MEINUNGEN

WERDEN KRANKENHÄUSER JEMALS VON DER CYBERBEDROHUNG VERSCHONT BLEIBEN?

Victor Poitevin
Editorial & Digital Manager, Stormshield

Das Volumen der Sicherheitsvorfälle in Gesundheitseinrichtungen ist zwischen 2020 und 2021 in die Höhe geschnellt: 35 % Anstieg in den USA, 45 % in Spanien und bis zu 50 % in Deutschland und Frankreich ... Eine kritische Situation, wenn diese sensiblen Umgebungen im Durchschnitt 28 Tage benötigen, um wieder normal zu funktionieren. Warum sind Krankenhauszentren trotz der Hilfe und Unterstützung, die insbesondere von staatlicher Seite geleistet wird, auch heute noch anfällig?

Analyse und Reaktion von Experten zu einem Phänomen, das Gesundheitsfachkräfte und die breite Öffentlichkeit beunruhigt.

INITIATIVEN ZUR BEWÄLTIGUNG DER CYBERBEDROHUNG

Die Anfälligkeit von Gesundheitseinrichtungen wurde deutlich durch die Covid-19-Pandemie Anfang 2020. Krankenhauszentren werden dann fast täglich von Cyberangriffen getroffen und lahmgelegt, unabhängig von ihrer Größe oder ihrem geografischen Standort. Die französische Liste scheint endlos zu sein: die Krankenhäuser von Paris im März 2020, Dax, Oloron-Sainte-Marie und Villefranche-sur-Saône im Februar 2021, Arles im August 2021, die GHT Coeur Grand-Est im April 2022 oder Corbeil-Essonnes erst kürzlich im August 2022.

Die Anfälligkeit von Gesundheitseinrichtungen ist jedoch nichts Neues und beschäftigt die Fachwelt schon seit über einem Jahrzehnt. Eine erste Initiative, um über die Cybersicherheit von Gesundheitseinrichtungen zu sprechen, entsteht in Frankreich bereits 2011 in der Stadt Le Mans. Mit dem Wunsch, sich zu treffen und auszutauschen, wird der erste nationale Kongress für die Sicherheit von Informationssystemen im Gesundheitswesen unter der Leitung von **Vincent Trely,** CISO des Universitätsklinikums von Le Mans, organisiert. Im Jahr 2013 wurde, ebenfalls in Frankreich, im Militärprogrammgesetz (Loi de programmation militaire, LPM) der Begriff der OIV (Operateurs d'importance vitale – Betreiber von lebenswichtigen Einrichtungen) verankert. Ein Akronym, das dann eine Reihe von Unternehmen und Organisationen kategorisiert, die für das Überleben der Nation unverzichtbar sind. Auch wenn die Liste nicht öffentlich bekannt gegeben wird, werden dann erste große Krankenhäuser aufgenommen. Im selben Jahr beginnt die American Association Hospital (AHA) mit der Veröffentlichung von Warnungen und Berichten über Cyberangriffe, die auf Gesundheitseinrichtungen in den USA abzielen. Einige Jahre später, im Juli 2016, wurde die NIS-Richtlinie (*Network and Information Security*) auf europäischer Ebene verabschiedet. Sie sieht insbesondere eine Verschärfung der Cybersicherheit von Betreibern aus Schlüsselsektoren vor, und zwar durch die Schaffung des Begriffs der OSE (opérateurs de services essentiels – Betreiber von Grundversorgungsdiensten), ein weiteres Akronym, das die OIV ergänzt. Im Jahr 2017 ermöglicht die Neugestaltung der Groupements de Coopération Sanitaire (GCS) der französischen Gesundheitseinrichtungen, den Austausch zwischen den CISOs der Gesundheitsgruppierungen zu erleichtern und auszubauen.

Das Bewusstsein scheint also relativ ausgeprägt zu sein, zumindest auf der Ebene der Fachleute im Gesundheitssektor (wie z. B. CSSOs oder auch ANSSI). **Genug, um einen gewissen Schutz vor Cyberbedrohungen zu gewährleisten?** Leider wurde dieser Optimismus durch die Gesundheitskrise und die Explosion der Fälle von Cyberangriffen getrübt. Laut dem US-amerikanischen Analysten **Brett Callow** infizierten fast 170 Ransomware-Angriffe fast 1.800 Kliniken und Gesundheitseinrichtungen in den USA im Zeitraum 2020-2021. In Frankreich verzeichnete die ANSSI im Jahr 2021 durchschnittlich einen Vorfall pro Woche in einer Gesundheitseinrichtung und gab bekannt, dass im selben Zeitraum 27 Einrichtungen Opfer eines Cyberangriffs geworden waren. Ein trauriger Rekord.

Als Reaktion auf diese neuen Angriffe mobilisiert sich die Branche erneut. Ab Februar 2020 führen einige private Cybersicherheitsunternehmen kostenlose Unterstützungsmaßnahmen für Gesundheitseinrichtungen durch. Parallel dazu veröffentlicht die ENISA einen Leitfaden mit zehn bewährten Verfahren, die in Gesundheitseinrichtungen zur Abwehr von Cyberbedrohungen umgesetzt werden sollten. Im März 2020 schlossen sich dann über 3.000 Fachleute für Internetsicherheit unter dem Namen COVID-19 Cyber Threat Coalition zusammen, um sich über Analysen und Indikatoren für Kompromittierungen auszutauschen. Threat Intelligence Feeds werden dann auf freiwilliger Basis erstellt und über die Community geteilt. Im September 2020 dann stellt der französische Staat mit dem Plan France Relance einen Fonds in Höhe von 136 Millionen Euro bereit, dessen Cybersicherheitskomponente darauf abzielt, die Sicherheit kritischer Infrastrukturen wie die von Gesundheitseinrichtungen zu erhöhen. Einige Monate später erhöht das Gesundheitsministerium dieses Budget um 350 Millionen Euro für die Krankenhäuser. Im April und Juni 2021 veröffentlicht der deutsche Staat eine Verordnung, die darauf abzielt, Dienstleister, die kritische Infrastrukturen nutzen, darunter auch Krankenhäuser, zu einer strengeren Cybersicherheit zu verpflichten, während die französischen Behörden ihrerseits 135 Krankenhausgruppen in die Liste der Betreiber von Grundversorgungsdiensten (OSE) aufnehmen. Schließlich kündigt die französische Regierung im August 2022 ein zusätzliches Budget von 20 Millionen Euro für die ANSSI an, um die Betreuung von Gesundheitseinrichtungen zu verstärken. Angesichts der Bedrohung durch das Internet sind Krankenhäuser also nicht auf sich allein gestellt. Aber ist das ausreichend?

WARUM SIND KRANKENHÄUSER IMMER NOCH VERWUNDBAR?

Angesichts solcher Mittel, Begleitungen und Initiativen bleiben die Gesundheitseinrichtungen verwundbar. Aber warum? In der Praxis **scheint der Hauptgrund einfach zu sein, da die Angriffsfläche für Krankenhäuser so groß ist**.

Die Erneuerung der Hardware in Umgebungen des Gesundheitswesens führt zu ersten Einschränkungen. Während eine herkömmliche IT-Ausrüstung alle fünf Jahre erneuert wird, haben medizinische Geräte Rentabilitätsmodelle von bis zu fünfzehn Betriebsjahren. Infolgedessen enthalten die Systeme heute Technologien, die am Ende ihres Lebenszyklus stehen und nicht mehr gewartet werden. **Charles Blanc-Rolin**, ehemaliger CISO einer Gesundheitseinrichtung und Projektleiter für digitale Sicherheit im Gesundheitswesen beim GCS e-santé Pays de la Loire, erklärt: „*Diese Investitionen in Höhe von mehreren zehn- oder hunderttausend Euro werden über zehn oder fünfzehn Jahre getätigt. Es ist nicht ungewöhnlich, Windows-Systeme oder Windows XP zu finden, das seit 2014 nicht mehr unterstützt wird. Manchmal sogar mit noch älteren Versionen von Windows, für die es keine Sicherheits-Patches mehr gibt. Es gibt echte Schlupflöcher und sehr anfällige Systeme. Hinzu kommt die CE-Kennzeichnung, die für den Hersteller vorschriftsmäßig ist. Aber es ist auch für die Gesundheitseinrichtung bindend, da sie keine Änderungen an diesem Gerät vornehmen kann, wie z. B. ein Update für einen Sicherheitspatch, ohne diese CE-Kennzeichnung zu verlieren.*“ Mit dem Ziel, das Risiko

der Verwendung von nicht gewarteten Betriebssystemen zu verhindern, müssen die IT-Sicherheitsrichtlinien stattdessen in der Lage sein, sich anzupassen, wie Charles Blanc-Rolin betont: *„es ist wichtig, einen Business Continuity Plan und einen Disaster Recovery Plan einzurichten, aber es ist auch entscheidend, abgestufte Verfahren zu haben. Heutzutage werden viele Sicherheitswerkzeuge eingesetzt, aber die Grundlagen und die notwendige Flexibilität werden vergessen.“*

„Es ist nicht ungewöhnlich, Windows-Systeme oder Windows XP zu finden, das seit 2014 nicht mehr unterstützt wird. Manchmal sogar mit noch älteren Versionen von Windows, für die es keine Sicherheits-Patches mehr gibt.”

Charles Blanc-Rolin, Projektleiter für digitale Sicherheit im Gesundheitswesen beim GCS e-santé Pays de la Loire

Parallel dazu werden **Krankenhäuser seit über einem Jahrzehnt einer forcierten Digitalisierung unterzogen**, die weitere Zwänge erzeugt. **Jean-Sylvain Chavanne,** CISO des Universitätskrankenhauses Brest und des Krankenhausverbands der Westbretagne, erläutert: *„Um ein Beispiel zu nennen: Der zu sichernde Perimeter für das Universitätsklinikum Brest besteht aus 140 Geschäftsanwendungen, 350 virtuellen Servern, 6000 Arbeitsplätzen, 10.000 an das Netzwerk angeschlossenen Objekten, 20.000 biomedizinischen Geräten (wie Spritzenpumpen, MRTs, Hyperbarkammern usw.), 2,7 Petabyte Rohdatenspeicher, die gesichert werden müssen. Es handelt sich also um einen sehr großen Umfang. Parallel dazu haben die Krankenhauszentren seit den 2010er-Jahren eine forcierte Digitalisierung erlebt, die durch eine Reihe von Projektausschreibungen finanziert wurde, ohne dass damit verbundene Budgets zur Aufrechterhaltung der Projekte zur Verfügung standen. Mechanisch haben die Krankenhäuser eine große technische Schuld, die sie nach und nach aufholen müssen.“* Im Zuge dieser Digitalisierung **wurden die Gesundheitseinrichtungen auch durch die Demokratisierung der vernetzten Produkte geschwächt**. Die Medizin und ihre Nutzung entwickeln sich ständig weiter, und die Bereiche der medizinischen Bildgebung, der häuslichen Krankenhausversorgung oder auch der Patientenidentifikation wurden durch diese Innovationen umgewälzt, wie Charles Blanc-Rolin in Erinnerung ruft: *„Mit neuen Nutzungsmöglichkeiten, wie dem Patiententracking mit RFID-Armbändern, kann man genau wissen, wo sich ein Patient innerhalb eines Krankenhauses befindet, um seinen Behandlungspfad zu verbessern. Sie müssen also ihren neuen digitalen Nutzungsmöglichkeiten einen Rahmen geben und eine Sicherheitsschicht hinzufügen, ohne technische Schulden zu verursachen.“* Aufgrund der Vielzahl dieser Objekte im Gesundheitswesen ist die unkontrollierte Ausweitung der

Angriffsfläche ein Problem, das Jean-Sylvain Chavanne anhand von drei Hauptrisiken analysiert: *„Das erste Risiko besteht darin, dass die vernetzten Objekte, die in einem Krankenhausinformationssystem eingesetzt werden, nicht beherrscht werden. Dies ist der Fall, wenn ein Anbieter sich ohne implementierte Sicherheitsmaßnahmen an das Netzwerk anschließt. Das zweite Risiko liegt in den vertraglichen Beziehungen. Ohne Verträge mit Subunternehmern oder Lieferanten werden keine Sicherheitsverpflichtungen verlangt, wie etwa die Aktualisierung der betreffenden Software. Und schließlich ist das dritte Risiko die eingebettete Software selbst, die eine echte „Black Box" darstellt. Wenn wir nicht wissen, was sie enthält, können wir die Sicherheit nicht beherrschen und Schwachstellen nicht patchen. Im Dezember letzten Jahres geschah dies mit Log4Shell, wo wir 200 Anbieter von medizinischen Geräten kontaktieren mussten, um herauszufinden, ob ihre Software es eingebettet hatte oder nicht."*

„Die Krankenhauszentren haben seit den 2010er-Jahren eine forcierte Digitalisierung erlebt, die durch eine Reihe von Projektausschreibungen finanziert wurde, ohne dass damit verbundene Budgets zur Aufrechterhaltung der Projekte zur Verfügung standen. Mechanisch haben die Krankenhäuser eine große technische Schuld, die sie nach und nach aufholen müssen."

Jean-Sylvain Chavanne, CISO des Universitätskrankenhauses von Brest

Aber auch der Mensch ist in Krankenhäusern ein Faktor, der zur Anfälligkeit führt. Da sie einem Personalmangel ausgesetzt sind, konzentrieren sich die IT-Teams auf das Ziel, Informationen schnell bereitzustellen. Manchmal auf die Gefahr hin, offensichtliche Sicherheitsregeln zu missachten. In diesem Rahmen sensibilisieren die ISS-Teams der Krankenhauszentren das Personal und kommen manchmal auf Freiheiten zurück, die das Gesundheitspersonal nicht hätte haben dürfen und die es zu dekonstruieren gilt, wie Jean-Sylvain Chavanne analysiert: *„Derzeit blockieren unsere Sicherheitseinrichtungen alle 50 Sekunden eine Spam-Mail und jede Stunde einen Virus. Wir müssen das Bewusstsein schärfen und darüber aufklären, dass wir keine volle Freiheit bei der Nutzung von Software haben, die Gesundheitsdaten speichert und verwaltet. Beispielsweise darf medizinisches Personal die Diagnosen ihrer Patienten nicht auf ihrem privaten Telefon haben. Wir erinnern das ganze Jahr über an gute Praktiken."* Medizinisches Personal, das unter ständigem Druck steht, das dazu neigt, Abkürzungen zu nehmen, um sich auf seine eigentliche Aufgabe, die Pflege, zu konzentrieren, und das für das Thema Cybersicherheit empfänglich gemacht werden muss. Eine echte Herausforderung für CISOs, die sich von der Mitteilung eines französischen Krankenhausdirektors an seine Mitarbeiter inspirieren lassen können.

Veraltete Geräte, eine noch zu perfektionierende Risikokultur, Probleme bei der Einstellung von Personal. Es gibt noch viele Punkte, die in Krankenhäusern geregelt werden müssen, um eine echte Cybersicherheit dieser lebenswichtigen Infrastrukturen zu gewährleisten.

AUF DEM WEG ZU EINER BREITEREN FRONT DER CYBERBEDROHUNG RUND UM GESUNDHEITSDATEN

Angesichts dieser verschiedenen Schwierigkeiten betont Charles Blanc-Rolin, dass **die entscheidende Herausforderung bei der Sicherheit von Gesundheitseinrichtungen die Patientendaten und die Behandlung der Patienten betrifft.** *„Insbesondere Cyberangriffe durch Ransomware können ein Krankenhaus lahmlegen und die Chancen auf eine Behandlung der Patienten verringern. Pflegekräfte, die keinen Zugang zu Daten oder Diagnosen haben, werden Kriegsmedizin betreiben müssen. Dies führt zu einer Verschlechterung der Qualität der Pflege. Darin liegt die eigentliche Gefahr."*

„Pflegekräfte, die keinen Zugang zu Daten oder Diagnosen haben, werden Kriegsmedizin betreiben müssen. Dies führt zu einer Verschlechterung der Qualität der Pflege. Darin liegt die eigentliche Gefahr."

Charles Blanc-Rolin, Projektleiter für digitale Sicherheit im Gesundheitswesen beim GCS e-santé Pays de la Loire

Doch Gesundheitsdaten haben parallel dazu noch ein anderes Interesse für Cyberkriminelle. Über den persönlichen und üblichen Charakter bestimmter Daten wie Name, Vorname und Geburtsdatum hinaus können diese Daten manchmal einen weitaus persönlicheren Aspekt enthalten, der zu Szenarien von Lösegeldforderungen führen kann, die für die Opfer selbst erschreckend sind. Genau das ist den Patienten der Firma Vastaamo im Laufe des Jahres 2020 passiert. Bei diesem Zusammenschluss von 25 Psychotherapiezentren in Finnland kam es zu einem Datenleck, das die psychiatrische Betreuung dieser Patienten enthielt. Wie VICE berichtete, hatten 30.000 Patienten eine Lösegeldforderung erhalten, die sie innerhalb von 24 Stunden begleichen mussten, da die Daten sonst an die Öffentlichkeit gelangten. Eine Entwicklung in der Methode von Cyberangriffen, bei denen das Lösegeld meist mit einem Unternehmen in Verbindung gebracht wird. In diesem Fall standen die Patienten jedoch an vorderster Front. Mehr als 25.000 Beschwerden wurden bei den Behörden eingereicht, was den Cyberangriff zum größten Kriminalfall in der Geschichte Finnlands macht. Einige Monate später verhängte die finnische Datenschutzbehörde eine Geldstrafe von 608.000 € gegen das Unternehmen, weil es gegen die Datenschutz-Grundverordnung verstoßen hatte. Auch Frankreich blieb nicht verschont, denn zur gleichen Zeit wurden 500.000 Krankenakten aus einer Gruppe von Laboren in Westfrankreich entwendet. Laut einer US-amerikanischen Studie vom März 2022 **hätten Gesundheitsdaten einen 25-mal höheren Wert als eine Kreditkarte**.

Wenn Gesundheitsdaten eine Geldquelle für Cyberkriminelle sind, können Daten aus der Welt des Gesundheitswesens ein Ziel staatlicher Mächte sein. Informationen über die Impfstoffentwicklung während der Gesundheitskrise zu erhalten, war daher für einige Länder, die nicht über Forschungs- und Entwicklungskapazitäten verfügten, eine Priorität. Laut dem Wall Street Journal sollen nicht weniger als sechs Pharmaunternehmen darunter Johnson & Johnson und Novavax Inc. zur gleichen Zeit von nordkoreanischen Cyberaktivisten ins Visier genommen worden sein. Ende 2020 soll dieselbe Gruppe, die sich als Personalvermittlungsfirma ausgab, mit gefälschten Stellenangeboten an Mitarbeiter des Unternehmens Astrazeneca herangetreten sein, um Dokumente mit Malware in das Unternehmen einzuschleusen. Im selben Jahr betrafen in Frankreich von 24 Vorfällen im Gesundheitssektor sieben die Pharmaindustrie, so **Charlotte Drapeau,** Leiterin des Büros Gesundheit und Gesellschaft bei der ANSSI. Laut *HIPAA Journal* ein Megatrend: Die Zahl der großen Sicherheitsverletzungen, bei denen es um den Diebstahl von Gesundheitsdaten geht, ist in den USA von 368 im Jahr 2018 auf 714 im Jahr 2021 gestiegen.

Für Jean-Sylvain Chavanne sind nicht alle Cyberangriffe auf französische Pharmaunternehmen das Werk von klassischen Cyberkriminellen: *„Alle französischen Pharmaunternehmen, die einen Impfstoff gegen Covid-19 entwickelt haben, sind Opfer eines Cyberangriffs geworden. Angesichts dieser Tatsache fällt es schwer, sich vorzustellen, dass es sich hierbei um das Ergebnis opportunistischer Aktionen der Angreifer handelt. Hier geht es um den Wunsch nach Destabilisierung oder Industriespionage."*

Die Gründe für die Anfälligkeit von Gesundheitseinrichtungen sind daher komplex. Da sie von strukturellen Problemen des Sektors herrühren, können sie sicherlich nicht innerhalb weniger Monate gelöst werden. Um technische Schulden zu tilgen, auf Personalmangel zu reagieren oder die Angriffsfläche zu verringern, muss der Gesundheitssektor jetzt handeln. Und dabei kann er auf die Unterstützung der Staaten zählen. Um das Krankenhaus (wieder) zu einem vernetzten und sicheren Raum zu machen.