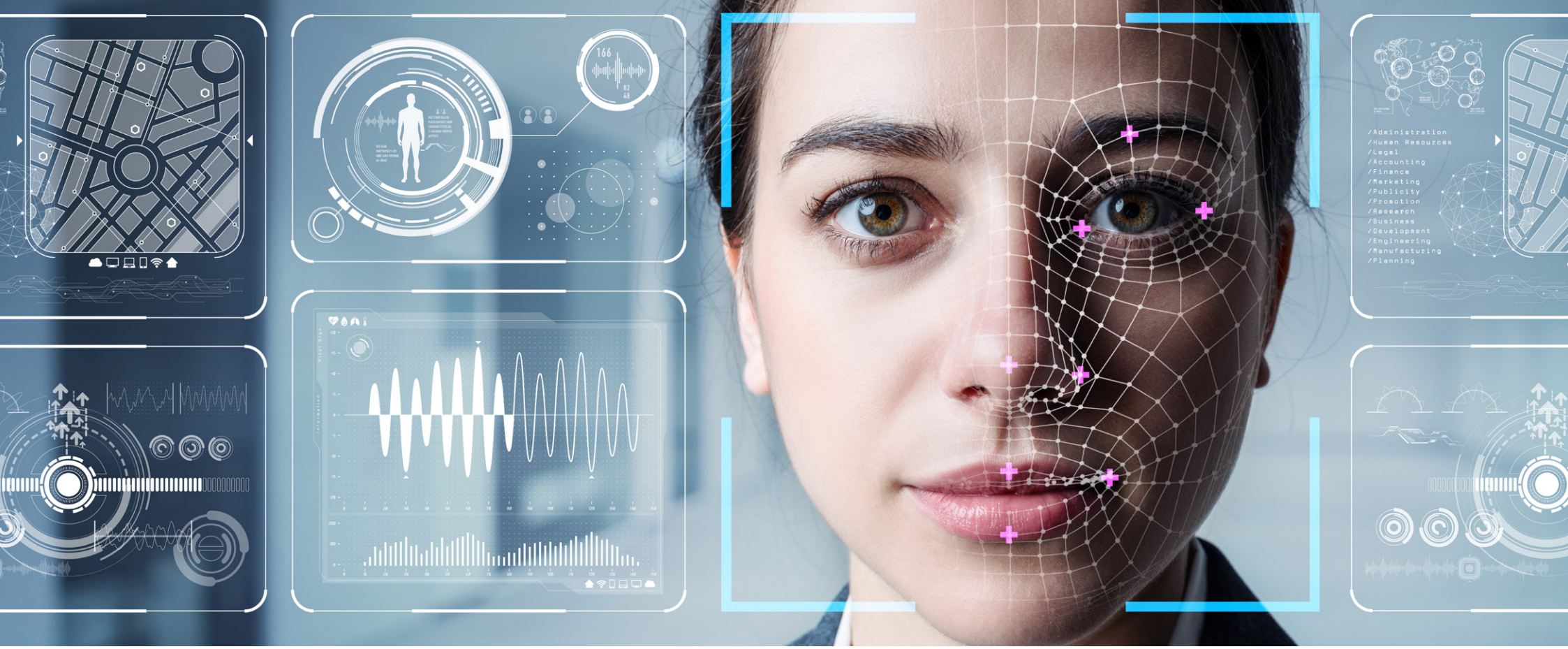


Cybersecurity im Gesundheitswesen in Zeiten der digitalen Transformation

Inklusive Interview mit Silvia Piai,
Research Director bei IDC Health Insights

IDC ANALYZE THE FUTURE

Broschüre

Alcatel·Lucent Enterprise

Kurzübersicht

Das Thema Cybersicherheit hat im Gesundheitswesen bereits seit langem eine hohe Priorität. Durch den stetigen Fortschritt der digitalen Transformation ändern sich auch die Anforderungen daran, was Cybersicherheit wirklich bedeutet. Digitale Transformation heißt, dass in Netzwerken des Gesundheitssektors vermehrt vernetzte und mobile Geräte eingesetzt werden und Mediziner, Partnerinstitutionen und niedergelassene Ärzte verstärkt auf Apps und Daten zugreifen werden, die außerhalb ihres eigenen Netzwerks liegen. Und der Wandel vollzieht sich immer schneller: Um mitzuhalten und die Netzwerksicherheit zu gewährleisten, braucht es daher neue Wege.

In diesem White Paper berichtet Silvia Piai, Research Director bei der International Data Corporation (IDC), über die Anforderungen an die Cybersicherheit in einem Gesundheitswesen im Wandel. Sie empfiehlt auch Strategien und Technologien, die in Zeiten der digitalen Transformation zur Sicherheit von Daten und Systemen beitragen. Alcatel-Lucent Enterprise führt außerdem aus, wie die Lösung Digital Age Networking (DAN) zunehmend digitalisiert arbeitende Unternehmen unterstützt. DAN setzt als Cybersecurity-Konzept gleich an mehreren Punkten an. Der Zugang zu vernetzten medizinischen Geräten, Patientendaten und Software-Anwendungen im Ökosystem des Gesundheitswesens erfolgt sicher und nach exakt festgelegten Regeln: DAN bedeutet Vertraulichkeit.

Bestandsaufnahme: Cybersicherheit im Gesundheitswesen heute

Der Gesundheitssektor hat 2019 global **5,5 Mrd. US-Dollar** in die Cybersicherheit investiert.

Studie um Studie der IDC zeigt sich, dass die Cybersicherheit für die Organisationen im Gesundheitssektor höchste Priorität hat.[1] Das überrascht nicht. Das Gesundheitswesen ist schon seit langem, und auch weiterhin, eine Branche, die besonders im Visier der Hacker steht. Und dieses Problem scheint weiter zu wachsen. 2018 verzeichnete das Gesundheitswesen 503 Cyberangriffe, die 15 Millionen Patientenakten betrafen, drei Mal so viel wie 2017, laut dem Protenus Breach Barometer.[2]

Diese Cyberangriffe gibt es, weil Gesundheitsdaten extrem wertvoll sind. Patientenakten enthalten eine Menge persönlicher Daten: Name, aktuelle und frühere Adressen, berufliche Laufbahn, Namen und Alter der Angehörigen sowie Finanzdaten, etwa Kreditkartennummern und Kontodaten.[3]

Der Schaden von Cyberangriffen geht dabei über den Datendiebstahl weit hinaus: Es kann zu Betriebsunterbrechungen kommen, der Ruf eines Krankenhauses steht auf dem Spiel und es werden ggf. auch Strafen fällig, weil gegen geltendes Recht verstoßen wurde, etwa den Health Insurance Portability and Accountability Act (HIPAA) in den USA oder die Datenschutz-Grundverordnung (DSGVO) in der Europäischen Union. Noch schlimmer ist, dass ein solches Ereignis das Potenzial hat, Patienten körperlich zu schädigen. Zum Beispiel, wenn eine Insulinpumpe die falsche Menge Insulin abgibt. Oder der behandelnde Arzt wichtige Informationen zum Patienten nicht erhält, etwa über Allergien oder Medikamente, die der Patient bereits einnimmt.

Nach Schätzungen der IDC hat der Gesundheitssektor 2019 global 5,5 Mrd. US-Dollar in die Cybersicherheit investiert, um diese Risiken abzumildern. Bis 2022, so prognostiziert IDC, werden die Ausgaben im Bereich der Cybersicherheit im Gesundheitssektor jährlich um 8,7 Prozent steigen, ähnlich wie in anderen Branchen auch.[4]

Aber trotz dieser Summen weist die Cybersicherheit im Gesundheitswesen weiterhin Schwachstellen auf. Zwar schreibt sich nahezu jede Organisation im Gesundheitssektor die Cybersicherheit auf die Fahne, in der Praxis jedoch kommt das Thema häufig zu kurz. Schließlich sehen es Mediziner als ihre Aufgabe, in erster Linie Menschen zu behandeln, und nicht, sich mit Fragen der Cybersicherheit zu beschäftigen. Das Gesundheitspersonal neigt zudem dazu, sich Maßnahmen für mehr Cybersicherheit zu widersetzen, wenn diese die klinischen Arbeitsabläufe vermeintlich erschweren. Wenn zum Beispiel Ärzte, Pflegepersonal oder Kliniker das Gefühl haben, dass sie zu viel Zeit damit verbringen, sich einzuloggen oder sich zu authentifizieren, um Zugang zu elektronischen Gesundheitsakten (EMR/EHR) zu erhalten, werden sie nach Wegen suchen, diesen Prozess abzukürzen. Bei vielen Klinikärzten herrscht allerdings auch kein ausreichendes Bewusstsein für Cybergefahren und deren weitreichende Folgen.

1 Zum Beispiel: Priorities, Strategies, and Investments: Overcoming DX Challenges in European Healthcare https://www.idc.com/getdoc.jsp?containerId=EMEA44355219

2 https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2019-so-far

3 https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#2bb1f96b50cf

4 IDC's Worldwide Semiannual Security Spending Guide https://www.idc.com/getdoc.jsp?containerId=IDC_P33461

Cyberbedrohungen im Wandel

Gleichzeitig wird die Cybersicherheit auf immer neue Art herausgefordert. Mittels künstlicher Intelligenz (KI) und maschinellem Lernen (ML) werden die Angriffe immer raffinierter und sie laufen zunehmend automatisiert ab. Durch neue Techniken des Social Engineering gelingt es Hackern, aus bruchstückhaften Informationen, die quer durch die sozialen Medien auffindbar sind, beeindruckend zutreffende Profile von Einzelpersonen oder von Datenbeständen zu erstellen, die bei Organisationen im Gesundheitswesens gelistet sind.

Mit der digitalen Transformation im Gesundheitssektor werden auch die Anforderungen an die Cybersicherheit anspruchsvoller: Die Komplexität nimmt zu, es sind immer mehr vernetzte Geräte im Einsatz, es vollzieht sich eine räumliche Entgrenzung – und all das in einem atemberaubenden Tempo.

Höhere Komplexität

Organisationen des Gesundheitswesens arbeiten mit neuer Technologie: Cloud, mobile Geräte, Internet der Dinge (IoT), Big Data, Analyse-Tools … Diese Lösungen bringen einen Komplexitätsgrad mit sich, der es erforderlich macht, das Thema Sicherheit ganz neu zu betrachten.

Zunehmende Nutzung vernetzter Geräte

Bis 2022 werden 97 Prozent der Pflegekräfte auf Station, 98 Prozent der Ärzteschaft, 96 Prozent der Apotheker und 94 Prozent des Personals in der Notaufnahme mit mobilen Geräten arbeiten.[5] Die Organisationen des Gesundheitswesens, wie auch die Patienten, setzen also immer mehr auf mobile Technologie, das Internet der Dinge und smarte Gesundheitsgeräte für Zuhause wie Fitbits. Das öffnet neue Einfallstore für Cyberkriminelle.

Bis 2022 werden 97 % der Pflegekräfte auf Station, 98 % der Ärzteschaft, 96 % der Apotheker und 94 % des Personals in der Notaufnahme mobile Geräte nutzen.

Bei der ersten Generation vernetzter medizinischer Geräte gab es beispielsweise nicht einmal eine Passwortabfrage. Da diese Geräte mit dem Netzwerk verbunden waren, gelang es Hackern, sich darüber Zugang zum gesamten Netzwerk zu verschaffen. Heute gibt es Vorschriften der FDA und europäischer Aufsichtsbehörden, die bestimmte Sicherheitsfunktionen zur Pflicht machen, u. a. hartcodierte Passwörter. Dennoch

5 https://www.aiin.healthcare/topics/connected-care/over-90-nurses-physicians-will-use-mobile-devices-2022

finden Angriffe unvermeidlich statt und ein derartiger unerlaubter Zugriff auf das gesamte Netzwerke ist nach wie vor nicht ausgeschlossen. Untersuchungen der IDC zeigen, dass nur 6 Prozent der europäischen Gesundheitsdienstleister über eine Strategie zum Umgang mit vernetzten medizinischen Geräten verfügen, die auf die Sicherheitsarchitektur ihres Unternehmens abgestimmt ist. Weiterhin haben erst 16 Prozent, beunruhigend wenige also, damit begonnen, sich mit den potenziellen Risiken vernetzter Geräte, die mit dem Netzwerk verbunden sind, auseinanderzusetzen.[6] Auf der fünften eHealth-Sicherheitskonferenz der Agentur der Europäischen Union für Cybersicherheit (ENISA) wurde berichtet, dass die Zahl der Angriffe auf IoT-Geräte, insbesondere medizinische Geräte, um geschätzte 600 Prozent gestiegen sei.[7]

Nur 6 % der europäischen Gesundheitsdienstleister verfügen über eine Sicherheitsstrategie für vernetzte medizinische Geräte.

Räumliche Entgrenzung

Die meisten Organisationen haben lange Zeit klar zwischen Nutzern und Ressourcen inner- und außerhalb des Netzwerks unterschieden.

Im Zuge der digitalen Transformation jedoch zeigen sich diese Organisationen nun offener für den Austausch mit einem weiter gefassten Ökosystem, zu dem auch Patienten, Partner, Kostenübernahmestellen, Krankenkassen und weitere Dienstleister im Rahmen einer integrierten Gesundheitsversorgung gehören. Die Nutzer greifen nicht mehr nur innerhalb der räumlichen Grenzen des Netzwerks auf Ressourcen zu. Sie können sich überall befinden. Chirurgen tauschen eventuell Informationen mit den Ärzten auf der Station über ein ganz anderes Netzwerk aus. Krankenhäuser betreuen Patienten nach deren Entlassung aus der Ferne weiter. Ärzte greifen auf Daten zu, die in den persönlichen Gesundheitsgeräten der Patienten gespeichert sind, um die Diagnose und Behandlung zu optimieren.

Auch die IT-Ressourcen befinden sich nicht mehr ausschließlich vor Ort. Sie sind zum Teil räumlich am Standort vorhanden, aber zum Teil auch in eine Cloud ausgelagert oder über APIs vernetzt. Organisationen im Gesundheitswesens benötigen moderne Ansätze zum Schutz der Ressourcen, wenn es keine räumlich klaren Grenzen mehr gibt.

Rasantes Tempo

In einer digitalisierten Welt geschieht alles atemberaubend schnell. Sicherheitstools müssen mit dieser Geschwindigkeit mithalten können.

6 IoT Security in European Healthcare https://www.idc.com/getdoc.jsp?containerId=EUR145549919

7 https://www.enisa.europa.eu/events/5th-ehealth-security-conference

Broschüre
Cybersecurity im Gesundheitswesen in Zeiten der digitalen Transformation

Interview mit Silvia Piai, Research Director bei IDC Health Insight

Alcatel-Lucent Enterprise hatte Gelegenheit zu einem Interview mit Silvia Piai, Research Director bei IDC Health Insights, und erfuhr, wie IDC das Thema der Cybersicherheit im Gesundheitssektor einschätzt und was IDC diesbezüglich empfiehlt.

IDC ANALYZE THE FUTURE

Empfehlungen der IDC für mehr Cybersicherheit im Gesundheitswesen

Trotz der neuen Herausforderungen, die sich klar abzeichnen, hält das Gesundheitswesen beim Thema Sicherheit bisher an konservativen Ansätzen fest. Organisationen im Gesundheitssektor implementieren Sicherheit häufig in der Form, dass zu Compliance-Zwecken Häkchen gesetzt werden müssen. Es wird dabei nicht bedacht, dass mit der digitalen Transformation ein Wandel einhergeht, der auch die Anforderungen an die Sicherheit betrifft.

IDC empfiehlt, Netzwerksicherheit als ganzheitliche Aufgabe zu betrachten: Dazu gehören eine Strategie ebenso wie Technologie, Menschen (Schulungen) und Prozesse (wie wird zum Beispiel die Sicherheit in die Workflows integriert). Im vorliegenden Dokument legen wir den Schwerpunkt auf die Aspekte Strategie und Technologie.

Strategie

Organisationen des Gesundheitswesens sollten nicht nur ein Minimum an Cybersicherheit umsetzen – gerade ausreichend, um gesetzliche Vorschriften zu erfüllen –, sondern die Gelegenheit nutzen, einen Strategieplan für mehr Sicherheit zu entwickeln, der den Umgang mit Risiken so gestaltet, wie es im heutigen Kontext der digitalen Transformation angemessen ist. Folgendes empfiehlt sich bzw. sollte beachtet werden:

- **Vorschriftenkonformität als Ausgangspunkt.** Vielfach liegt das Augenmerk nur darauf, das Nötigste zu tun, damit die DSGVO, oder eine gleichwertige Vorschrift im außereuropäischen Ausland, erfüllt ist. Stattdessen sollte der Gesundheitssektor diese Konformität als Ausgangspunkt betrachten, und davon ausgehend neu überlegen, wie Daten in den Organisationen und im Austausch mit Partnern künftig verwaltet und gepflegt werden.
- **Mehr Sicherheit bedeutet einen höheren Geschäftswert** durch garantierte Geschäftskontinuität. Organisationen des Gesundheitswesens haben ein Interesse daran, Einnahmeverluste zu vermeiden (und Risiken für die Patientensicherheit zu verringern), die entstehen, wenn IT-Systeme durch Cyberangriffe ausfallen. Stimmen Sie die Sicherheit Ihrer Systeme auf die übergeordneten Unternehmensziele ab und integrieren Sie sie in Ihr tägliches Betriebsgeschehen.
- **Grundsatz der konzeptionsintegrierten Sicherheit:** Betriebliche Workflows haben Risiken, und diese verändern sich ständig, genauso wie die Technologie. Die Organisationen des Gesundheitswesens sollten ihre Arbeitsabläufe direkt von Anfang an unter

dem Aspekt der Sicherheit gestalten. Die Sicherheit ist ein zentraler Geschäftswert und ist bei jeder geschäftlichen Entscheidung mit zu bedenken.

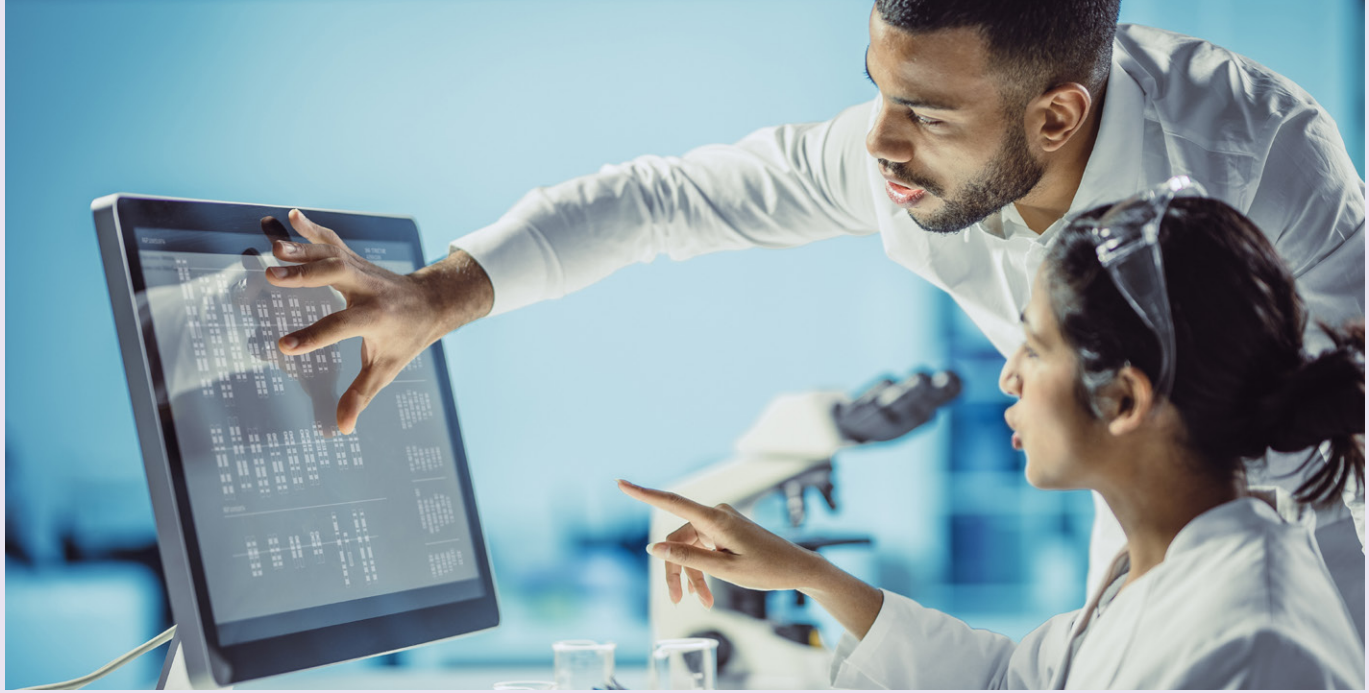
- **Mit dem Ökosystem arbeiten.** Organisationen im Gesundheitssektor haben in der Regel nicht mehr einen räumlich klar abgegrenzten Bereich, den es zu schützen gilt: Die medizinische Versorgung erfolgt zunehmend integriert mit anderen Organisationen und Partnern. Beim Thema Cybersicherheit sollte daher auf Ebene dieses Ökosystems angesetzt werden.

Technologie

Die Organisationen des Gesundheitswesens digitalisieren ihre Abläufe: Daher muss ein sicheres, vernetztes Ökosystem oberste Priorität haben. Ein solches Ökosystem braucht einen mehrschichtigen Ansatz. Es kommt darauf an, die vier Kerndisziplinen im Bereich der Sicherheit – Identitätsmanagement, Schwachstellen-Management, Bedrohungsmanagement und Vertrauensmanagement – neu zu definieren, damit eine Skalierbarkeit, Schnelligkeit, Intelligenz und Automatisierung von ganz neuer Dimension möglich wird. Dieser Ansatz sollte auf die digitale Umgebung des Unternehmens im weiteren Sinne und die Unternehmensziele abgestimmt sein, die erreicht werden sollen.

Bei einer mehrschichtigen Technologie für die Netzwerksicherheit sind einige Kernaspekte zu beachten:

- **Endpunkt-Sicherheit** – Eindämmung der Sicherheitsrisiken, die durch und für die einzelnen Geräte bestehen.
- **Identitätsmanagement** – Authentifizierung der Nutzer und Zugriffskontrolle. Die Lösung sollte eine Nutzerauthentifizierung bieten und auf einem detailliert aufgeschlüsselten Sicherheitskonzept



beruhen, damit die Nutzer jeweils genau in dem Umfang Zugriff erhalten, wie es notwendig ist, aber nicht mehr.

- **Sicherer Datenaustausch** – Über Verschlüsselung und sichere Datenaustauschprotokolle ist zu gewährleisten, dass die Daten auch während des Transfers sicher sind.
- **Containment-Technologie** – Um zu verhindern, dass eine Bedrohung, die es ins Netzwerk geschafft hat, ein System nach dem anderen lahmlegt, sollte die Lösung in der Lage sein, über Containment-Technologie und Segmentierung des Netzwerks die einzelnen Systeme zu isolieren.
- **Vertrauensmanagement** – Das Risikomanagement in Organisationen des Gesundheitswesens muss der Tatsache Rechnung tragen, dass Nutzer und Ressourcen sich auch außerhalb des räumlich eingegrenzten Netzwerks befinden können. Ist einmal klar, was im Netzwerk normales und abweichendes Verhalten darstellt, ist ein wesentlicher Grundstein dafür gelegt, dass eine solche Umgebung vertrauenswürdig ist. Über Tools für das Identitäts- und Autorisierungsmanagement, die mit künstlicher Intelligenz (KI) arbeiten, können Sie bestimmen, welches Verhalten im Netzwerk als normal gelten soll. Dabei evaluieren diese Tools jeden Nutzer und jedes Gerät und die Anforderungen, die in Bezug auf die Anwendung, Sicherheit und den Quality of Service bestehen, und leiten daraus ein Szenario normalen Verhaltens ab. Anschließend erkennt die KI ungewöhnliche Vorfälle oder Aktionen umgehend, etwa wenn ein Überwachungssystem auf elektronische Gesundheitsakten zugreift. Gestützt auf Analysetools wird dann ermittelt, warum eine Anomalie aufgetreten ist.
- **Eine softwaredefinierte Architektur** – Eine automatisierte Lösung für Netzwerkmanagement ist schnell genug, um mit der digitalen Transformation Schritt zu halten.

Die Lösung von Alcatel-Lucent Enterprise

Digital Age Networking im Gesundheitswesen von Alcatel-Lucent Enterprise ist ein ganzheitlicher Ansatz für die Cybersicherheit im Gesundheitssektor und bietet als mehrschichtiges Konzept eine umfassende Sicherheit für vernetzte medizinische Geräte und Anwendungen.

Flexible Konnektivität durch ein über Dienste definiertes Netzwerk

Das Fundament unseres Ansatzes ist ein flexibles, dienstedefiniertes Netzwerk, in dem es schnell und einfach möglich ist, verbindliche Regeln für das Netzwerk und die Cybersicherheit zu konfigurieren, die für die hohe Anzahl vernetzter Nutzer, Geräte und Anwendungen gelten sollen, die alle Bestandteil der digitalen Transformation sind.

Früher war die IT vorrangig dafür da, die Hard- und Software im Betrieb am Laufen zu halten. Die IT installierte neue Geräte, setzte sie in Betrieb und verwaltete das Netzwerk, nicht selten in mühevoller Handarbeit. DAN hingegen ist ein smartes, automatisiertes Netzwerk, mit dem es ein Leichtes ist, Nutzer und Geräte sicher mit den jeweils benötigten Anwendungen zu verbinden. DAN basiert auf der iFab-Technologie (Intelligent Fabric) von Alcatel-Lucent Enterprise. Unsere eigene Intelligent Fabric ist dabei mit marktüblicher SPB-Technologie (Shortest Path Bridging) kombiniert. Nicht nur ist es dadurch einfacher möglich, Netzwerke aufzubauen und zu konfigurieren, sondern die Lösung unterstützt auch Multipath Routing und Link Aggregation, so dass der Aufbau mehrerer Netzwerkverbindungen parallel möglich ist. Das erhöht den Durchsatz und bietet die notwendige Redundanz.

Bei unserem Ansatz ist es Aufgabe der IT, Netzwerkdienste, die Architektur, Zugriffsregeln und Container festzulegen. Das Netzwerk selbst baut sich dann automatisch auf. Steht die Architektur des Netzwerks, nimmt das Netzwerk bei jedem Element, das verschoben, geändert oder hinzugefügt wird, automatisch und unbemerkt die notwendigen Anpassungen vor. Wenn zum Beispiel ein Switch ausfällt, umgeht das Netzwerk diesen automatisch.

Ein über Dienste definiertes Netzwerk bietet Organisationen des Gesundheitswesens den Vorteil der Automatisierung: Das System ist weniger störanfällig, weil kaum noch etwas manuell konfiguriert werden muss, und es ist in der Lage, mit der rasanten Geschwindigkeit mitzuhalten, in der sich die Organisationen weiterentwickeln. Da die IT ihre Zeit dank der Automatisierung nicht mehr dafür aufwenden muss, Abläufe manuell zu regeln, kann sie wertschöpfend für das Unternehmen tätig werden.

Umfassende Zugriffskontrolle durch ein intelligentes, automatisiertes Berechtigungskonzept

Mit DAN sind Organisationen des Gesundheitswesens in der Lage, Regeln und Konzepte festzulegen, über die gesteuert wird, welche Zugriffs- und Nutzungsrechte für Anwendungen und Geräte gelten – und sie haben die Nutzer dabei überall im Blick. Zum Beispiel können folgende Regeln festgelegt werden:

- Ärzte erhalten Zugriff auf alle Systeme, mit Ausnahme von Finanzsoftware
- Patienten erhalten Zugang zu Internetdiensten
- Für Unternehmen aus dem Life-Sciences-Sektor oder andere Partner gilt ein vertraglich vereinbartes Konzept

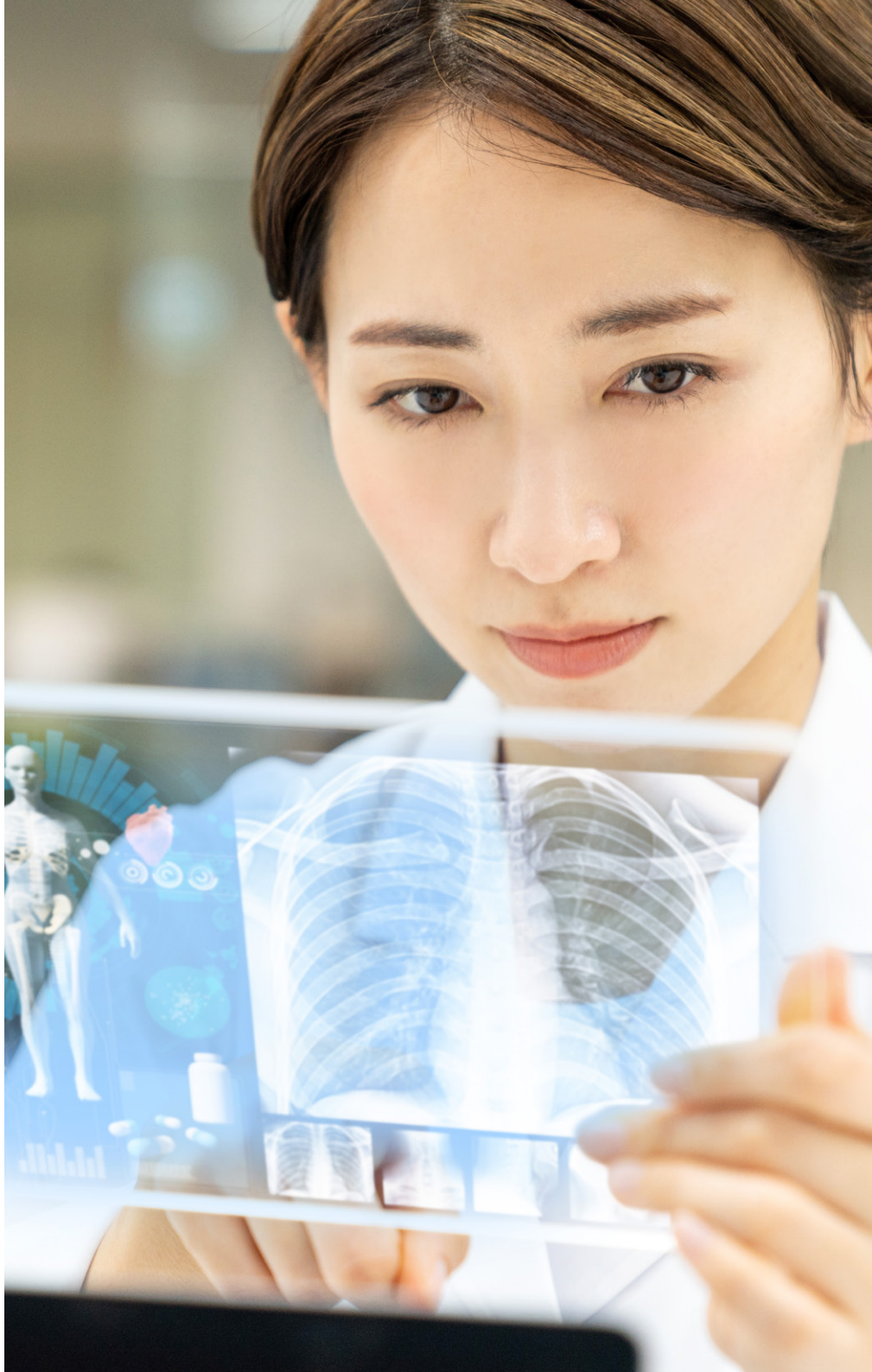
Alcatel-Lucent Enterprise bietet außerdem standortbasierte Dienste, etwa zur Orientierung in Gebäuden oder das Tracking von Ausrüstung und Personen. Das macht Nutzungsregeln möglich, die den Standort der Nutzer mit einbeziehen.

Die Möglichkeit des Unified Policy Managements bedeutet, dass Nutzungsregeln automatisch durchgesetzt werden, sobald ein Nutzer sich einloggt. So ist sichergestellt, dass Nutzer nur die Zugriffsberechtigung haben, die ihnen zugeteilt wurde. Haben sich Nutzer einmal durch den Login am PC, Laptop oder mobilen Gerät legitimiert, ist keine weitere Authentifizierung erforderlich. Solange das Gerät eingeschaltet ist, bleiben die Nutzer eingeloggt und das System achtet darauf, dass das geltende Berechtigungskonzept Anwendung findet.

Es ist auf diese Weise gewährleistet, dass alle Nutzer, ob extern oder intern, nur zu zulässigen Bereichen Zugang haben und die Zugriffskontrolle konsequent umgesetzt wird. Das vereinfacht die Abläufe in der Klinik und stärkt gleichzeitig die Cybersicherheit. Mediziner haben die Möglichkeit, schnell auf Systeme und Daten zuzugreifen, die sie benötigen, um ihre Patienten optimal zu versorgen, und werden nicht durch zeitaufwendige Anmeldeprozesse aufgehalten.

Geringere Sicherheitsrisiken durch Containment-Technologie und Segmentierung

In Organisationen des Gesundheitswesens kommen viele IoT-Geräte zum Einsatz, etwa MRT-Geräte, Patientenmonitore, Infusionspumpen, automatisierte Dosiersysteme für verschreibungspflichtige Medikamente, aber auch Kameras, HLK-Systeme, Sprinkleranlagen, Systeme zur Angriffserkennung usw. Die DAN-Lösung bietet die Möglichkeit, Geräte voneinander zu isolieren. Dazu wird ein virtuelles Netzwerksegment aufgebaut, das verhindert,



das ein Gerät zum Angriffsvektor wird. Containment-Technologie oder auch Containerisierung bedeutet bei DAN, dass aus einem einzigen physischen Netzwerk mehrere virtuelle Netzwerke gebildet werden, die über ein einziges Managementsystem verwaltet werden.

Containerisierung stellt die IT bei der Umsetzung vor keinerlei Schwierigkeiten. Die DAN-Lösung erkennt automatisch jedes einzelne Gerät im Netzwerk. Wird ein Gerät mit dem Netzwerk verbunden, versucht das Alcatel-Lucent OmniVista® 2500 Network Management System, das entweder vor Ort oder in der Cloud betrieben wird, dieses Gerät zu identifizieren. Ist das Gerät nicht in der Datenbank des Systems verzeichnet, wird eine cloudbasierte Datenbank, die über 17 Millionen Geräte enthält, abgefragt.

Ist das Gerät erkannt, wird es vom System einer Kategorie zugeordnet, etwa als Sicherheitskamera. Steht das Gerät auf der Freigabeliste für Lieferanten von Sicherheitskameras, wird es mit dem Netzwerk verbunden. Falls nicht, wird die Verbindung verweigert. Anschließend wird ein virtueller Container für das Gerät eingerichtet, damit es vom Rest des Netzwerks segmentiert ist. Wird ein mit dem Netzwerk verbundenes Gerät Opfer eines Hackerangriffs, gelingt es dem Angreifer nicht, über das Gerät weiter ins Netzwerk vorzudringen.

Künstliche Intelligenz als vertrauensbildender Faktor

Sind Geräte mit dem Netzwerk verbunden, müssen sie kontinuierlich überwacht werden, damit Gefahren rechtzeitig erkannt werden und das Vertrauen in die Arbeitsumgebung erhalten bleibt. Über die Funktionalität, die wir im Bereich der Analyse und Sichtbarkeit bieten, haben Netzwerkadministratoren für jedes einzelne Gerät stets im Blick, was im Netzwerk passiert. Die Analyse-Werkzeuge erkennen, welche Muster ein normales, erwartetes Verhalten im Netzwerk darstellen, aber auch Abweichungen. Es kann auch das Verhalten von Anwendungen am Rand des Netzwerks betrachtet werden, um dann zu entscheiden, ob eine Verbindung zu dieser Anwendung zugelassen wird. Auch ungewöhnliches Verhalten von Anwendungen, die bereits im Netzwerk sind, fällt auf, zum Beispiel, wenn eine Kamera mehr Daten generiert als erwartet.

Zeigt ein Gerät ein ungewöhnliches Verhalten, ist das über die Analyse-Werkzeuge zu sehen. Dann kann der für das Netzwerk zuständige Sicherheitsmanager eingreifen. Bisher erfolgt die Untersuchung eines Vorfalls noch manuell, ALE arbeitet jedoch daran, die Reaktion mittels KI und ML zu automatisieren.

Auch Remote-Dienste für Patienten werden durch KI unterstützt. Wir entwickeln Geräte, durch die es Krankenhäusern möglich wird, Patienten aus der Ferne zu betreuen, während diese sich zu Hause von einer Krankheit oder einer OP erholen. Bei diesen Geräten muss

gewährleistet sein, dass die Übertragung der Daten vom Gerät ins Krankenhaus sicher ist. Zur Überwachung der Aktivität von IoT-Geräten lässt sich KI einsetzen, um das tatsächliche mit dem erwarteten Verhalten abzugleichen. Auch Patienten nutzen in immer größerer Zahl Apps, um ihren Gesundheitszustand zu überwachen. Hat ein Kliniker Zugriff auf eine Apple Watch® oder andere derartige Geräte, die ein Patient trägt, kann er den Patienten in seinen gesundheitlichen Zielen unterstützen und genauere Diagnosen stellen. Mit der KI-Funktionalität, wird für Organisationen im Gesundheitssektor ersichtlich, ob eine Anwendung oder Aktivität im Netzwerk vertrauenswürdig ist.

Sicheres Netzwerk-Equipment senkt Sicherheitsrisiken

Organisationen des Gesundheitswesens wissen inzwischen, wie wichtig es ist, IoT-Geräte im Netzwerk zu schützen. Der Unterbau eines Netzwerks jedoch, u. a. Switches und Access Points, geraten schnell aus dem Blick.

Alcatel-Lucent Enterprise setzt verschiedene Technologien ein, damit von diesen Komponenten weniger Gefahr ausgeht. Unsere Lösungen:

- Stärkung der OS-Software, damit der Programmiercode sicher und diversifiziert ist.
- Prüfung und Validierung der OS-Software durch Dritte, damit sichergestellt ist, dass es keine verletzlichen Zugangspunkte oder Hintertüren gibt.
- Immer wenn ein Switch bootet, wird der Speicher unterschiedlich kompiliert und bereitgestellt. Zwar funktionieren alle Switches gleich, die interne Speicherkonfiguration unterscheidet sich jedoch von Gerät zu Gerät. Würde ein Switch gehackt, gelänge der Angriff auf diese Weise bei keinem zweiten Switch.
- Schutz durch integrierten Denial of Service (DoS). Unsere CPU erkennt ein ungewöhnliches Aufkommen beim Datenverkehr im Netzwerk und schaltet sich ggf. automatisch ab.
- Vollständige Sicherheitszertifizierungen nach verschiedenen Standards, u. a. JDIC und FIPS.
- Kontinuierliche Software-Upgrades.

Sichere Verbindungen für ein- und ausgehenden Datenverkehr

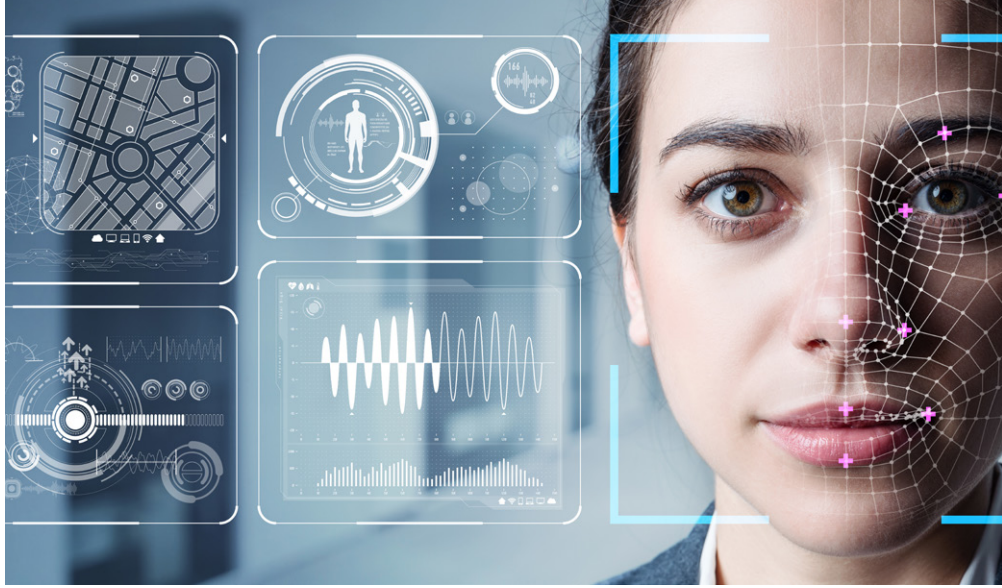
Für eingehenden Datenverkehr bieten unsere VPN-Funktionalitäten eine verschlüsselte Verbindung zum lokalen Netzwerk. Ende-zu-Ende-Verkehr wird über MACsec (auch als IEEE 802.1AE bekannt) verschlüsselt, damit die Daten geschützt sind, wenn sie das Netzwerk durchqueren. Durch die Möglichkeit, Dienste ohne Reboot erneut zu laden, etwa TLS und HTTPS, läuft das Netzwerk unterbrechungsfrei.

Reporting

Über das Reporting, das ALE bietet, haben verschiedene Stellen im Unternehmen Zugriff auf Daten, die Aufschluss über den Status, die Stabilität und die Leistung des Netzwerks geben und anzeigen, wie die Anwendungen laufen. Auch die Benutzerzufriedenheit kann abgefragt werden. Die IT sieht jederzeit die Daten zur Netzwerkleistung und zum Betrieb im Netzwerk. Geschäftsbereiche können über das Reporting feststellen, ob ihre Geräte, zum Beispiel bildgebende Systeme (MRT, Röntgengeräte), die Daten störungsfrei an Server und Tablets übertragen. Die Führungsetage kann prüfen, ob das Netzwerk die Dienste bereitstellt, die es Klinikern ermöglichen, sich ohne unnötige Zeitverluste ganz den Patienten zu widmen, und ob das Netzwerk als Ressource optimal ausgeschöpft wird.

Fazit

Immer mehr vernetzte Geräte, räumliche Entgrenzung, Veränderungen, die sich immer schneller vollziehen: Im Zuge der digitalen Transformation haben sich die Anforderungen an die Cybersicherheit in Krankenhäusern fundamental gewandelt. Die Lösung Digital Age Networking im Gesundheitswesen von Alcatel-Lucent Enterprise sorgt für die Sicherheit Ihrer IT-Infrastruktur und der Patientendaten, auch und gerade in Zeiten der digitalen Transformation. Mit der DAN-Lösung haben Sie die Kontrolle über alle Zugriffe Ihrer Nutzer, sind geringeren Sicherheitsrisiken im Zusammenhang mit der Nutzung von IoT-, mobilen und Netzwerkgeräten ausgesetzt, verhindern ein Eindringen über ein Gerät als Angriffsvektor und können im Netzwerk Ihres Ökosystems vertrauensvoll kommunizieren.



Wir sind Alcatel-Lucent Enterprise.
Wir sind ALE. Wir unterstützen Sie dabei, Ihre Patienten, Mitarbeiter und Gesundheitsökosysteme sicher zu vernetzen. Wir liefern Technologien, die echten Nutzen bringen, im gesamten Gesundheitsbereich und darüber hinaus.
www.al-enterprise.com/de-de/industries/healthcare

Alcatel·Lucent
Enterprise