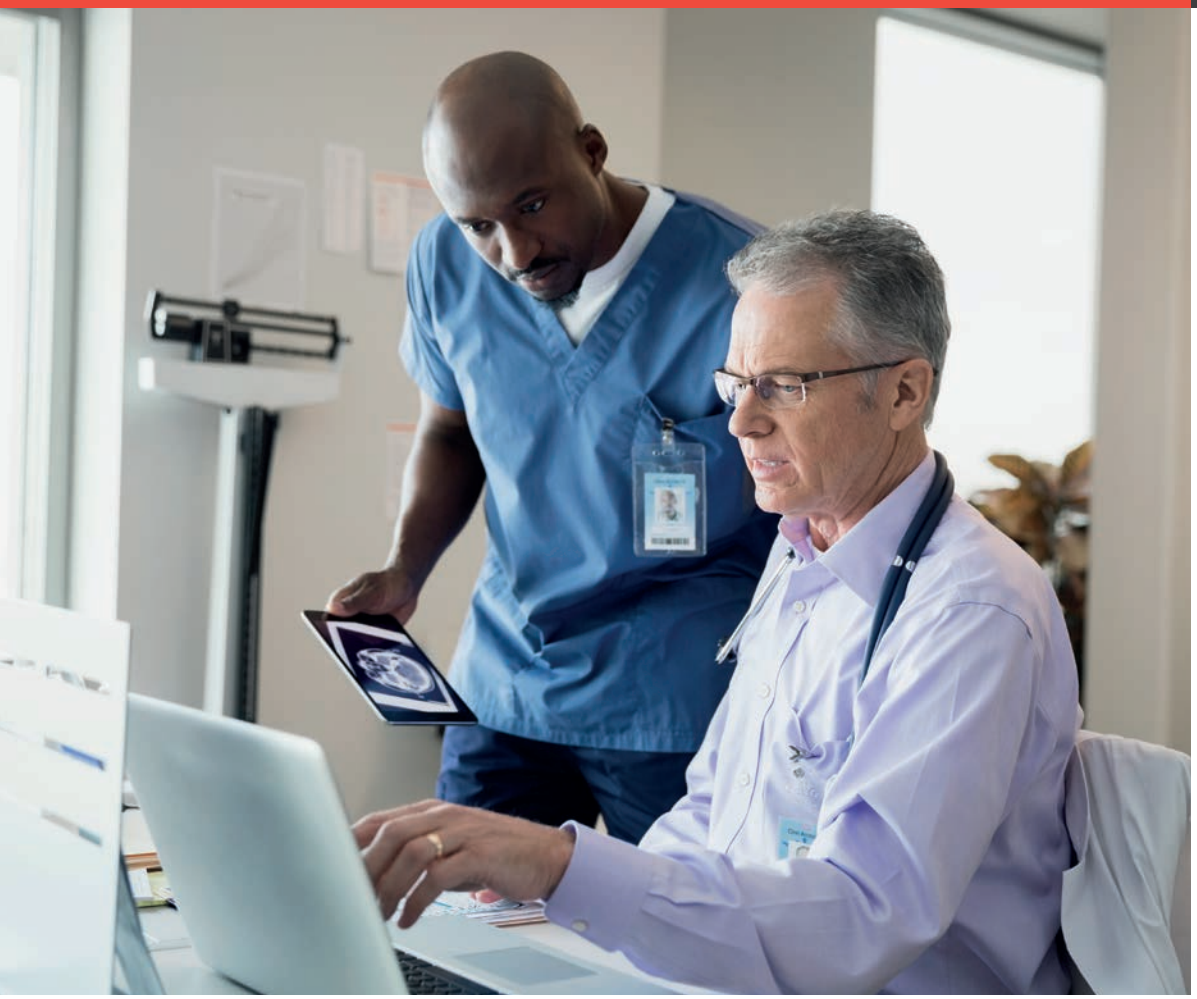
Die unsichtbare Gefahr: Wie steht es um die Cybersicherheit von OT-Systemen in Krankenhäusern?

Wie Steuerungssysteme (Operational Technology) in medizinischen Geräten, Gebäuden und technischen Anlagen ein vulnerabler Angriffspunkt für Krankenhäuser sein können.



pwc

Eine neue Variante von Cyberangriffen

Stellen Sie sich folgendes Szenario vor: Sie sind Geschäftsführer eines Krankenhauses mit mehreren hundert Betten. Viele dieser Betten sind mit einem Anschluss für medizinischen Sauerstoff ausgestattet. Eines Morgens werden Sie alarmiert und darüber informiert, dass die Sauerstoffzufuhr an unzähligen Betten unterbrochen wurde.

Einige Patienten befinden sich jetzt in unmittelbarer Lebensgefahr. Verzweifelt bemüht sich das gesamte Personal darum, die Patienten in ihren Betten auf andere Stationen zu bringen – in der Hoffnung, dass dort noch Sauerstoff verfügbar ist. Bald stellt sich heraus, dass die Aufzüge nicht mehr funktionieren und sich die Betten auf den Fluren stauen.

Dann erhalten Sie eine weitere Nachricht: Die Klimaanlage ist im gesamten Gebäude ausgefallen. Dadurch steigt die Temperatur auf der Intensivstation und in den Operationssälen rapide an, was dazu führt, dass medizinische Eingriffe abgebrochen und Operationen bis auf weiteres abgesagt werden müssen.

Im Ergebnis ist Ihr Krankenhaus effektiv lahmgelegt worden. In diesem Moment erhalten Sie die erste Mitteilung der Cyber-Kriminellen, die mit ihrem Angriff dieses Chaos verursacht haben. Sie teilen Ihnen mit, welche Bedingungen Sie erfüllen müssen, damit der Krankenhausbetrieb fortgesetzt werden kann.

Steuerungssysteme als Achillesferse

Das klingt leider nicht mehr nach Science-Fiction und ist durchaus ein realistisches Szenario. Die Steuerungssysteme vieler Krankenhäuser sind erschreckend anfällig für Cyberangriffe. Das Spektrum an möglichen Angreifern ist gleichzeitig breit – von Erpressern bis zu Terroristen oder anderen Nationen, die dazu bereit und fähig sind, einen solchen Angriff durchzuführen oder vorzubereiten. Die COVID-19 Pandemie hat zwar nicht zu einer größeren Anfälligkeit der Steuerungssysteme innerhalb der Krankenhäuser geführt, aber die gesellschaftliche Bedeutung zuverlässig funktionierender medizinischer Einrichtungen verdeutlicht. Das macht Krankenhäuser zu attraktiven Zielen für Angreifer – stellen Sie sich vor, ein fremder Staat hätte einen „roten Knopf", mit dem sich die Sauerstoffversorgung, Klimaanlagen oder sonstige Gebäudetechnik in allen Krankenhäusern eines Landes unterbrechen ließe.

Vor diesem Hintergrund stellt sich die Frage, warum Steuerungssysteme im medizinischen Bereich nicht besser vor Cyberangriffen geschützt werden. Tatsache ist, dass der Fokus der Gesundheitsorganisationen im Hinblick auf Cybersicherheit momentan mehr darauf liegt, die Informationstechnologie (IT) und die medizinischen Daten zu schützen, als die Steuerungssysteme von Geräten und Gebäuden. Warum dies so ist, liegt klar auf der Hand: In den letzten Monaten und Jahren waren IT-Systeme von Krankenhäusern mehrfach gezielten Angriffen und Schadprogrammen ausgesetzt. Dabei wurden Patientendaten gestohlen oder verschlüsselt und dann für die Wiederherstellung dieser Daten Lösegeld verlangt. Die OT war bislang selten betroffen.

Die Update-Falle von Medizinprodukten

Die Situation rund um Medizinprodukte kann sich delikat darstellen in Bezug auf Cybersicherheit. Sie werden von den Herstellern in einer Softwareversion ausgeliefert, die zum Zeitpunkt der Inbetriebnahme bereits veraltet sein kann. Die strenge Regulierung von Medizinprodukten ermöglicht es dem Betreiber jedoch nicht, die Software eigenständig auf dem neuesten Stand zu halten. Am Beispiel eines Penetration-Tests von Röntgensystemen konnten wir selbst feststellen, wie ein Krankenhausbetreiber gezwungen war, ein medizinisches Großgerät zu betreiben, in dem der Hersteller Drittkomponenten (in diesem Fall Webserver) verwendet hatte, die unsicher waren und dazu geführt haben, dass unsere Experten binnen Minuten vollen administrativen Zugriff auf die Modalität hatten, sowie auf den Datenbestand.

Zum Zeitpunkt des Zulassungsverfahrens wird dieses Gerät vermutlich den Anforderungen genügt haben. Der Stand der Technik entwickelt sich je-doch in einer Geschwindigkeit weiter, der Zulassungsbehörden nicht Schritt halten können. Hinzu kommt, dass es leider häufig immer noch gängige Praxis ist, dass die Netzwerke für medizinische Geräte und die restliche Krankenhaus-IT nicht voneinander getrennt sind. Selbst wenn dies vorbildlich umgesetzt wurde und solche Geräte in separierten Netzwerken betrieben werden, gibt es zu ihrer Nutzung immer eine Schnittstelle in die Krankenhaus-IT, über die z. B. Bilddaten, Laborresultate oder Steuerungs- und Wartungsinformationen ausgetauscht werden.

Cybersicherheit als staatliches Förderziel

Der WannaCry-Angriff hat im Jahr 2017 allen Nationen das Risiko von Cyberangriffen auf kritische Infrastrukturen, insbesondere Krankenhäuser, vor Augen geführt. Damals traf es viele britische Krankenhäuser. Doch auch im deutschsprachigen Raum gibt es eine unschöne Regelmäßigkeit von Cybervorfällen im Gesundheitswesen. Ein dramatischer Höhepunkt war im September 2020 als die IT-Systeme des Düsseldorfer Universitätsklinikums von einem Schadprogramm befallen wurden. Eigentliches Ziel der Cyber-Kriminellen war wohl die Universität, die mit dem Klinikum verbunden war. Dennoch waren die Folgeschäden fatal: Wegen dieses Angriffs konnte das Krankenhaus eine Patientin nicht aufnehmen, die daraufhin später verstarb – der vermutlich erste bekannte Todesfall im Zusammenhang eines Cyberangriffs auf ein Krankenhaus. Bereits vor diesem tragischen Vorfall haben in Deutschland Bemühungen begonnen, die Cybersicherheit von Krankenhäusern zu verbessern, nachdem in den letzten Jahren eine ganze Reihe von Krankenhäusern Cyber-Kriminellen zum Opfer gefallen war. Im September 2020 wurde das sogenannte Krankenhauszukunftsgesetz verabschiedet, das 4,3 Milliarden Euro an öffentlichen Mitteln für die Digitalisierung und Sicherheit in Krankenhäusern zur Verfügung stellt. Diese sollten auch genutzt werden, denn deutsche Krankenhäuser haben jetzt vier Jahre Zeit, digitale Dienste zu entwickeln und zur Verfügung zu stellen. 15 Prozent der Investitionen müssen dabei explizit in Cybersicherheit fließen, einer der Fördertatbestände adressiert sogar explizit Projekte, die ausschließlich der Steigerung der Cybersicherheit dienen. Ein Blick nach Österreich zeigt, dass auch dort der Schutz von Krankenhäusern als Teil des österreichischen Programms zum Schutz kritischer Infrastruktur als wesentlich erkannt wird. Eine vergleichbare Förderung gibt es aber bislang nicht.

Der blinde Fleck in Organisation und Management

Der Krankenhauszukunftsfonds hat zum Ziel, die Digitalisierung in Krankenhäusern zu steigern und gleichzeitig die Cybersicherheit zu verbessern. In der Regel zielen förderbare Projekte auf digitale Dienstleistungen bzw. vernetzte Prozesse. Somit ist die Aufmerksamkeit auf die Anwendungsebene und die Gefahren durch Ransomware-Attacken auf das Krankenhausinformationssystem und deren angebundene IT-Infrastruktur gelenkt.

Bei allem Fokus auf Modernisierung und Schutz der IT-Systeme können andere Risiken übersehen werden, die mindestens ebenso alarmierend sind: z. B. die Gefahr, die von Angriffen auf Steuerungssysteme, insbesondere die Gebäudemanagementsysteme ausgeht. Diese Anlagen sind Teil des OT-Netzwerks der Krankenhäuser und spielen eine erhebliche aber oft unsichtbare Rolle für die Funktionsfähigkeit aller Bereiche der Patientenversorgung. Ein solches System reguliert beispielsweise die Be- und Entlüftungssteuerung, Heizung, Klimatisierung oder Zutritts- und Transportsysteme wie etwa Lifte, aber auch die Beleuchtung. Neben der Gebäudesteuerung gibt es aber noch Steuerungssysteme für medizinische Produkte, wie beispielsweise Röntgen- oder Beatmungsgeräte. Besonders in der Intensivmedizin oder Spezialabteilungen ist eine Nutzung von vernetzten Medizingeräten unabdingbar für die Patientenversorgung.

Schwachstellen in Hinblick auf das Management von Cyber-Risiken in Krankenhäusern sind häufig bereits in den Organisationsstrukturen zu finden. Der Chief Information Security Officer (CISO) sollte verantwortlich sein für die Cybersicherheit im gesamten Unternehmen. Der Zuständigkeitsbereich des CISO in Krankenhäusern beschränkt sich jedoch meist auf den IT-Bereich und umfasst nicht immer die Gebäudesteuerung oder die Medizingeräte. Mit anderen Worten: Oftmals herrscht keine Klarheit über die Zuständigkeit für und Verantwortung von Cyber-Risiken für Geräte und Steuerungssysteme, obwohl diese unmittelbaren physischen Einfluss auf Patienten und den Krankenhausbetrieb haben können. Noch gefährlicher ist die Situation in den vielen kleinen und mittleren medizinischen Versorgungszentren, in denen es die Rolle eines dedizierten CISO nicht gibt und die Gefahren somit nicht professionell erfasst und mitigiert werden.

OT-Cyber-Risiken finden sich nicht nur in Krankenhäusern

Alle größeren Gebäude in denen Menschen arbeiten – also nicht nur Krankenhäuser, sondern auch Bürogebäude, Einkaufszentren und Produktionsstätten – nutzen ein Gebäudesteuerungssystem zur Regulierung und Überwachung der Gebäudetechnik und der Anlagen auf dem Betriebsgelände.

Während IT-Systeme und Netzwerke primär dazu da sind, Daten zu speichern, abzurufen, zu verarbeiten und darzustellen, liegt der Fokus bei OT-Systemen auf der Überwachung und dem Betrieb der physischen Funktionen von Geräten und Anlagen. In einem Krankenhaus geht es hierbei ebenfalls um Gebäudeleittechnik aber auch um eine Vielzahl medizinischer Geräte mit eingebauten Steuersystemen.

Ein wichtiges Element im OT-Netzwerk von Krankenhäusern ist die Gebäudeleittechnik. Dies gilt nicht nur für „smarte“ Gebäude jüngster Bauzeit. In den meisten modernen Gebäuden sind digitale Kontrollsysteme verbaut, die mittels Sensorik auf bestimmte Ereignisse reagieren und Prozesse auslösen. in Krankenhäusern sind das z. B. die Messung und Überwachung der Temperatur in verschiedenen Bereichen, sodass das Gebäudeleitsystem die Klimaanlage und die Heizung jederzeit auf angenehmen Temperaturen für Personal und Patienten halten kann. Ebenso werden auch Beleuchtung, Be- und Entlüftungsöffnungen sowie Sicherheitsvorrichtungen kontrolliert. Auch die Aufzüge werden durch Gebäudeleittechnik überwacht und gesteuert.

Ein besonders sensibler Bereich sind Schnittstellen zwischen der IT- und der OT-Infrastruktur. Diese finden sich dort, wo bildgebende Diagnostik beispielsweise von Radiologiesystemen (z. B. CT, Röntgengerät) an die Dokumentations- und Kommunikationssysteme (PACS bzw. KIS) übertragen werden. Diese Systeme altern über einen vergleichsweise langen Lebenszyklus teurer Großgeräte und sind dennoch schwer wartbar, weil sie im Geltungsbereich des Medizinprodukte-gesetzes nicht einfach regulären Updates unterzogen werden können. Die Verfügbarkeit und Zuverlässigkeit hybrider IT/OT-Systemlandschaften in Krankenhäusern kann dadurch zu einer möglichen Gefahr für die Patientensicherheit werden. Diese Systeme müssen im Alltagsbetrieb fehlerfrei arbeiten und selbst unter widrigen Umständen funktionieren.

4 Die unsichtbare Gefahr: Wie steht es um die Cybersicherheit von OT-Systemen in Krankenhäusern?

... aber die Auswirkungen von Angriffen können hier um ein Vielfaches schlimmer sein

Zwar sind die Grundstrukturen der OT in Krankenhäusern mit anderen Gebäudearten vergleichbar, doch die möglichen Auswirkungen eines Cyberangriffs auf das OT-Netzwerk sind in Krankenhäusern um ein Vielfaches verheerender. Nehmen wir ein Wohngebäude als Beispiel: Ein Zusammenbruch der OT führt hier zu Unannehmlichkeiten und möglicherweise zu finanziellen Verlusten. In einem Krankenhaus jedoch sind die Auswirkungen erheblich größer. In einem Bürogebäude ist ein Ausfall der Klimaanlage oder der Aufzüge im schlimmsten Fall unbequem, im Krankenhaus können Menschenleben auf dem Spiel stehen. Ebenso dramatisch wären die Auswirkungen eines Zusammenbruchs der Strom- oder Wasserversorgung. Der Ausfall von Medizingeräten kann dramatische Folgen haben.

Angriffe auf OT-Systeme können jederzeit und völlig unerwartet auftreten und viele Bereiche treffen: Gebäudeinfrastruktur- und Gebäudeverwaltungssysteme wie Beleuchtung, Türöffnungsmechanismen, Aufzüge oder Klimaanlagen. Alles Systeme, die in vielen Fällen schon seit Jahrzehnten verwendet werden, aber mittlerweile über digitale Anwendungen gesteuert und häufig auch mit dem Internet verknüpft sind, um eine einfache Wartung zu ermöglichen. Zuständig ist nicht selten ein externer Dienstleister, für dessen Auswahl Kostengründe oder Bequemlichkeit sprachen. Ein Angreifer, der Kontrolle über diese Systeme erlangt, kann den Betrieb eines Krankenhauses komplett lahmlegen – und die Geschäftsführung unter erheblichen Druck setzen, jegliche Lösegeldforderung zu begleichen.

Ganz unmittelbar kritische Systeme in Krankenhäusern sind die Wasser- und Gasversorgung innerhalb der Gebäude. Die Funktion des Systems, heißes Wasser, Druckluft und medizinische Gase wie Sauerstoff oder Stickstoff überall dahin zu transportieren, wo sie gebraucht werden, macht sie unentbehrlich für die Erbringung von medizinischen Leistungen. Die Infrastruktur, die jedes Bett mit Sauerstoff versorgen kann, ist im Wesentlichen nichts anderes als ein großes Rohrsystem mit einem Sauerstoff- bzw. Wassertank an einem Ende, das von einem Steuerungssystem geregelt wird. Um sich die Auswirkungen einer Manipulation der Steuerungseinheit dieses Versorgungssystems auszumalen, bedarf es wenig Fantasie.

Risiken der OT-Systeme: Schichten und Kontrollen

Im Hinblick auf Cyber-Risiken ist jede der verschiedenen digitalen Systemschichten innerhalb eines Krankenhauses durch eine Kette aus Liefer- und Supportfunktionen untereinander verbunden, sodass sich ein digitales „Supply Chain Netzwerk“ formt. Dies birgt die Gefahr, dass Angreifer über eine „Hintertür“ von der OT-Schicht auch Zugriff auf die kritischen IT-Systeme eines Krankenhauses erlangen können und anders herum.

Bis heute sind vergleichbare Angriffe auf Steuerungssysteme von Krankenhäusern zum Glück sehr selten. Aber es ist nur eine Frage der Zeit, bevor OTs aus dem Gesundheitswesen in den Fokus der Cyber-Angreifer gelangen. Die Herausforderungen für Krankenhäuser, sich auf solche Angriffe vorzubereiten, werden dadurch noch größer. Die Maßnahmen zur Absicherung müssen von IT-Abteilungen umgesetzt werden, die nicht selten bereits am Limit der Ressourcen arbeiten.

Beispiele für Vorfälle oder Beinahe-Vorfälle

2017 – Luxusklinik vergaß IT im Netz (Schweiz)
Das Gebäuesteuerungssystem einer schweizer Luxusklink war aus dem Internet erreichbar.

2017 – Herzschrittmacher angreifbar (USA)
Herzschrittmacher und Defibrillatoren eines amerikanischen Herstellers weisen eine Sicherheitslücke auf, die dazu genutzt werden kann, das Implantat zu stören.

2019 – Schwachstelle in implantierten Defibrillatoren (USA)
Die implantierten Geräte können über eine Funkverbindung ohne Verschlüsselung, Authentifizierung und Autorisierung programmiert werden.

2019 – Schwachstelle in Beatmungs- und Anästhesiegeräten eines internationalen Herstellers (USA)
Die identifizierten Schwachstellen erlauben es einem Angreifer im selben Netzwerk, die weit verbreiteten Medizingeräte zu übernehmen und zu manipulieren.

2020 – Verschiedene Schwachstellen in Medizinprodukten (USA)
Verschiedene medizinische Geräte eines amerikanischen Herstellers sind mit vergleichbar trivialen Attacken angreifbar.

Wirksame Sicherheitskonzepte umfassen drei Faktoren: Prozesse, Menschen und Technologie. Wird nur einer der drei Aspekte vernachlässigt, tun sich Schwachstellen auf. Die sicherheitsrelevanten Prozesse beginnen etwa schon bei formellen Beschaffungs- und Entsorgungsverfahren für technische Geräte, die Standards für Cybersicherheit einbeziehen müssen. Mitarbeiter durch frontale Seminare und Workshops zu schulen reicht heute nicht mehr aus – auch moderne digitale Formate und Lernerfolgsmessung sind nur ein Zwischenschritt zu einer Kultur der Cybersicherheit, auf die alle Maßnahmen zielen müssen. Der Stand der Technik ist schließlich in steter Weiterentwicklung, sodass nur gut ausgebildetes und wachsames Personal und ständig optimierte Prozesse dafür sorgen können, dass die Technologie zeitgemäß, performant und sicher bleibt. Unabdingbar sind aber zielgerichtete und anwendbare Sicherheitsmaßnahmen, die den medizinischen Betrieb nicht einschränken.

Eine Sicherheitsstrategie in vier Schritten

Die Zukunft der Medizin ist hochgradig digital. Deshalb müssen wir uns auch die Frage stellen, wie Krankenhäuser und andere Gesundheitseinrichtungen ihre Systeme und Geräte bestmöglich gegen Cyber-Bedrohungen schützen können. Ein ungelöstes Problemfeld liegt in der rasanten Weiterentwicklung technischer Komponenten, die immer weiter vernetzt werden, während das Bewusstsein für die neuen und unbekannten Risiken, die damit unweigerlich verbunden sind, nicht in gleicher Geschwindigkeit zuwächst. Dieses Spannungsfeld müssen Krankenhäuser unbedingt schließen.

Die folgenden vier Schritte können Krankenhäuser dabei unterstützen, Resilienz gegen Cyber-Bedrohungen aus der OT-Sphäre zu stärken:

1

Die Gefahr verstehen

Im ersten Schritt muss ein Verständnis geschaffen werden, dass nicht nur die IT-, sondern auch die OT-Systeme eines Hauses gefährdet sind. Die spezifischen Risiken der einzelnen Systeme werden erfasst, Schwachstellen identifiziert und unmittelbare Gegenmaßnahmen entwickelt. Bereits in diesen Prozess muss die Krankenhausleitung unbedingt eingebunden werden.

2

Ein Zielbild für die OT-Security entwickeln

Die Risiken der OT-Landschaft sind Ausgangspunkt, um grundlegende Fragen zu stellen. Welche Gegenmaßnahmen sind am drängendsten? Welche Systeme sind nicht mehr wartbar, weil der Servicezeitraum des Herstellers abgelaufen ist oder sie nachträglich undokumentiert verändert wurden? Welche dieser „Altlasten" können oder müssen zwangsläufig durch Neuanschaffungen ausgetauscht werden? Und auch, wie kann der komplette Bereich der OT-Security unter eine Governance- und Managementstruktur gestellt werden?

3

Integration in eine Cyber-Sicherheitsstrategie

Sind die Handlungsfelder der OT-Security erfasst, können sie in eine übergeordnete Cyber-Sicherheitsstrategie integriert werden. Hierzu braucht es ein Cyber-Team, das um weitere Experten für Gesundheitstelematik, Medizintechnik, Gebäudeleittechnik und OT-Security ergänzt wird. Der CISO hat somit nicht nur die strategische Konzeption, sondern auch eine multidisziplinäre Koordinationsaufgabe zu managen. Die Sicherheitsagenda ist ein Thema für das Top-Management, bei dem letztendlich auch die Verantwortung liegt. Eine ehrliche Kommunikation über Risiken und Schwachstellen ist daher ebenso erforderlich, wie ein Verständnis über die medizinischen Abläufe im Haus und die Wechselwirkungen zwischen Cyber-Risiken in IT und OT. Fehlt Expertise in einem Bereich, werden nicht selten unabhängige Sicherheitsteams herangezogen.

4

IT- und OT-Strategie finanzieren und umsetzen

Je nach bisherigem Reifegrad der Cybersicherheit stehen nun entweder nur die OT-Sicherheitsstrategie zur Umsetzung an oder die gesamte IT- und OT-Sicherheitsstrategie. Die Maßnahmen können nach Umfang, Auswirkungen, Umsetzungsgeschwindigkeit und Kosten priorisiert werden. Für die Finanzierung bieten sich derzeit für deutsche Krankenhäuser Mittel aus dem Krankenhauszukunftsfonds an, mit dem Bund und Länder insgesamt 4,3 Milliarden Euro zur Verfügung stellen, die für die Sicherheit und Digitalisierung in Krankenhäusern eingesetzt werden können.

Gewährleistung der zukünftigen Sicherheit von Steuerungssystemen

Wirksame Cyber-Sicherheitsmaßnahmen müssen grundsätzlich die drei Elemente Prozesse, Menschen und Technologie umfassen. Wo immer einer dieser drei Bereiche vernachlässigt wird, bleiben Steuerungssysteme oder Organisationen ungeschützt und verwundbar. Darin unterscheidet sich die Cybersicherheit nicht von der Bekämpfung anderer Bedrohungen, wie physischer Sabotage, elektrischen Kurzschlüssen, Feuer oder Wasserschäden. Ein Krankenhauskeller ohne Feuermelder und Feuerlöscher ist natürlich undenkbar – es ist ein logischer Schritt für Krankenhäuser, die selbe Denkweise für Cyber-Überwachungs- und Verteidigungsmechanismen zu etablieren. Dies ist nicht nur wünschenswert, sondern zwingend erforderlich.

Aufbau einer „Cyber-Hygiene“-Kultur

Um Cyber-Bedrohungen sowohl für OT- als auch für IT-Systeme wirksam bekämpfen zu können, sollten Krankenhäuser eine Kultur der digitalen Sicherheit entwickeln und verankern. Diese Kultur muss analog der guten Praxis von Hygiene im medizinischen Alltag gehen, die für jeden, der in einem Krankenhaus arbeitet, eine Selbstverständlichkeit ist.

Unser Team für Sie

Jörg Asma
PwC Deutschland
Partner, Digitalisierung und Sicherheit im Krankenhaus
Mobiltel.: +49 160 6142945
E-Mail: joerg.asma@pwc.com

Dr. Benedict Gross
PwC Deutschland
Senior Manager, Digitalisierung und Sicherheit im Krankenhaus
Mobiltel.: +49 151 14325832
E-Mail: benedict.gross@pwc.com

Dr. Oliver Hanka
PwC Deutschland
Director, OT Security
Mobiltel.: +49 160 5105836
E-Mail: oliver.hanka@pwc.com

Georg Beham
PwC Österreich
Partner, Cybersecurity & Privacy Leader
Tel.: +43 732 611750
E-Mail: georg.beham@pwc.com

Florian Brunner
PwC Österreich
Senior Manager, Cybersecurity & Privacy
Mobiltel.: +43 676 8337 75455
E-Mail: florian.brunner@pwc.com

Rafael Maman
PwC Israel
Partner, Cyber Security
Tel.: +972 52 358 9008
E-Mail: rafael.maman@pwc.com