig ist, dass vorbeugende Maßnahmen Geld kosten und Ressourcen binden. Richtig ist jedoch auch, dass beispielsweise ein günstigerer Wartungsvertrag bei Nutzung eines Fernzugangs zusätzliche Risiken verursacht, die für einen sicheren Betrieb mit Maßnahmen versehen werden müssen. Ich bezweifle, dass solche Aspekte bei der Kosten-Nutzen-Rechnung bzw. der Abwägung von Risiken und Chancen ausreichend berücksichtigt werden. IT-Sicherheit ist daher wohl eher eine Frage der Priorisierung, die in hohem Maße von einem Verständnis der Abhängigkeit von funktionierender IT und den damit zusammenhängenden Risiken abhängt.

Mögliche Ziele sind ja nicht nur die großen Server der Kliniken, sondern auch Bereiche wie Medizin- oder Gebäudetechnik. Auch hier kann großer Schaden angerichtet werden. Wie sensibilisiert sind die Hersteller von Medizingeräten für Cybersicherheitsaspekte?

Im Bereich der Medizintechnik, aber auch im Bereich der Gebäudeleittechnik, scheint die IT-Sicherheit noch nicht wirklich angekommen zu sein. Häufig laufen uns immer noch Windows XP oder noch ältere Systeme über den Weg. Große Studien mit allgemeiner Aussagekraft sind nur schwer zu finden, jedoch zeigen Beispiele einiger Sicherheitsforscher, Penetrationstester oder White-Hat-Hacker leider immer wieder enorme Sicherheitslücken im Bereich der Medizintechnik. Ein wesentlicher Grund hierfür liegt meiner Meinung nach an den etablierten Entwicklungsprozessen der Vergangenheit: In der klassischen IT haben Geräte und Anwendungen eine übliche Einsatzdauer von zwei bis fünf Jahren. Ohne die obligatorischen Updates, die wir dort alle kennen, sind sie aber bereits nach wenigen Wochen „unsicher". Geräte der Medizintechnik, wie beispielsweise ein klassisches Röntgen- oder Ultraschallgerät, waren auf Betriebsdauern von zehn bis 30 Jahren ausgelegt und ohne „Updates" nach dieser Zeit immer noch „sicher". Mit der Vernetzung muss sich ein Wandel vollziehen, der beide Welten sinnvoll miteinander vereint.

Die Medizinprodukteverordnung (MDR) ist im Vergleich zu der vorherigen Version etwas anders strukturiert. Stellt sie eine echte Verbesserung für den Schutz von Patienten und Bedienern dar?

Nicht automatisch. Zwar werden einige Anforderungen, wie z. B. in Bezug auf Software, detaillierter als in der MDD geregelt, konkrete, sicherheitsfördernde Ableitungen werden aber auch mit der MDR nicht gegeben. Theoretisch fordern MDD wie auch MDR alles Notwendige zur Gewährleistung guter IT-Sicherheit – Verantwortung des Herstellers für die Sicherheit der Produkte, Risikoanalysen, Einhaltung des Standes der Technik, Korrekturprozesse und vor allem: Sicherheit der Patienten (MDR und MDD, jeweils Anhang I.I.1.). Anders als im Deutschen, wo es lediglich ein Wort für „Sicherheit" gibt, wird im Englischen zwischen „Safety" und „Security" unterschiedene. Erstere bezeichnet den sehr gut etablierten Teil bei Medizingeräten. Die Geräte sind also „safe" solange sie bestimmungsgemäß genutzt werden. Im Zuge der zunehmenden Digitalisierung und Vernetzung muss aber auch hinterfragt werden, wie „secure" oder resilient die Geräte gegen Angriffe sind. Die etablierten Methoden zum Risikomanagement sowie die Prüfverfahren im Zulassungsprozess müssen dahingehend angepasst werden. Meiner Meinung nach ist es unverantwortlich, dass zum einen die Hersteller keine verbindlichen Vorgaben an den Betreiber für einen sicheren IT-Betrieb ihrer Geräte machen müssen und zum anderen bislang noch keine verbindlichen Prüfverfahren zur Überprüfung der IT-Sicherheit bei Medizinprodukten festgelegt sind, wie beispielsweise regelmäßige Penetrationstests oder dass die Einschätzungen von IT-Risiken durch die Hersteller qualitativ von IT-Experten bewertet werden.

Die IT-Abteilung des Krankenhauses hat Server und Netzwerke bestmöglich gesichert, aber einzelne Mitarbeiter nutzen jahrelang die in den Werkseinstellungen vorgegebenen Zugangscodes (beispielsweise bei den Tür- und Schließsystemen), importieren Daten aus privaten USB-Sticks oder loggen sich auf Klinikrechnern in ihren

privaten Mailaccount und öffnen somit Tür und Tor für Malware jeglicher Art – da ist doch die beste Sicherheitsstrategie seitens der Gerätehersteller oder der Klinik machtlos?

Eine ganze Menge lässt sich positiv durch entsprechende technische Maßnahmen beeinflussen. In Bezug auf Ihre Beispiele ist man mit einem konsequenten Netzwerksegmentierungskonzept, aktuellem Schutz vor Schadsoftware, Datensicherungen und der Deaktivierung von eigentlich nicht benötigten Schnittstellen aus dem Gröbsten raus. Eine ganzheitliche Informationssicherheitsstrategie lässt sich aber auf rein technischem Weg nicht erreichen. Man muss natürlich die Mitarbeiter mitnehmen. Das schwächste Glied der Kette bestimmt hier letztlich das Sicherheitsniveau.

Sind die Menschen hier einfach gedankenlos oder wissen sie tatsächlich nicht um die Risiken eines solch leichtfertigen Verhaltens?

Bediener von Krankenhaus-IT sind eben meist keine IT-Security-Experten. Die Mitarbeiter müssen daher umfassend für einen sicheren Umgang mit Informationen und IT geschult werden. Eine kleine Online-Schulung „nebenbei", wie sie häufig zu finden ist, reicht meiner Meinung nach dafür nicht aus.

Gleichsam haben aber auch die IT-Fachleute häufig zu geringe Einblicke in die klinischen Prozesse, sodass die Umsetzung der vorgeschlagenen IT-Policies manchmal gar nicht mit der klinischen Realität vereinbar ist und hier „notgedrungen" IT-Sicherheitsmaßnahmen umgangen werden. Analog zur Verschmelzung von IT und Medizintechnik müssen entsprechend beide Seiten deutlich mehr miteinander in den Dialog treten.

Stichwort elektronische Patientenakte, Telemedizin, sektorenübergreifende Informationslogistik. Daten in einem abgeschlossenen System sicher zu verwalten ist schon anspruchsvoll – umso mehr noch, wenn auf sie von überall zugegriffen werden soll. Haben Sie als Experte manchmal Bauchschmerzen, wenn Sie den Status quo betrachten oder sind Sie guter Dinge, dass wir hier auf einem sicheren Weg sind?

Leider eher Bauchschmerzen. Eine Besonderheit von medizinischen Daten im Vergleich zu Passwörtern oder Kontodaten ist, dass diese deutlich länger geschützt werden müssen. Erbkrankheiten z. B. müssen über Generation hinweg vertraulich verarbeitet werden und können nicht einfach „gewechselt" werden, wie ein kompromittiertes Passwort. Eine der gängigen Forderungen: „so sicher wie Onlinebanking" reicht daher nicht aus. Für heutige Verschlüsselungsstandards wird eine „Sicherheit" von fünf bis 20 Jahren geschätzt, in Abhängigkeit von der Entwicklung der Rechenleistung, bislang unbekannten Sicherheitslücken und neuartigen Technologien (Stichwort: Quantencomputer). Das heißt ein Abgriff von heute verschlüsselten Daten aus zentraler Quelle, kann mit hoher Wahrscheinlichkeit in einigen Jahren „geknackt" werden. Ich bin mir nicht sicher, ob Chancen und Risiken bei der Zentralisierung von medizinischen Daten in einem günstigen Verhältnis für die Patienten stehen.

Ist die Gesetzgebung bzgl. des Datenschutzes manchmal auch hinderlich bei der Entwicklung innovativer IT-Systeme?

Mit dem Fokus auf Innovation kann man wahrscheinlich mit einem Ja antworten. Die entscheidende Frage ist aber doch, ob insbesondere in der Medizin Innovation vor Sicherheit gehen sollte. Ich bin der Meinung, dass die DSGVO im Kern sehr sinnvolle Anforderungen an den Umgang mit personenbezogenen Daten stellt. Da keine wesentlichen Verbote ausgesprochen, sondern vielmehr Abwägungen zwischen Chancen und Risiken gefordert werden, verlangt die DSGVO aus meiner Sicht nicht viel mehr, als ich mir im Falle eines verantwortungsvollen Umgangs mit sensiblen Daten ohnehin vorstellen würde. Leider gibt es immer noch eine Menge Fehlinterpretationen der Anforderungen der DSGVO, die zu viel Aufwand aber wenig Sicherheit führen und damit selbstredend Innovationen bremsen.

Wie zuverlässig sind digitale Signaturen?

Grundsätzlich lassen sich elektronische Nachrichten über Signaturverfahren zuverlässig absichern, also eindeutig einem Absender zuweisen oder die Unverändertheit bestätigten. Dies gilt jedoch nur unter der Bedingung, dass die Verfahren richtig implementiert sind, die Anwender einen sicheren Umgang pflegen (Stichwort: Passwort am Bildschirm) und die eingesetzten technischen Verfahren mit dem Stand der Technik gehen. Ähnlich wie bei der Verschlüsselung, können Signaturverfahren ihre Sicherheit nur über eine begrenzte Dauer gewährleisten. Auf der kurzfristigen Zeitskala kann die Integrität von Daten aber sehr gut mittels Signaturen geschützt werden.

IT-Experten werden überall händeringend gesucht. Wie können Krankenhäuser sich als attraktiver Arbeitgeber empfehlen? Mit der Höhe des Gehalts wohl eher nicht …

Ich glaube, dass gute Ärzte nicht wegen der Höhe des Gehaltes, sondern aufgrund von spannenden und verantwortungsvollen Aufgaben sowie einer hohen Anerkennung gerne in Kliniken arbeiten. Ich denke, dass – insbesondere in Kliniken – die Wertschätzung von IT-Experten häufig nicht ihrem Anteil und ihrer Kritikalität am Funktionieren des Gesamtsystems entspricht. Dementsprechend sollten sie auf Augenhöhe behandelt, mit spannenden, herausfordernden und verantwortungsvollen Aufgaben beschäftigt und insbesondere nicht mit erdrückender Arbeitslast beladen werden. Mit fairer, aber nicht überhoher Entlohnung sollte man dann eigentlich gute und motivierte Mitarbeiter finden und halten können.

Herr Dr. Ulucay, vielen Dank für das Gespräch. ■

Das Interview führte KU-Fachredakteurin Birgit Sander.