Cybersicherheit in sensiblen Umgebungen: Eintauchen in die Welt des Gesundheits-wesens

WHITEPAPER



STORMSHIELD

Cyberkriminelle lassen sich durch nichts aufhalten. Angesichts der vitalen Bedeutung der medizinischen Versorgung schrecken sie nicht davor zurück, die durch die Gesundheitskrise deutlich gewordenen oder die durch die digitale Transformation des Bereichs entstandenen Schwachstellen auszunutzen. In Frankreich und im internationalen Umfeld sehen sich Krankenhäuser, Apotheken, Labore und andere Einrichtungen des Gesundheitswesens aufgrund einer großen Verwundbarkeit der IT unaufhörlich mit Cyberangriffen konfrontiert.

Im Gesundheitswesen verdoppelten sich die Meldungen von Vorfällen im Jahr 2021 im Vergleich zu 2020[1]. Wie lässt sich dieser beispiellose Anstieg erklären? Die Antworten sind so vielfältig wie die Schwachstellen der Einrichtungen und neuerdings kommt auch noch das neuartige Profil bestimmter Ziele hinzu. Tatsächlich sind diese Vorfälle mittlerweile auch bei Dienstleistern im Gesundheitssektor aufgetreten.

Sensible Daten, die im medizinischen Umfeld übertragen werden, stehen im Mittelpunkt des Interesses. Denn auch wenn sie für Cyberkriminelle zweifellos attraktiv sind, sorgt auch der Umgang mit ihnen für zahlreiche Debatten, insbesondere vor dem Hintergrund der derzeitigen Ausarbeitung eines europäischen Regelwerks.

Ziel dieses Whitepapers ist es daher, IT-Managern sowie dem gesamten Systemumfeld von Subunternehmern und Dienstleistern der Branche zu ermöglichen, in den neuesten Stand der Technik rund um das Thema Cybersicherheit der medizinischen Einrichtungen einzutauchen.

Daher möchten wir auf den folgenden Seiten die Probleme des Gesundheitssektors aufführen, Ihnen eine operative Bestandsaufnahme möglicher Lösungen bieten und einige Prognosen für die Zukunft der IT-Sicherheit in diesem Sektor aufstellen.

04 – Referenten

01. Cybersicherheit im Gesundheitswesen: Warum gibt es eine so hohe Anfälligkeit?

08 – *Infografik: Weltreise der Cyberangriffe auf Gesundheitseinrichtungen*
10 – Starke materielle Einschränkungen: eine IT-Umgebung der ganz besonderen Art
14 – Digitale Transformation im Gesundheitswesen: ein später Wandel, der beschleunigt werden muss
16 – Der besondere Fall von Gesundheitsdaten
17 – *Interview mit Charles Blanc-Rolin: Welche Verbindung besteht zwischen dem Zugang zu Daten, Gesundheit und Sicherheit?*

02. Anatomie einer polymorphen Bedrohung mit zahlreichen Eintrittspunkten

22 – Wie dringen Cyberkriminelle in die Informationssysteme von Gesundheitseinrichtungen ein?
26 – Den gesamten Behandlungspfad im Visier
28 – Dies ist kein Cyberangriff

03. Welche Mittel gibt es, um das Gesundheitswesen sicher zu machen?

32 – Welche Maßnahmen gibt es zum Schutz der medizinischen Infrastruktur?
37 – *Fokus: Welche regulatorischen Verpflichtungen haben medizinische Einrichtungen?*
38 – Ein Bewusstsein und Bemühungen, die durch öffentliche Maßnahmen unterstützt werden
40 – *Krezinterview: Ist die EU-Verordnung über die Verfügbarkeit der elektronischen Gesundheitsdaten den heutigen Herausforderungen gewachsen?*

04. Und in Zukunft?

46 – Pflegedauerzustand auf europäischer Ebene
48 – Präventivmedizin, datengestützte Steuerung des Krankenhauses: Versprechen (und Herausforderungen) von Big Data in der Medizin
50 – Eine Zusammenarbeit, die aufgebaut werden muss
52 – *Interview mit Jacky Grisey: Die Zukunft der Cybersicherheit im Gesundheitswesen*

Sprecher

CHARLES BLANC-ROLIN

PROJEKTLEITER DIGITALE SICHERHEIT
EHEALTH PAYS DE LA LOIRE

„Es ist mir bereits passiert, dass ich zusammen mit dem Leiter der Biomedizin Lösungen zur physischen Blockierung von USB-Anschlüssen umsetzte. So wird z. B. verhindert, dass jemand das Ultraschallgerät zum Aufladen seines Smartphones benutzt …“

SEITE 31

Welche Verbindung besteht zwischen dem Zugang zu Daten, Gesundheit und Sicherheit?

SEITE 17

JACQUES LABIDURIE

CISO UNIKLINIK LIMOGES

„Die Industrie muss in Cybersicherheit geschult werden, da viele noch immer Computertechnik wie vor 30 Jahren betreiben. Auch die IT-Sicherheit sollte in die medizinischen Lehrpläne aufgenommen werden und nicht nur der Datenschutz, wie es derzeit der Fall ist.“

SEITE 34

JACK GRISEY

SECURITY OPERATIONS MANAGER
FÜR SANTÉ ADVENS

„Die großen Cyberangriffe der letzten Jahre haben die technischen und organisatorischen Missstände der Informationssysteme in medizinischen Einrichtungen ans Licht gebracht. Es hat eine Bewusstseinsbildung stattgefunden, auch auf höchster staatlicher Ebene.“

SEITE 42

Die Zukunft des Gesundheitswesens in der Cybersicherheit

SEITE 52



CORALIE ACHARD-TORTUL

DPO UNIKLINIK LIMOGES

„Die Kontextualisierung ist bei unseren Aufklärungsmaßnahmen sehr wichtig. Ein vorheriges Treffen mit dem Abteilungsleiter erleichtert beispielsweise das Verständnis für die Funktionsweise der Abteilung und das Aufzeigen tatsächlicher Beispiele, wie z. B. die Tatsache, dass man seine Karte bei verschiedenen Funkmanipulationen an Ort und Stelle lässt.“

SEITE 35

JEAN-SYLVAIN CHAVANNE

CSO UNIKLINIKUM BREST

„Eine falsche Rechnung, eine trickreiche Aufforderung zur Erneuerung des Passworts, eine imaginäre Patientenbeschwerde … die Qualität der Phishing-Kampagnen, die wir abfangen, nimmt zu. Einige gehen sogar so weit, die Identität des Universitätsklinikums Brest anzunehmen.“

SEITE 23

Vernetzte medizinische Geräte im Scheinwerferlicht

SEITE 13

STÉPHANE PRÉVOST

PRODUCT MARKETING MANAGER STORMSHIELD

„Die Installation eines Patches für eine kritische Schwachstelle auf einer im Internet aktiven Komponente ist keine Garantie gegen einen Missbrauch wie in der Vergangenheit. Außerdem sollten die Protokolle auf Ausbeutung untersucht und im Zweifelsfall alle Konten erneuert werden.“

SEITE 34

RAYNA STAMBOLIYSKA

EXPERTIN FÜR DIGITALE DIPLOMATIE, SPEZIALISTIN FÜR CYBERSICHERHEIT UND UNABHÄNGIGES MITGLIED DER ENISA-ARBEITSGRUPPE ZU AUFKOMMENDEN UND ZUKÜNFTIGEN BEDROHUNGEN

„Die DSA- und DMA-Texte, die das Thema übergreifend und systemisch angehen, sind Teil einer Reihe verschiedener Dokumente, darunter die DSGVO, die NIS-Richtlinie oder der Data Act. Dadurch wird versucht, sowohl Innovationen als auch die Bürger Europas zu schützen und die strategische Autorität der Europäischen Union zu festigen.“

SEITE 37

Ist die EU-Verordnung über die Verfügbarkeit der elektronischen Gesundheitsdaten den heutigen Herausforderungen gewachsen?

SEITE 41

DAMIAN KLIMAS

DOTLAW-PARTNER UND BEOBACHTER
DES EHEALTH NETWORK

„Die Umsetzung der EHDS-Verordnung wird sich mit der Einführung von MaSanté@EU beschleunigen. Das bedeutet, dass es bis 2025 für die Gesundheitseinrichtungen aller Mitgliedsstaaten sowie Norwegens möglich sein wird, einfach und sicher auf Daten zu Allergien, Verschreibungen und der Krankengeschichte jedes Patienten in ihrer Sprache zuzugreifen, selbst wenn der Patient in einem anderen europäischen Land lebt.“

SEITE 47

Ist die EU-Verordnung über die Verfügbarkeit der elektronischen Gesundheitsdaten den heutigen Herausforderungen gewachsen?

SEITE 41



01.

Cybersicherheit im Gesundheitswesen: Warum gibt es eine so hohe Anfälligkeit?

Wie ist es zu erklären, dass Krankenhäuser, Kliniken, Apotheken und Labore so anfällig für Cyber-Risiken sind? Von der Architektur der Gesundheitsinformationssysteme über ihre Komponenten bis hin zu den neuen Nutzungsmöglichkeiten in der medizinischen Welt – die Gründe sind leider ebenso vielfältig wie unterschiedlich.

Rund um die Welt
gibt es Cyberangriffe auf
Einrichtungen der medizinischen Versorgung



Medizinisches Zentrum der Presbyterianer in Hollywood
2016 – USA

Baton Rouge General Hospitals, Jack Huston Memorial und Southwest Health[2]
2022 – USA

Healthcare Service Executive
2021 – IRLAND

Gesundheitssystem der Provinz Neufundland und Labrador[3]
2021 – KANADA

Boston Children's Hospital
2014 – USA

Ministerium für Gesundheit
2021 – BRASILIEN

Gesundheitsorganisationen
2020 – VEREINIGTES KÖNIGREICH

National Health Service
2017 – VEREINIGTES KÖNIGREICH

Krankenhauszentrum Issoudun
2019 – FRANKREICH

Großhändler einer Apotheke in Rouen
2020 – FRANKREICH

Universitätsklinikum der Ile-de-France AP-HP
2020 – FRANKREICH

Universitätsklinikum Sud Francilien de Corbeil Essonne
2022 – FRANKREICH

Französisches Versicherungssystem
2022 – FRANKREICH

Gesundheitssystem[4]
2022 – DÄNEMARK

Universitätsklinikum Düsseldorf (UKD)
2020 – DEUTSCHLAND

Lieferkette für Impfstoffe gegen Covid[5]
2020 – DEUTSCHLAND

Gesundheitszentren
2022 – SPANIEN

Krankenhausgruppe Life Healthcare
2020 – SÜDAFRIKA

Krankenhaus Osaka
2022 – JAPAN

Referenzwebsite, die dem Thema Gesundheit gewidmet ist
2019 – INDIEN

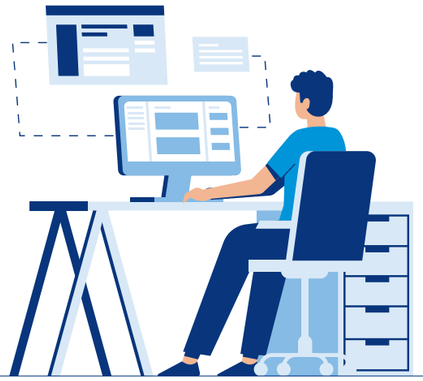
Gruppe von Gesundheitseinrichtungen SingHealth
2018 – SINGAPUR

Krankenhäuser in Dharmais und Harapan Kita
2017 – INDONESIEN

Australisches Versicherungsunternehmen
2022 – AUSTRALIEN

1.1 Starke materielle Einschränkungen: eine IT-Umgebung der ganz besonderen Art

Die IT-Infrastruktur ist ein kritischer Teil des Krankenhausbetriebs. Sie stellt eine direkte Schnittstelle von der Außenwelt zum internen operativen Netzwerk dar, und muss zudem mit den typischen Hard- und Software-Schwachstellen im Gesundheitssektor zurechtkommen.



OBSOLESZENZ, IT-OT-KONVERGENZ, DURCHLÄSSIGE NETZWERKE: GEMEINSAME SCHWACHSTELLEN

Wie auch andere Branchen, insbesondere die Industrie, ist auch der Gesundheitssektor anfällig für Software-Obsoleszenz. So ist es nicht ungewöhnlich, IT-Umgebungen in Gesundheitseinrichtungen mit Softwareanwendungen vorzufinden, die seit 20 Jahren nicht weiterentwickelt wurden. Aufgrund dieser langen Lebensdauer, die auf eine Abschreibung der medizinischen Geräte zurückzuführen ist, werden diese Systemversionen nicht gepflegt und sind veraltet wie z. B. Windows XP. Sie schwächen dann die Sicherheit dieser Umgebungen.

Diese Anfälligkeit wird durch die Durchlässigkeit der Netzwerke noch verstärkt, wie z. B. die Konvergenz der Informationssysteme in den Krankenhausverbänden (Groupements Hospitaliers de Territoire, GHT) in Frankreich. Ungesichert miteinander verbunden, erhöht sich nämlich das Risiko der Verbreitung von Cyberangriffen.

Schließlich stellt auch die Fernwartung, die in Krankenhäusern aufgrund der Fernzugriffe durch Hersteller von Medizinprodukten, Herausgeber oder Integratoren von Anwendungslösungen seit langem verbreitet ist, ein Risiko dar, da die Zugriffe unzureichend gesichert sind.

DIE SENSIBLE VERWALTUNG VON KRANKENHAUSGEBÄUDEN

Wenn man von Cybersicherheit spricht, denkt man sofort an die Welt der Informationssysteme. Heute ist es jedoch aufgrund der zunehmenden Verbindung von Computernetzwerken und operativen Netzwerken notwendig, das Thema breiter anzugehen.

So umfasst dies auch die technische Infrastruktur (zentrale technische Verwaltung [GTC], technische Gebäudeverwaltung [GTB]). Diese ermöglichen es, den Brandschutz, den Zugang, die Videoüberwachung, das Energiemanagement oder auch die Qualität der Innenraumluft in einem Krankenhausgebäude zu verwalten.

„Selbst wenn man sich auf das General Security Reference System (GSR)[6] stützt, ist es immer noch schwierig, die Großunternehmen der Biomedizin dazu zu bringen, die Mindestsicherheitsanforderungen beispielsweise für ihre Fernwartungsprotokolle umzusetzen. Oftmals ist die Erhöhung der Sicherheit auf dieser Ebene immer noch ein zähes Ringen.“

CHARLES BLANC-ROLIN – PROJEKTLEITER FÜR DIGITALE SICHERHEIT IM GESUNDHEITSWESEN BEIM GCS EHEALTH PAYS DE LA LOIRE

Diese verschiedenen Betriebssysteme, die aus Automaten heterogener Marken und Generationen bestehen, sind noch allzu oft ungesichert mit dem Computernetzwerk verbunden und bleiben oft unter dem Radar der Verantwortlichen für die Sicherheit der Informationssysteme. Ebenso wird die Telefoninfrastruktur der Gesundheitseinrichtung oft vernachlässigt. Wenn jedoch die IP-Telefone eines Krankenhauses durch einen DDoS-Angriff außer Betrieb gesetzt werden würden, hätte dies verheerende Folgen.

Diese Problematik wird dadurch noch komplexer, dass manchmal innerhalb derselben Struktur verschiedene Einrichtungen verwaltet werden, die über das ganze Land verstreut sind.

FLASHER

SZENARIO EINES CYBERANGRIFFS

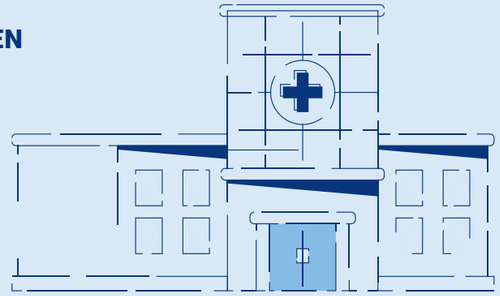
→ Erfahren Sie mehr zum konkreten Szenario eines Cyberangriffs auf die Brandschutzeinrichtungen eines Krankenhauses. –

ZU BEACHTEN

DIE LUFTQUALITÄT

ist in Patientenzimmern eine Frage des Komforts, aber im Operationssaal ist sie lebenswichtig.

DIE SENSIBLE VERWALTUNG VON KRANKENHAUSGEBÄUDEN



- Verbindungen zu anderen Notdiensten
- Integration des Systems
- Validierung des Systems
- Geschäfts- und Verwaltungssysteme
- Dienstleistungen für Patienten
- Energiemanagement
- Heizung, Lüftung und Klimaanlagen
- Schutz der Umgebung
- Strukturierung und Kabelmanagement
- Sprach- und Datenkommunikation
- IP-Konvergenz
- Dienstleistungen und Wartung
- Antennenfernsehen
- Video für öffentliche Informationen/Plakatwände
- Dienstleistungen für sehr niedrige Spannungen
- Beschallung und Sprachansagen
- Beleuchtung
- Branderkennung und -alarm
- Zugangskontrolle
- Verwaltung von Aufzügen und Rolltreppen
- Verwaltung der Lokalisierung von Patienten/Gütern / des klinischen Arbeitsablaufs
- Sicherheit/ Überwachungskameras und digitale Videoüberwachung

DER SCHUTZ BIOMEDIZINISCHER GERÄTE IM BLICKPUNKT DER ÖFFENTLICHKEIT

Die meisten biomedizinischen Geräte, die in der medizinischen Bildgebung oder in der Biologie eingesetzt werden, sind mit dem Informationssystem (SIEM) verbunden.

Das ermöglicht es zum Beispiel einigen Chirurgen, über eine angeschlossene Kamera live von einem Kollegen oder einer Kollegin am anderen Ende der Welt unterstützt zu werden.

Dieses Internet der medizinischen Dinge (IoMT) verbessert nicht nur den Komfort bei der Patientenversorgung, sondern hilft auch bei der Diagnose und verbessert die Zusammenarbeit zwischen den Angehörigen der Gesundheitsberufe. Es bietet im Fall der Telemedizin sogar eine Teilantwort auf das Problem der medizinischen Wüsten. Er stellt jedoch ein Sicherheitsrisiko für das Krankenhaus dar.

Diese Geräte, die selten gezielt ins Visier genommen werden, gehören oft zu den Kollateralschäden von Cyberangriffen. Ihre Schwäche: Sie sind mit dem Netzwerk verbunden, ohne die nötige Sicherheit zu haben ... Und das, obwohl sie in direktem Kontakt mit den Patienten stehen.

Sie werden von industriellen Herstellern mit begrenzter Cyberkultur entworfen und stellen oft potenzielle Brutstätten für Viren dar.

AKTUELLES

EIN HARTES PASSWORT

→ Im Oktober 2022 wurde eine Sicherheitslücke in einer medizinischen Laborausrüstung bekannt, die für Vorsorgeuntersuchungen auf Gebärmutterhalskrebs verwendet wird. Schuld daran sind hartkodierte Identifikationsdaten in der Ausrüstung.

20.000

„Gesundheitseinrichtungen kennen oft weder das Betriebssystem, auf dem diese häufig anfälligen und veralteten Geräte basieren, noch eingebettete Software und Bibliotheken. Unter diesen Umständen ist es schwierig, auf die Veröffentlichung von Schwachstellen zu reagieren.“

CHARLES BLANC-ROLIN – PROJEKTLEITER FÜR DIGITALE SICHERHEIT IM GESUNDHEITSWESEN BEIM GCS EHEALTH PAYS DE LA LOIRE

KENNZAHL

BIOMEDIZINISCHER GERÄTE

Dabei handelt es sich um die Anzahl der biomedizinischen Geräte, die über das gesamte Universitätsklinikum (CHU) Brest verteilt sind.

AKTUELLES

EIN ANGRIFF ZU VIEL

Nach dem Angriff auf das Centre Hospitalier Sud-Francilien[7] mit Sitz in Corbeil-Essonnes Ende August 2022 pumpte die Regierung 20 Millionen Euro in die ANSSI, um deren Unterstützung für Krankenhäuser zu verstärken.

EIN SEKTOR UNTER SPANNUNG

Die Cybersicherheit im Gesundheitswesen leidet auch unter dem allgemeinen Mangel an Mitteln in diesem Sektor. In den letzten Jahren wurden von der Regierung Finanzmittel bereitgestellt, die jedoch nur für Neuinvestitionen und nicht für Instandhaltung vorgesehen sind. Die IT-Sicherheit im Gesundheitswesen leidet auch unter einem Mangel an Ressourcen und engagierten Experten. –

„Zur Zeit konzentrieren wir unsere Personalressourcen im Bereich IT-Sicherheit auf den Projektteil: Wir haben keine operativen Ressourcen, obwohl wir im Februar eine Stellenanzeige geschaltet haben.“

JACQUES LABIDURIE – CISO UNIKLINIKUM LIMOGES

VERNETZTE MEDIZINISCHE GERÄTE IM SCHEINWERFERLICHT

MIT **JEAN-SYLVAIN CHAVANNE** – CISO AM UNIVERSITÄTSKLINIKUM BREST

→ Medizinischer CE-Kennzeichnung. Dieses Konformitätszeichen, das auf medizinischen Geräten angebracht wird, stellt eine große Sicherheitsherausforderung dar. Denn jede strukturelle Veränderung würde die Markierung in Frage stellen, was es unmöglich macht, die notwendigen Sicherheitsupdates und -patches an diesen Gesundheitsgegenständen oder -maschinen durchzuführen.

Diese Situation macht Medizinprodukte besonders anfällig für Schwachstellen vom Typ Log4Shell und zwingt zu perimetrischen Sicherheitslösungen (Netzwerkabschottung, Überwachungselemente usw.).

Dieser Ansatz erfordert bestimmte Fähigkeiten, die IT-Teams nicht unbedingt beherrschen. Es gibt also eine echte Herausforderung, in Cybersicherheit zu schulen und die Zusammenarbeit zwischen IT, CISR und biomedizinischen Abteilungen zu fördern.

Andernfalls wird es weiterhin zu kritischen Situationen kommen, wie z. B. bei Strahlentherapiegeräten, die aufgrund einer veralteten Windows-Version auch 2022 noch mit dem Conficker-Wurm infiziert sind. –

1.2 Digitale Transformation im Gesundheitswesen: ein später Wandel, der beschleunigt werden muss

In den letzten Jahren ist der Wandel der medizinischen Welt in Richtung eHealth nicht mehr zu leugnen. Der Sektor befindet sich in einem Prozess der Neugründung. Es werden neue Nutzungsweisen angenommen, die in der angespannten Situation der Covid-19-Pandemie auf die Probe gestellt wurden.



AUFSCHWUNG DER TELEMEDIZIN UND FERNÜBERWACHUNG

Die zunehmende Nutzung von Telemedizin und Telemonitoring, insbesondere im Rahmen von Hauspflege, erweitert die potenzielle Angriffsfläche von medizinischen Einrichtungen. Denn wenn ein Patient zu Hause beatmet wird, kann sein Beatmungsgerät zu einem neuen Zugangspunkt zum Krankenhausinformationssystem werden.

AUSLAGERUNG VON DIENSTLEISTUNGEN

Die wohl symbolträchtigste Dienstleistung dieser Art ist die Auslagerung der Terminvereinbarung über Online-Plattformen wie Doctolib, die viele Fragen und Kontroversen aufwirft, insbesondere in Bezug auf die Sicherheit der ausgetauschten Daten.

„Die massive Nutzung von ausgelagerten, oft weniger sicheren digitalen Diensten ist dort eine weit verbreitete Praxis, die Angreifer gerne ausnutzen.“

ANSSI – 2020[8]

MENSCHLICHE FEHLER: UNWISSENHEIT ÜBER CYBERRISIKEN

Und es gibt den menschlichen Faktor. Denn die digitale Transformation im Gesundheitswesen wirkt sich auf die Mitarbeiter der medizinischen Einrichtungen aus. Mitarbeiter, die nicht alle dieselben Reflexe der digitalen Hygiene besitzen ... Wie die ANSSI in ihrem Leitfaden zur digitalen Hygiene ausführlich erläutert: *„Jeder Nutzer ist ein vollwertiges Glied in der Kette der Informationssysteme. In dieser Eigenschaft und sobald sie in der Organisation ankommen, müssen sie durch Sensibilisierungs- und Schulungsmaßnahmen über die Sicherheitsprobleme, die einzuhaltenden Regeln und die richtigen Verhaltensweisen in Bezug auf die Sicherheit der Informationssysteme informiert werden.“*

26. Januar 2022

Eine Anfälligkeit, die durch die Praxis des Bring Your Own Device (BYOD) noch verstärkt wird: Einige Ärzte, die ihre Zeit zwischen Privatpraxis und Krankenhaus aufteilen, verwenden Geräte, die nicht von letzterem bereitgestellt werden und manchmal nicht dessen IT-Sicherheitsvorschriften entsprechen. –

STICHTAG

26. JANUAR 2022 IN FRANKREICH

Datum, an dem die französische Gesundheitsbehörde die ersten vier Arbeiten zum medizinischen Telemonitoring veröffentlicht hat, und zwar für folgende Erkrankungen: Diabetes, chronische Herzinsuffizienz, chronische Niereninsuffizienz und chronische Ateminsuffizienz.

Weitere Arbeiten werden folgen, um diese Grundlage zu erweitern, die dazu bestimmt ist, die Fernüberwachung dauerhaft und sicher einzusetzen. –

1.3 Der Sonderfall von Gesundheitsdaten

Das Gesundheitswesen steht aufgrund der Vielzahl an sensiblen und lebenswichtigen Daten die verarbeitet werden, besonders im Visier von Cyberkriminellen. Um welche Daten handelt es sich konkret und welche Herausforderungen sind damit verbunden?



WELCHE VERBINDUNG BESTEHT ZWISCHEN DEM ZUGANG ZU DATEN, GESUNDHEIT UND SICHERHEIT?

INTERVIEW

CHARLES BLANC-ROLIN
– PROJEKTLEITER FÜR DIGITALE SICHERHEIT IM GESUNDHEITSWESEN BEIM GCS E-HEALTH PAYS DE LA LOIRE



„Chirurgen werden es vorziehen, zur Kriegsmedizin zurückzukehren: Das bedeutet, ohne Daten auszukommen, anstatt sich auf potenziell falsche oder unvollständige Daten zu verlassen.“

Wie definieren Sie einen medizinischen Datensatz?

C.BR – Der Begriff bezeichnet alle Daten, die sich auf die Gesundheit des Patienten beziehen, sei es ein Operationsbericht, die Quotierung einer medizinischen Maßnahme oder auch ein Termin mit einem Angehörigen der Gesundheitsberufe.

Inwiefern hat der Zugang zu diesen Gesundheitsdaten mit der Sicherheit der Patienten zu tun?

C.BR – Das Thema sensible Daten wird oft unter dem Gesichtspunkt der **Vertraulichkeit** behandelt. Die breite Öffentlichkeit fürchtet die Offenlegung ihrer Kreditkartennummern, kann sich aber kaum vorstellen, welche Folgen der Diebstahl einer Sozialversicherungsnummer haben kann. Im Falle von medizinischen Daten sind die Folgen jedoch schwerwiegender als anderswo. Die **Integrität** der Daten ist eine Frage der Sicherheit: Wenn eine Dosierung verändert oder ein Allergiehinweis entfernt wird, steht manchmal das Leben des Patienten auf dem Spiel. Die **Verfügbarkeit** ist ebenfalls sehr wichtig, Chirurgen benötigen zum Beispiel Bilder, um zu operieren.

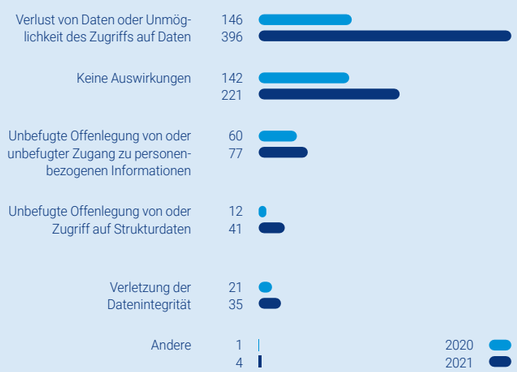
Warum ist das Vertrauen in Daten im Gesundheitswesen kritisch?

C.BR – Um das Beispiel der Chirurgen aufzugreifen: Sie würden lieber wieder zu einer **Kriegsmedizin** zurückkehren: Das bedeutet, ohne Daten zu arbeiten, anstatt sich auf potenziell falsche oder unvollständige Daten zu verlassen.

Kommt die Unzugänglichkeit von Daten im Gesundheitssektor häufig vor?

C.BR – Laut CERT-Santé war dies der Fall bei der Hälfte der im Jahr 2021 gemeldeten Vorfälle für “alle oder einen Teil der Strukturanwendungsdaten“. –

AUFLISTUNG DER SICHERHEITSVORFÄLLE NACH ART DER AUSWIRKUNGEN AUF DIE DATEN



Quelle: Beobachtungsstelle für Meldungen von Sicherheitsvorfällen in Informationssystemen für den Gesundheitssektor (2021)

IMMER MEHR DATEN ZU SCHÜTZEN

Ein weiterer Parameter, den es zu berücksichtigen gilt, ist die Menge der von Gesundheitseinrichtungen erzeugten Daten, die in den letzten Jahren stetig gewachsen ist.

Die Entmaterialisierung ist mit der Einführung von digitalen Basisdiensten wie „Mein Gesundheitsraum“ eindeutig im Alltag der Fachleute angekommen. Dieser Bereich ist seit Anfang 2022 verfügbar und ermöglicht es jeder Französin und jedem Franzosen, alle ihre/seine Gesundheitsdokumente (Rezepte, Testergebnisse usw.) zu finden, personenbezogene Informationen über ihre/seine Familiengeschichte einzugeben und sich auf sichere Weise mit Gesundheitsfachkräften auszutauschen.

Die Digitalisierung ist mittlerweile auch integraler Bestandteil der Geschäftsprozesse von Pflegekräften, wie die Zunahme von Diagnosehilfsmitteln wie Psychaclic[9] oder die in Frankreich seit dem 1. März 2022 geltende Verpflichtung, Todesbescheinigungen elektronisch auszustellen, zeigen.

Die Datenbanken werden immer umfangreicher, ihre Verwaltung und Einhaltung der Richtlinien wird zwischen Aufbewahrungspflichten und dem Recht auf Löschung[10], das in der DSGVO vorgesehen ist, immer komplexer ...

EINE FUNDGRUBE AN INFORMATIONEN

Gesundheitsdaten können im Mittelpunkt von böswilligen Handlungen stehen, die darauf abzielen, den Betrieb eines Krankenhauses zu destabilisieren oder einer bestimmten Person zu schaden. Beispiel im Juni 2022: 1 Milliarde chinesische personenbezogene Daten, darunter auch medizinische Informationen, waren für 10 Bitcoins (200.000 US-Dollar) zum Verkauf angeboten worden[11].

KENNZAHL

x30

DAS GESAMTVOLUMEN DER EHEALTH-DATEN

Im Jahr 2016 gab die Anap an, dass sich das Gesamtvolumen der eHealth-Daten alle 73 Tage verdoppelt ... Es hat sich seitdem also um das 30-fache erhöht.

KENNZAHL

Zwischen 50 und 250 €

MEDIZINISCHE AKTE

Das ist der Wiederverkaufspreis für eine einzige Krankenakte[12]

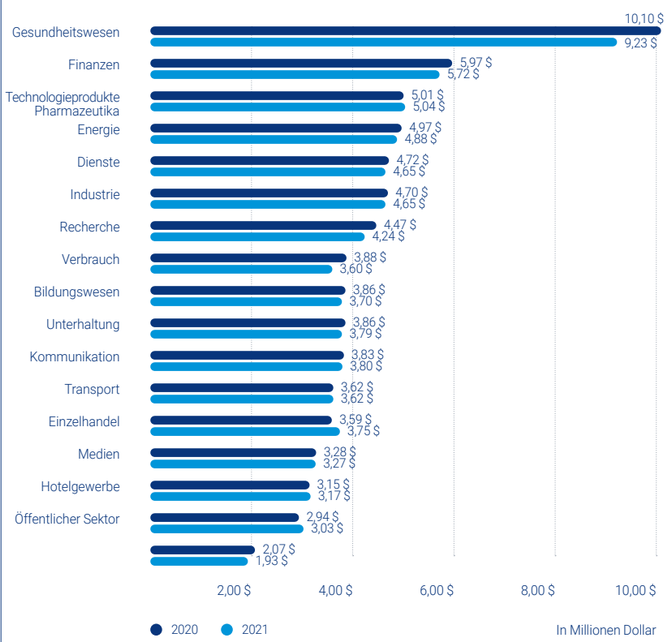
Gesundheitsdaten sind daher eine wertvolle Ressource, an der auch andere Akteure wie die GAFAM interessiert sind. Die investigative Website The Markup[13] deckte im Juni 2022 auf, dass US-amerikanische Gesundheitseinrichtungen sensible Daten (Name des Arztes, Suchbegriffe oder auch Krankheitsbilder) über ihre Patienten durch Nutzung von „Meta Pixel“ an Facebook weitergaben.

LECKS, DIE VIEL GELD KOSTEN

Mit zunehmender Medienpräsenz sensibilisiert diese Art von Fällen allmählich die öffentliche Meinung. Auch der Ruf der betroffenen Unternehmen wird auf die Probe gestellt, wie zum Beispiel bei Shields, einem US-amerikanischen Konzern für Bildgebung und ambulante Chirurgie, der einem Datendiebstahl zum Opfer fiel, der fast 2 Millionen Menschen betraf.

Aber auch der Preis, der dafür zu zahlen ist, ist beachtlich und einschneidend. Ein IBM-Bericht[14] schätzt, dass die durchschnittlichen Kosten einer Datenverletzung im Fall einer Gesundheitseinrichtung über 10 Millionen US-Dollar betragen. –

DIE DURCHSCHNITTLICHEN KOSTEN EINES DATENVERLUSTS NACH VERTIKALEN MÄRKTEN, DOMINIERT VOM GESUNDHEITSWESEN



1,5 Mio €

KENNZAHL

GELDSTRAFE

1,5 Millionen Euro. Dies ist die Höhe der Geldstrafe, die das Unternehmen Dedalus Biologie wegen Sicherheitsmängeln erhielt, „die zum Abfluss von medizinischen Daten von fast 500.000 Personen führten“ (CNIL).

WEITERFÜHRENDE INFORMATIONEN

FÜNF BESONDERE WEBINARE

→ Sehen Sie sich unsere fünfteilige Webinarreihe[15] an, um mehr über die außerordentliche Anfälligkeit von Krankenhausumgebungen gegenüber Cyberangriffen zu erfahren.



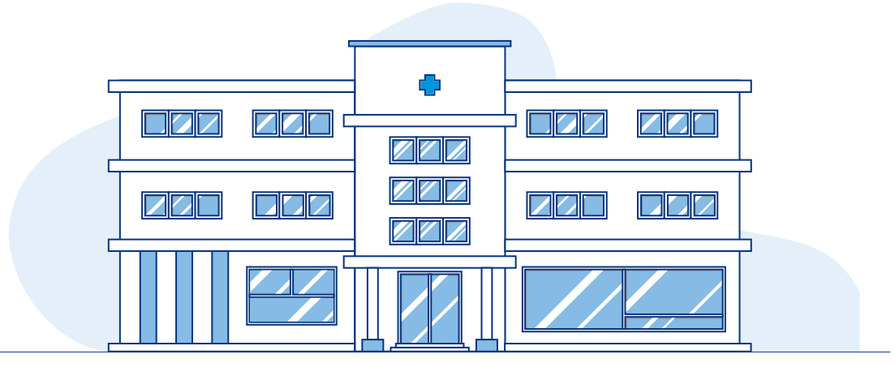
02.

Anatomie einer polymorphen Bedrohung mit zahlreichen Eintrittspunkten

Über welche Vektoren gelangt die Cyberbedrohung in Gesundheitseinrichtungen? Welchen verschiedenen Arten von Angriffen sind sie ausgesetzt? Handelt es sich dabei immer um gezielte Vorfälle? Cyberkriminellen mangelt es bei Angriffen auf die medizinische Welt nicht an Einfallsreichtum, aber manchmal ist der Sicherheitsvorfall auf einen Fehler und nicht auf einen Cyberangriff zurückzuführen. Seine Folgen sind jedoch ebenso katastrophal.

2.1 Wie dringen Cyberkriminelle in die IT-Struktur von Gesundheitseinrichtungen ein?

Die Einfallstore für Cyberbedrohungen in Gesundheitseinrichtungen sind leider zahlreich. Sie können in vier Vektoren zusammengefasst werden.



1. MENSCHEN

Cyberangriffe nutzen oder zielen auf eine oder mehrere Personen ab(Ärzte, Pfleger, Agenten, Administratoren bis hin zu den Patienten selbst).
Im Jahr 2020 gab ein Großhändler aus Rouen, der Apotheken in der Region belieferte, einen Auftrag im Wert von 6,6 Millionen Euro für Gele und Masken an eine Firma, die sich schließlich als Phantom herausstellte. Ein dramatisches Beispiel für einen meisterhaften Betrug[16] vor dem angespannten Hintergrund der Covid-19-Pandemie.

2. SOFTWARE

Softwarebasierte Cyberangriffe umfassen alle Angriffe, die eine Schwäche, einen Fehler oder die Überalterung einer Software ausnutzen, die auf einem Computer oder einem computergestützten, medizinischen Instrument installiert ist.
Im Jahr 2020 wurde eine Reihe von Sicherheitslücken in einer Lösung der Dedalus-Gruppe, die sich auf Gesundheitssoftware spezialisiert hat, aufgedeckt. Eine dieser Lücken ermöglichte den Zugriff auf Tickets von Kunden wie Krankenhäusern und Laboren in denen sich möglicherweise Kennungen und Passwörter für die Fernadministration befanden.

3. NETZWERK

Wie der Name schon sagt, handelt es sich bei einem Cyberangriff auf ein Netzwerk um alle Cyberangriffe, die über das Netzwerk eines Krankenhauses laufen.
Die Dienste der Assistance Publique – Hôpitaux de Paris (AP-HP) wurden im Jahr 2020 von einem Denial-of-Service-Netzwerkangriff (DDoS) auf zwei ihrer Internetadressen angegriffen. Das Ergebnis: der Zugriff auf E-Mails und Anwendungen für die Mitarbeiter war gestört.

4. PHYSISCH

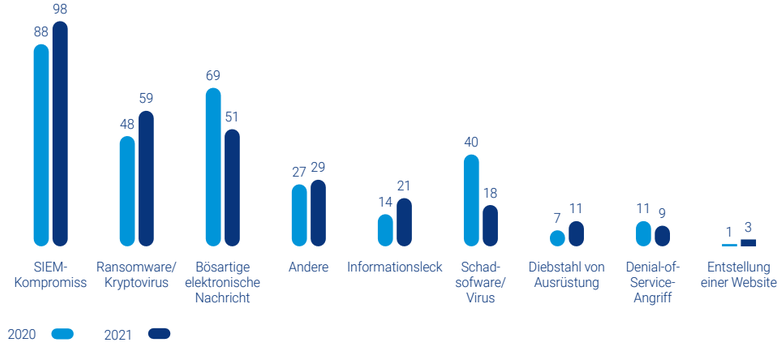
Physische Cyberangriffe umfassen Angriffe, die speziell auf die materielle Dimension einer medizinischen, informationstechnischen oder betrieblichen Ausrüstung abzielen.
Ab 2019 simulierten israelische Forscher einen MITM-Angriff *Man-In-The-Middle* indem sie einen Raspberry Pi direkt in ein Krankenhaus einschleusten. So konnten sie medizinische Bilddaten abfangen, die über das DICOM-Protokoll übertragen wurden, und nachweisen, dass diese Daten manipuliert werden können.

Unabhängig davon, welche Angriffsvektoren Cyberkriminelle wählen, ist heutzutage Ransomware die am häufigsten vorkommende „Virenlast" im Gesundheitswesen.
Zudem ist es auch stark gefährdet durch Datendiebstahl und DDoS-Angriffe (Distributed Denial of Service).

„Die Qualität der Phishing-Kampagnen, die wir abfangen, nimmt zu, und einige gehen sogar so weit, die Identität des Universitätsklinikums Brest anzunehmen. Der auffälligste Anstieg ist jedoch bei den Initial Access Brokers (IAB) zu verzeichnen. Diese Erstzugangsvermittler sind darauf spezialisiert, Benutzerkennungen zu finden, um sie weiterzuverkaufen."

JEAN-SYLVAIN CHAVANNE
– CISO DES UNIVERSITÄTS-KLINIKUMS VON BREST

ANZAHL DER VORFÄLLE NACH ART DER HERKUNFT



Quelle: IBM Security Report, Cost of Data Breach (2022)



2.2 Der gesamte Gesundheitsbereich in der Schusslinie

Krankenhäuser und Kliniken sind das erste Ziel von Cyberangriffen im Gesundheitswesen. Aber sie sind nicht die Einzigen. Auch Labore, Lieferanten und sogar Patienten sind im Visier von Cyberkriminellen.



Auch in den USA (Baton Rouge General in Louisiana, Jack Huston Memorial in Phoenix und das Southwest Health Center in Wisconsin) sowie in Frankreich (Vitry-le-François, Saint-Dizier, Charleville-Mézières, Corbeil-Essonnes) und Spanien (Barcelona) waren bereits 2022 mehrere Krankenhäuser davon betroffen.

Aber auch die Laboratorien werden ins Visier genommen, insbesondere wegen der medizinisch-administrativen Daten, die sie in Software für medizinische Biologie vom Typ Mega Bus[18] eingeben.

In jüngster Zeit haben Cyberkriminelle ihre Zielgruppen noch weiter ausgedehnt. Zum einen nehmen sie nun verschiedene Anbieter ins Visier, die ihnen die virtuellen Türen zu den Informationssystemen von Krankenhäusern öffnen können. Und zum anderen schrecken sie nun nicht mehr davor zurück, die Patienten selbst anzugreifen, um sie durch den Diebstahl ihrer Gesundheits- und/oder persönlichen Daten zu erpressen. –

WENN CYBERKRIMINELLE AUF PATIENTEN ABZIELEN

→ Im Jahr 2020 erlebten die Patienten von etwa 20 finnischen Psychotherapiezentren, die von der Firma Vastaamo betrieben werden, eine böse Überraschung: Sie erhielten eine Lösegeldforderung in Höhe von 500 Euro, die sie in Bitcoin bezahlen sollten, da ansonsten die während ihrer Sitzungen gesammelten Daten preisgegeben werden würden. Ein Fall von doppelter Erpressung[19], der Tausende Beschwerden bei den Behörden zur Folge hatte. –

WENN CYBERKRIMINELLE DIE LIEFERKETTE INS VISIER NEHMEN

→ Im Jahr 2020 wurden Dienstleister, die auf die Kühlkette von Covid-19-Impfstoffen spezialisiert sind, Ziel von Phishing-Kampagnen. Das Ziel: sensible Informationen über den Transport und die Verteilung abzurufen. Eine Kampagne, die laut den Cybersicherheitsexperten von IBM die Merkmale eines Angriffs auf staatlicher Ebene aufweist. –

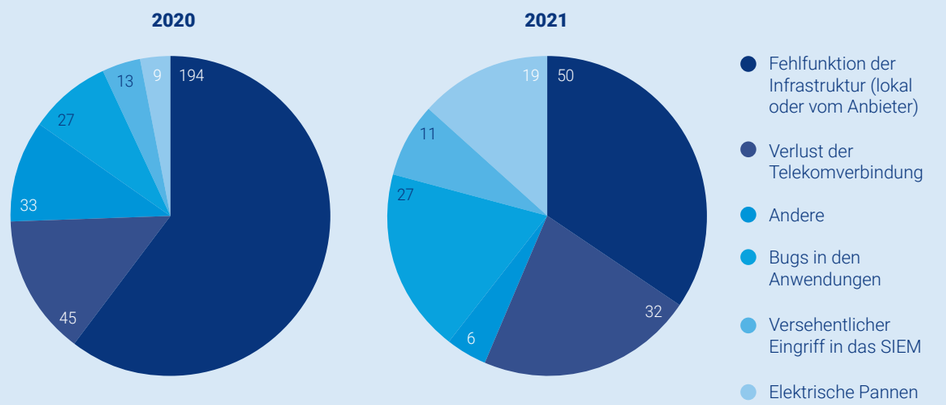
2.3 Dies ist kein Cyberangriff

Auch wenn man natürlich alle notwendigen Maßnahmen ergreifen muss, um sich vor Cyberangriffen zu schützen, darf man nicht vergessen, dass auch Vorfälle, die nicht böswilligen Ursprungs sind, schwerwiegende Folgen für das Gesundheitssystem haben können.



In einer anfälligen und instabilen Krankenhausumgebung kann ein Computervorfall in der Tat zu einem Sicherheitsvorfall führen. Wie im Juni 2022 auf der Seite des Universitätsklinikums von Nantes, wo ein größerer Stromausfall, verursacht durch das installierte Antivirusprogramm, alle Windows 7-Arbeitsplätze betraf, darunter auch biomedizinische Geräte, die dadurch unbrauchbar wurden. –

VERTEILUNG DER VORFÄLLE MIT NICHT BÖSWILLIGEM URSPRUNG



Quelle: Beobachtungsstelle für Meldungen von Sicherheitsvorfällen in Informationssystemen für den Gesundheitssektor (2021)

48 %

KENNZAHL

NICHT BÖSARTIG

48 % der Meldungen an das CERT-Gesundheitsobservatorium[20] sind nicht bösartigen Ursprungs

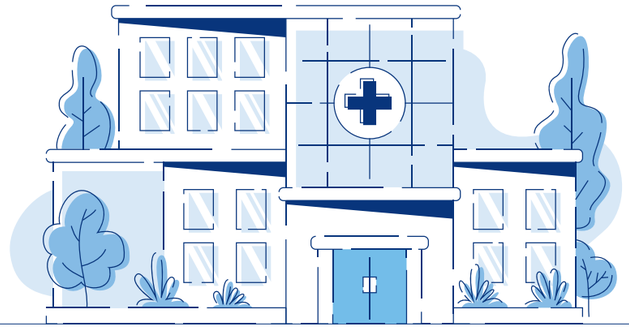


Welche Abhilfemaß-nahmen gibt es, um das Gesundheits-wesen sicherer zu machen?

Wie kann man sich vor Cyberangriffen schützen?
Was sagt die aktuelle Gesetzgebung zu diesem Thema?
Welche Unterstützung können die staatlichen Behörden hier leisten? Dieser Schritt kann kompliziert sein, ist aber für einen angemessenen Schutz lebenswichtig.

3.1 Welche Maßnahmen können Sie ergreifen, um die Infrastruktur des Gesundheitswesens zu schützen?

Die Infrastrukturen von Gesundheitseinrichtungen sind von Natur aus lebenswichtig. Die Leistungsfähigkeit und Verfügbarkeit von Computernetzen in unseren Gesundheitssystemen ist umso wichtiger, als das Leben von Patienten oft von den Informationen abhängt, die über diese Netze ausgetauscht werden.



SCHRITT 1: PRÜFUNG UND RISIKOANALYSE

Der erste Schritt in jedem Ansatz zum Schutz vor Cyberangriffen besteht in der Kenntnis der Systeme. In dieser Phase geht es darum, die sensibelsten Vermögenswerte zu identifizieren, um die Angriffsfläche durch die Festlegung einer Sicherheitsrichtlinie zu verringern.

„Diese Kartografie ermöglicht es, die Komponenten der Informations- und Betriebssysteme der Gesundheitsstrukturen nach verschiedenen Kriterien wie Überalterung oder Kritikalität zu identifizieren und zu klassifizieren.“

STÉPHANE PRÉVOST – PRODUCT MARKETING MANAGER BEI STORMSHIELD

SCHRITT 2: EINSATZ GEEIGNETER SICHERHEITSLÖSUNGEN

Lösungen wie beispielsweise die von Stormshield decken umfangreiche Sicherheitsbereiche ab.

Schutz der Netze

Zu den Funktionen, die zusammengeführt werden müssen, um Computernetzwerke in Krankenhäusern zu sichern, gehören:

- Netzwerksegmentierung,
- Zugangskontrolle, Verwaltung von Fernwartung und anderen Fernzugriffen,
- Sicherung der Kommunikation,
- Zwei-Faktor-Authentifizierung,
- Filterung nach Benutzer,
- Sicherung der Kommunikationsprotokolle von biomedizinischen Geräten (Intrusion Prevention – IPS OT).

Schutz von Arbeitsplätzen

Um von einem verstärkten Schutz ihrer Endgeräte zu profitieren, müssen Gesundheitseinrichtungen darauf achten, dass sie Folgendes eingerichtet haben:

- Zwei-Faktor-Authentifizierung,
- Desktop Intrusion Prevention (HIPS) durch Verhaltensanalyse,
- Die Verwaltung von externen Geräten (bis hin zur Einrichtung von Isolierstationen).

„Ich habe schon manchmal in Zusammenarbeit mit dem biomedizinischen Leiter Lösungen zur physischen Blockierung von USB-Anschlüssen eingeführt. So wird z. B. verhindert, dass jemand das Ultraschallgerät zum Aufladen seines Smartphones benutzt und damit das Gerät gefährdet. “

CHARLES BLANC-ROLIN – PROJEKTLEITER FÜR DIGITALE SICHERHEIT IM GESUNDHEITSWESEN BEIM GCS EHEALTH PAYS DE LA LOIRE

PSEUDONYMISIERUNG ODER UMKEHRBARKEIT DER ANONYMITÄT

MIT **JEAN-SYLVAIN CHAVANNE** – CISO AM UNIVERSITÄTSKLINIKUM BREST

→ ***„Es ist eine Besonderheit des Gesundheitswesens, dass bestimmte sensible Daten nicht vollständig anonymisiert werden können: Eine Gesundheitseinrichtung muss beispielsweise auch zu einem späteren Zeitpunkt auf einen Patienten zurückgreifen können, der sich einer bestimmten Behandlung unterzogen hat. Aus diesem Grund werden die Patientendaten in zwei Datenbanken aufgeteilt, um bei Bedarf eine erneute Identifizierung zu ermöglichen.“ –***

Die Anwendung einer ausreichend starken Passwortrichtlinie[21] ist ebenfalls notwendig, um zu verhindern, dass man Ziel böswilliger Aktionen aus dem Internet wird.

Schließlich ist eine verbesserte Nachverfolgung von Korrekturen unerlässlich, um das Sicherheitsniveau an den Arbeitsplätzen in Gesundheitseinrichtungen zu erhöhen. Dazu müssen exponierte Komponenten überwacht und aktualisiert werden, wenn ein Patch zur Verfügung gestellt wird, wobei kritische Schwachstellen vorrangig zu behandeln sind. So hätte das Drama beim Cyberangriff auf das Düsseldorfer Krankenhaus vermieden werden können: Ein Patch der ausgenutzten Schwachstelle war nämlich sieben Monate zuvor zur Verfügung gestellt worden.

Datenschutz

Während die erste Maßnahme auf dieser Ebene darin besteht, den Versand jeglicher Patientenakten per unverschlüsselter E-Mail zu verbieten, sind weitere Maßnahmen erforderlich. Folgendes muss gewährleistet sein:

- Eine verschlüsselte Krankenakte mit verschiedenen Zugangsschlüsseln,
- Die End-to-End-Verschlüsselung von Informationen, insbesondere wenn sie aus dem SIEM extrahiert werden, um sie an ein anderes Krankenhaus weiterzuleiten (z. B. im Rahmen eines koordinierten Behandlungspfades),
- Ein Anonymisierungs- und Pseudonymisierungsprozess für eine effektive Datenverarbeitung.



SCHRITT 3: ÜBERPRÜFUNG UND KONTINUIERLICHE VERBESSERUNG

Der nächste Schritt ist die Kontrolle der Einhaltung und die Überprüfung von Abweichungen von der Sicherheitsrichtlinie. Zu diesem Zweck ist insbesondere Folgendes erforderlich:

- regelmäßig die Protokolle der Perimeterausrüstung analysieren,
- Sicherheitsprüfungen oder Penetrationstests durchführen,
- eine Planungsphase erneut starten, um Korrekturmaßnahmen durchzuführen.

„Das Interesse der Gesundheitsstrukturen am Managed SOC bestätigt die Attraktivität der Zusammenlegung von Ressourcen angesichts der Schwierigkeiten, diese Stellen zu besetzen (Mangel an Profilen, Finanzierung usw.).“

JACKY GRISEY – SECURITY OPERATIONS MANAGER FÜR GESUNDHEIT, ADVENS

„Die Installation eines Patches für eine kritische Schwachstelle auf einer im Internet aktiven Komponente ist keine Garantie gegen einen Missbrauch wie in der Vergangenheit. Sie sollten auch ihre Protokolle analysieren, um zu überprüfen, ob sie nicht auf einer anderen Komponente ausgenutzt wurden, und im Zweifelsfall alle ihre Konten erneuern.“

STÉPHANE PRÉVOST – PRODUCT MARKETING MANAGER STORMSHIELD

ENGAGEMENT FÜR SENSIBILISIERUNG UND AUSBILDUNG

Zur Erhöhung des Schutzniveaus in Gesundheitseinrichtungen ist eine Sensibilisierung zwingend erforderlich. Diese Kampagnen sollten sich zunächst an die Fachleute des Sektors richten, wie hier in Centre-Val de Loire[22] mit der Entwicklung von **Sensibilisierungs- und Schulungsplattformen** für Einrichtungen im Gesundheitswesen und in der Sozialmedizin. Diese Kommunikations- und Sensibilisierungsmaßnahmen müssen sich jedoch auch an Patienten und Hersteller von Medizinprodukten richten. Und zwar in einer Form, die der jeweiligen Bevölkerung angepasst wird.

„Die Industrie muss in Cybersicherheit geschult werden, da viele noch immer Computertechnik wie vor 30 Jahren betreiben. Auch die IT-Sicherheit sollte in den Lehrplan der Ärzte aufgenommen werden und nicht nur der Datenschutz, wie es derzeit der Fall ist.“

JACQUES LABIDURIE – CISO UNIKLINIKUM LIMOGES

Einige Akteure zögern nicht, bei der Befähigung der Nutzer noch einen Schritt weiter zu gehen. Das Krankenhauszentrum Calais protokolliert nun die Sitzungen auf seinen als kritisch eingestuften Servern[23]. Diese neue Richtlinie gilt sogar für ihre Auftragnehmer, von denen 40 % nun so verfahren.

In diesem bereits stark angespannten Sektor ist es jedoch zwingend notwendig **dass die Cybersicherheit mit den Geschäftspraktiken in Einklang steht:** z. B. sind wiederholte Aufforderungen zur Eingabe eines zwölfstelligen Passworts in Notsituationen nicht angemessen. –

WIE KANN MAN MEDIZINPRODUKTE SICHERN, OHNE IHRE CE-KENNZEICHNUNG IN FRAGE ZU STELLEN?

→ Die wichtigste Lösung für die Netzwerksicherheit besteht darin, Netzwerke abzuschotten und sie über eine Mikrosegmentierung vom Rest des SIEM zu isolieren. Wenn also ein Bedarf für den Austausch von Datenströmen besteht, sollte man versuchen, diese sehr fein zu filtern, und wenn möglich, die Erkennung von Anomalien auf denselben Datenströmen z. B. über eine IDS-Sonde vorsehen. –

„Die Kontextualisierung ist bei unseren Aufklärungsmaßnahmen sehr wichtig. Ein vorheriges Treffen mit dem Abteilungsleiter erleichtert beispielsweise das Verständnis für die Funktionsweise der Abteilung und das Aufzeigen tatsächlicher Beispiele, wie z. B. die Tatsache, dass man seine Karte bei verschiedenen Funkmanipulationen an Ort und Stelle lässt. Verwaltung, Einkauf, klinische Forschung – sie alle haben ein spezifisches Vokabular, das man beherrschen muss, um effektiv arbeiten zu können.“

CORALIE ACHARD-TORTUL – DPO DES UNIVERSITÄTSKLINIKUMS CHU LIMOGES

CYBERSICHERHEIT FÜR GESUNDHEITS-EINRICHTUNGEN MIT STORMSHIELD

CYBERSICHERHEIT UND GESUNDHEIT

→ Stormshield beteiligt sich am Aufbau einer vertrauenswürdigen europäischen Cybersicherheit. Alle Produktlinien sind Teil unseres laufenden Qualifizierungs- und Sicherheitszertifizierungsprozesses bei den zuständigen europäischen Behörden.

STORMSHIELD NETWORK SECURITY FÜR DEN NETZWERKSCHUTZ

Die Stormshield Network Security-Firewalls (SNS) gewährleisten die Kontinuität und Verfügbarkeit von Diensten durch Netzwerksegmentierung, Bypassing und Intrusion Prevention. Und um die Patientendaten beim Austausch zu schützen, sichern diese Firewalls den Fernzugriff zur Fernwartung über Virtual Private Networks (VPN).

STORMSHIELD DATA SECURITY FÜR DEN DATENSCHUTZ

Der Schutz von Gesundheitsdaten wird zu einer zentralen und lebenswichtigen Achse für Gesundheitseinrichtungen. Mit einer End-to-End-Verschlüsselung bewahrt die Stormshield Data Security (SDS) die Integrität und Vertraulichkeit sensibler Informationen. Insbesondere, wenn die Daten aus dem Informationssystem entnommen werden.

STORMSHIELD ENDPOINT SECURITY FÜR DEN SCHUTZ VON SERVERN UND DESKTOPS

Um die Veränderungen im medizinischen Bereich und die neuen professionellen Nutzungsmöglichkeiten zu unterstützen, bietet die Lösung Stormshield Endpoint Security (SES) einen autonomen Schutz für Endgeräte, die in der Lage sind, die Schutzstufen dynamisch an ihre Umgebung anzupassen.

STORMSHIELD LOG SUPERVISOR FÜR DIE SICHTBARKEIT VON NETZWERKEREIGNISSEN

Mit dem Tool Stormshield Log Supervisor (SLS) ist es möglich, den Status Ihres Computernetzwerks auf einen Blick zu sehen und auf Ereignisprotokolle zuzugreifen. Eine ideale Lösung zur Optimierung von Suchaufgaben und der Reaktion auf Vorfälle.

WELCHE RECHTLICHEN VERPFLICHTUNGEN BESTEHEN FÜR GESUNDHEITSEINRICHTUNGEN?



IN DEN VEREINIGTEN STAATEN

→ Es gilt der US-amerikanische Standard HIPAA (Health Insurance Portability and Accountability Act) und dessen Abschnitt über personenbezogene Gesundheitsdaten mit dem Namen ePHI (electronic Protected Health Information).

AUF EUROPÄISCHER EBENE

→ Die NIS-2-Richtlinie listet eine Reihe von Verpflichtungen für Betreiber kritischer Dienstleistungen (ESOs) auf, zu denen die meisten Gesundheitseinrichtungen mit einem medizinischen Notdienst gehören. Dazu gehört auch die Pflicht, Sicherheitsvorfälle zu melden. Wie alle Unternehmen, die in der Europäischen Union tätig sind, müssen sie auch die DSGVO beachten.

IN FRANKREICH

→ Diese kritischen Einrichtungen, die manchmal als Betreiber von lebenswichtigen Einrichtungen (OIV) eingestuft werden, unterliegen ebenfalls dem Gesetzbuch über das öffentliche Gesundheitswesen, der interministeriellen Anweisung Nr. 901 und der PGSSI-S. Seit April ist das erste einklagbare Dokument der PGSS-S, der Referenzrahmen für die elektronische Identifizierung[24], verfügbar. Es verpflichtet Einrichtungen und Herausgeber zur Identifizierung von Patienten und Fachkräften, um die Sicherheit des Zugangs zu erhöhen. Ergänzend dazu können Gesundheitseinrichtungen den vom ANSSI herausgegebenen Leitfaden für bewährte Verfahren heranziehen.

3.2 Ein Bewusstsein und durch öffentliche Maßnahmen unterstützte Bemühungen

Die Anfälligkeit von Gesundheitseinrichtungen ist jedoch nichts Neues und beschäftigt die Fachwelt schon seit über einem Jahrzehnt. Es gibt bereits Initiativen, sowohl auf europäischer als auch auf nationaler Ebene.



AUF EUROPÄISCHER EBENE

Angesichts der Entstehung einer echten Datenwirtschaft ist die Europäische Union im Begriff, eine ganze Reihe von Gesetzen zu erarbeiten, die derzeit geprüft werden oder bereits in Kraft getreten sind:

- Datenschutz-Grundverordnung (DSGVO).
- Europäisches Daten-Governance-Gesetz (Data Governance Act [DGA]).
- Gesetz über digitale Dienste (Digital Services Act [DSA]).
- Gesetz über digitale Märkte (Digital Markets Act [DMA]).

Der Entwurf der Verordnung über den Europäischen Gesundheitsdatenraum (EHDS)[25] ist der erste vertikale Text des Korpus, d. h. der erste Text, der einen Rahmen für die gemeinsame Nutzung von Daten für einen bestimmten Sektor vorschlägt. Anfang Mai 2022 veröffentlicht, wurde er von Margarítis Schinás, dem Vizepräsidenten der Europäischen Kommission als *„Neuanfang der digitalen Gesundheitspolitik der Union"*[26] bezeichnet. –

STICHTAG

Juli 2016

Bereits im Juli 2016 griff Europa das Thema Cyber durch die NIS-Richtlinie und die Identifizierung von Betreibern kritischer Dienstleistungen (OSE) im Gesundheitssektor auf (neben anderen Sektoren wie Energie, Transport, Wasser, Bankwesen oder auch digitale Infrastruktur). Das Ziel: Schutz ihrer kritischen Informationssysteme.

„Diese Arbeiten (DSA und DMA), die das Thema übergreifend und systemisch angehen, stehen im Einklang mit den verschiedenen Texten, darunter die DSGVO, die NIS-Richtlinie oder der Data Act. Sie versuchen gleichermaßen, Innovationen zu fördern, die Einwohner Europas zu schützen und die strategische Autorität der Europäischen Union zu festigen."

RAYNA STAMBOLIYSKA – EXPERTIN FÜR DIGITALE DIPLOMATIE, CYBERSICHERHEITSEXPERTIN UND UNABHÄNGIGES MITGLIED DER ENISA-ARBEITSGRUPPE FÜR AUFKOMMENDE UND ZUKÜNFTIGE BEDROHUNGEN

KREUZINTERVIEW:

IST DIE EU-VERORDNUNG ÜBER DIE VERFÜGBARKEIT DER ELEKTRONISCHEN GESUNDHEITSDATEN DEN HEUTIGEN HERAUSFORDERUNGEN GEWACHSEN?

Ja
schon eher

Diese Verordnung ist eine Antwort auf die Herausforderungen, mit denen wir heutzutage konfrontiert sind. Sie muss in fünf bis zehn Jahren aktualisiert werden, um die neuen Bedrohungen zu berücksichtigen, die durch die Technologien der Dezentralisierung, Web 3.0 usw. entstanden sind, aber zum jetzigen Zeitpunkt **handelt es sich um eine willkommene Ergänzung der DSGVO und der NIS-Richtlinie.**

Es ist also durchaus ein wichtiger Meilenstein in unserer gemeinsamen Geschichte, aber mir scheint, dass es die COVID-19-Pandemie war, die diese Wiederbelebung eingeleitet hat. In diesem Zusammenhang hat das eHealth Network, das Vertreter der Mitgliedstaaten im Bereich der digitalen Gesundheit zusammenbringt und an dem ich als Beobachter teilnehme, ein erstes Beispiel für europäische Zusammenarbeit geliefert: eine gemeinsame Toolbox für die Entwicklung von mobilen Anwendungen zur Kontaktüberwachung.

Die Pandemie hat deutlich gemacht, dass der Sektor weiter reguliert werden muss, um den Schutz von Gesundheitsdaten wirklich zu gewährleisten. Die europäischen Entscheidungsträger haben das verstanden, und diese Verordnung ist der Beweis dafür. **Sie schlägt ein Schema zur Sicherung des Informationsaustauschs vor, verschärft die Meldepflichten bei Vorfällen und die Interoperabilität.**
Verschiedene Zertifizierungsstandards (für elektronische Patientenakten, Pflegeanwendungen usw.) sollten ebenfalls daraus hervorgehen.

Diese Verordnung als Schnittstelle zu anderen Vorschriften gehört zu den fortschrittlichsten: Wir können sogar von einem einzigartigen Text sprechen, was die Kapitel über die primäre und sekundäre Nutzung von Daten betrifft. Letztere ebnen den Weg für die Verwendung in der Forschung, um die öffentliche Gesundheitspolitik zu lenken und die Patientenbetreuung zu verbessern. –



DAMIAN KLIMAS –
DOTLAW-PARTNER
UND BEOBACHTER DES
EHEALTH NETWORK

Nein
nicht ganz

Als sektoraler Rahmen baut der Text auf dem horizontalen Rahmen auf, der durch die NIS2-Richtlinie in Bezug auf Sicherheitsfragen geschaffen wurde. Artikel 50 enthält jedoch spezifische Elemente zur Sicherheit von Zugängen.

Der Zweck dieses Textes ist es, einen Rahmen für die gemeinsame Nutzung von Daten vorzuschlagen, der große Auswirkungen auf die Art und Weise haben wird, wie Daten in Europa verwendet werden. Seine Ambitionen sind bedeutend: Harmonisierung des Begriffs der sekundären Nutzung von Gesundheitsdaten zwischen verschiedenen Staaten und Implementierung einer robusten technologischen Infrastruktur, um die Nutzung dieser Daten zu ermöglichen.



RAYNA STAMBOLIYSKA –
EXPERTIN FÜR DIGITALE DIPLOMATIE,
CYBERSICHERHEITSEXPERTIN UND
UNABHÄNGIGES MITGLIED DER
ENISA-ARBEITSGRUPPE FÜR AUFKOMMENDE
UND ZUKÜNFTIGE BEDROHUNGEN

An dieser Stelle stellt sich die Frage zur Datenhoheit im Zusammenhang mit dieser gemeinsamen Nutzung. **Wir können die Schaffung eines Auskunftsrechts bedauern, das inkohärent mit dem bereits in der DSGVO festgelegten Auskunftsrecht ist**, was wiederum zu Situationen der Rechtsunsicherheit führen könnte. Auch das Thema der Kontrolle durch den Einzelnen wird dort nur unzureichend behandelt: Im Leitungsorgan des EHDS ist beispielsweise kein Patientenvertreter vorgesehen.

Schließlich **ist die Frage, wie ein solcher Raum implementiert werden soll, in der jetzigen Form nicht ganz klar:** wir können glauben, dass es darum geht, eine einzige riesige Datenbank aufzubauen, wo die Verordnung in Wirklichkeit vorsieht, verschiedene dezentralisierte Datenbanken miteinander zu verbinden.

Dieser Aufbau verweist auf eine ganze Reihe von Fragen (Governance, Benutzerwege, Datenformate, Vorgehen bei Beschwerden usw.), deren Antworten nicht in erster Linie technologischer Natur sein können und sollten. –

ZUM MERKEN

→ Diese Verordnung sieht immerhin einige technische Sicherheitsanforderungen zu praktischen Fragen des Zugangs und der Rückverfolgbarkeit vor (CF Artikel 50).

132

KENNZAHL

132 Schulen nehmen am Parcours für Cybersicherheit des Plans France Relance teil

CHARLOTTE DRAPEAU – LEITERIN DES BÜROS GESUNDHEIT UND GESELLSCHAFT, ANSSI, 2022[29]

AUF NATIONALER EBENE

Die französische Regierung hat im April 2019 einen Fahrplan vorgelegt, um *„die Beschleunigung des digitalen Wandels im Gesundheitswesen“*[27] als Teil eines umfassenderen Plans mit dem Namen *Ma Santé 2022* voranzutreiben. Dieser Veröffentlichung folgte die Veröffentlichung einer technischen Doktrin[28]. Diese wird jährlich überarbeitet, setzt einen Bezugsrahmen und gibt allen Akteuren im Bereich eHealth in Frankreich den Weg vor.

Die digitale Komponente des Segur im Gesundheitswesen ist Teil dieses Bezugsrahmens und soll den Transformationsprozess beschleunigen. Im Rahmen dieses Prozesses hat das Ministerium für Solidarität und Gesundheit Investitionen in Höhe von 2 Milliarden Euro freigegeben. Die Ziele: Begleitung des digitalen Übergangs von Gesundheits- und Pflegeeinrichtungen, Modernisierung der bestehenden Informationssysteme und Stärkung von Interoperabilität, Konvergenz und Sicherheit. Dieses Budget beinhaltet 350 Millionen Euro, die speziell für die Cybersicherheit dieser Strukturen bestimmt sind.

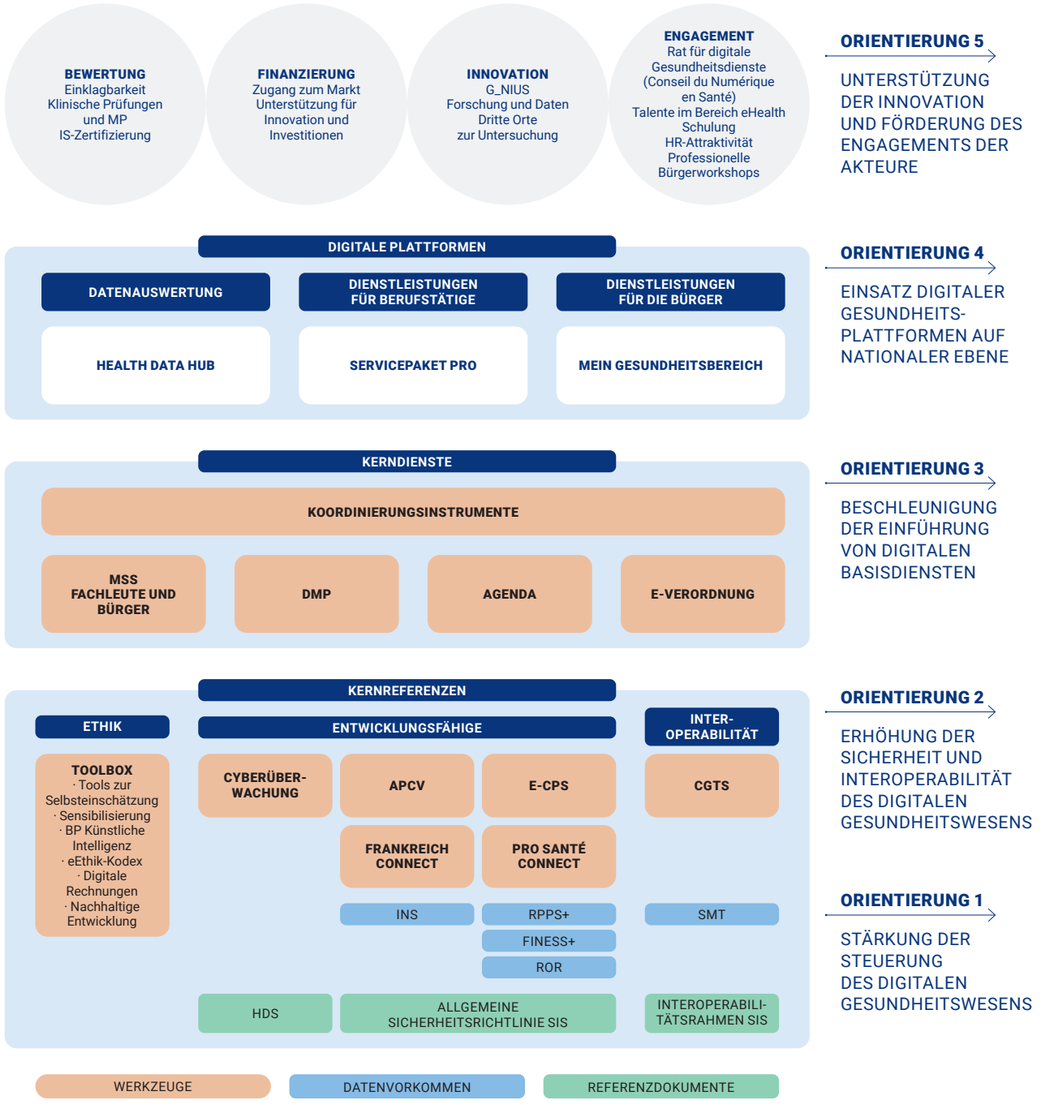
Die ANSSI ihrerseits erhielt im Rahmen des Plans France Relance einen Betrag von 136 Millionen Euro, um die Cybersicherheit des Staates zu stärken. Von dieser Summe werden 25 Millionen für die Cybersicherheit von Gesundheitseinrichtungen über die Durchführung von Audits im Rahmen des Parcours zur Cybersicherheit bereitgestellt. –

„Die großen Cyberangriffe der letzten Jahre haben die technischen und organisatorischen Schwachstellen der Informationssysteme von Gesundheitseinrichtungen ans Licht gebracht. Es hat eine Bewusstseinsbildung stattgefunden, auch auf höchster staatlicher Ebene.“

JACKY GRISEY – SECURITY OPERATIONS MANAGER FÜR GESUNDHEIT, ADVENS

VOM FRANZÖSISCHEN STAAT ZUR VERFÜGUNG GESTELLTE KOMPONENTEN DES BEZUGSRAHMENS

Dieses Schema fasst die Komponenten des Bezugsrahmens für eHealth in Frankreich zusammen, die von unten nach oben zu lesen sind: zuerst die Basisreferenzen, dann die Basisdienste und schließlich die digitalen Plattformen.



Quelle: Gesetzestext zur Digitalisierung im Gesundheitswesen des Ministeriums für Gesundheit und Soziales (Doctrine du numérique en santé, Ministère des Solidarités et de la Santé) (2021)



04.

Und in Zukunft?

Wie wird die Welt des Gesundheitswesens in den nächsten Jahren aussehen? Welche Auswirkung(en) auf ihre IT-Sicherheit? Eine vorausschauende Übung, die den Umfang der Aufgabe unterstreicht.

4.1 Pflegedauerzustand auf europäischer Ebene

Der Austausch von Gesundheitsdaten zwischen Angehörigen der Gesundheitsberufe, Forschern und der Industrie soll den Bürgern eine bessere Gesundheitsversorgung ermöglichen. Dies ist das Versprechen des European Health Data Space (EHDS), den die Europäische Kommission als den zukünftigen europäischen Raum für Gesundheitsdaten vorgestellt hat. Unter der Voraussetzung, dass Interpretierbarkeit mit der Sicherheit einhergeht.





Wenn die EHDS-Verordnung ohne große Änderungen verabschiedet wird, wird das Programm MeineGesundheit@EU (MyHealth@EU) in der Europäischen Union verpflichtend werden und jedem Einwohner die Möglichkeit geben, in jedem Mitgliedsstaat eine kontinuierliche Gesundheitsversorgung zu erhalten. Der Dienst wird in Frankreich über das Portal Sesali.fr bereits seit Juli 2021[30] eingesetzt.

Interoperabilität und Datensicherheit dürften daher auch in den kommenden Jahren ein zentrales Thema der europäischen Gesundheitspolitik sein. –

„Die Übernahme des EHDS wird die Einführung von MaSanté@EU beschleunigen. Das bedeutet, dass bis 2025 Gesundheitseinrichtungen in allen Mitgliedstaaten und Norwegen einfachen und sicheren Zugang zu den Allergien, Verordnungen und der Krankengeschichte jedes Patienten in ihrer Sprache haben werden, auch wenn der Patient in einem anderen europäischen Staat wohnt.“

DAMIAN KLIMAS – DOTLAW-PARTNER UND BEOBACHTER DES EHEALTH NETWORK

4.2 Präventivmedizin, datengestützte Steuerung des Krankenhauses

Versprechungen (und Herausforderungen) von Big Data in der Medizin

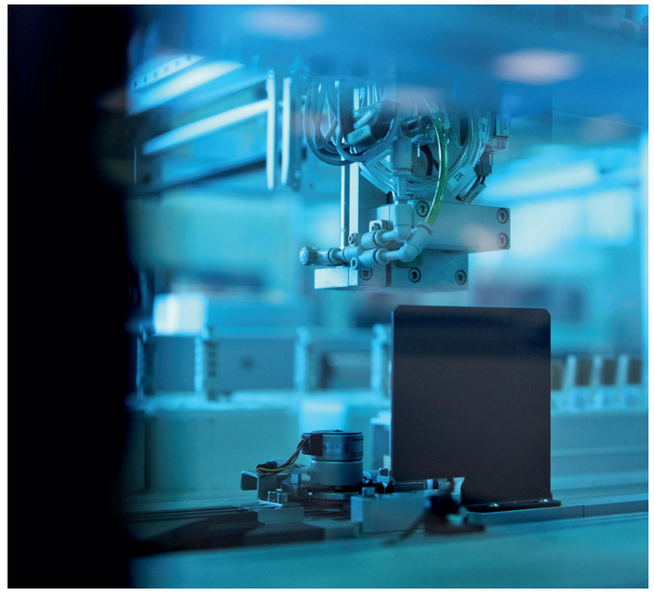
Während die Erfassung medizinischer Daten einer relativ einfachen Aufgabe gleicht, sind ihre Verarbeitung und Analyse komplexere Handlungen. Hinter dem Begriff der medizinischen Big Data verbergen sich die Versprechungen einer personalisierten und prädiktiven Medizin, die jedoch auch Anforderungen an die Cybersicherheit stellen.



Die Dimensionen werden umso strategischer sein, je vielversprechender die Aussichten sind, die mit der Nutzung großer Datenmengen verbunden sind. Viele Unternehmen setzen auf Machine Learning, um Pflegekräften Diagnosewerkzeuge zur Verfügung zu stellen. Dazu gehört das litauische Start-up-Unternehmen Ligence[31], das eine Software zur Analyse von Echokardiogrammen für Kardiologen bereitstellt. All diese Lösungen müssen die Frage der Cybersicherheit von Anfang an in ihre Konzeption einbeziehen.

„Wenn wir in Zukunft Krankheiten eher erkennen als behandeln wollen, müssen wir uns unbedingt mit Fragen der Governance von Gesundheitsdaten und damit verbundenen Sicherheitsmaßnahmen befassen. Daher besteht die Aufgabe des CISO in Gesundheitseinrichtungen darin, die Voraussetzungen für dieses Vertrauen in die Krankenhaus-IT bei den Fachkräften wie auch bei den Patienten zu schaffen.“

JEAN-SYLVAIN CHAVANNE – CISO DES UNIVERSITÄTSKLINIKUMS VON BREST



In Bezug auf Fragen der datengestützten Steuerung von Gesundheitsstrukturen sind einige Akteure wie der Fonds FHF[32] der Ansicht, dass das PMSI (Programme de Médicalisation des Systèmes d'Information) als erste landesweite medizinische Datenbank ausreichend strukturierte Informationen liefert, um einen Algorithmus für das Process Mining einzuspeisen. Eine Operation würde es letztlich ermöglichen, die Felddaten aus dem PMSI mit einem idealen Patientenverlauf zu vergleichen und die Behandlung Schritt für Schritt zu optimieren. –

„Viele Gesundheitseinrichtungen befinden sich noch in der Phase der Bestandsaufnahme und des Aufbaus einer Roadmap.“

CHARLES BLANC-ROLIN – PROJEKTLEITER FÜR DIGITALE SICHERHEIT IM GESUNDHEITSWESEN BEIM GCS EHEALTH PAYS DE LA LOIRE

WEITERFÜHRENDE INFORMATIONEN

DATA MANAGER
→ Daten zu haben ist gut; sie gemeinsam zu nutzen ist besser. Das Data Sharing ermöglicht es Forschern auf der ganzen Welt zwar, ihre Ressourcen zusammenzulegen, aber es muss äußerst strenge Vorschriften einhalten, die den Schutz und die Sicherheit von Patientendaten zum Ziel haben. Damit könnte ein eigenständiger Beruf eines Datenmanagers im Gesundheitswesen geschaffen werden.

4.3 Eine aufzubauende Zusammenarbeit

Mit der Integration von biomedizinischen und betrieblichen Systemen zur Gebäudeverwaltung wird die Abdeckung des SSI in den Einrichtungen immer größer und es wird zwingend notwendig, alle Akteure an einen Tisch zu bringen: IT, SSI und Biomedizin.



Die Entwicklung dieser Zusammenarbeit bedeutet, dass die Prioritäten und das Tempo der einzelnen Beteiligten miteinander in Einklang gebracht werden müssen: die IT-Abteilung, die schnell vorankommen will, die IT-Teams, die sich mehr oder weniger vom Sicherheitsaspekt betroffen fühlen (obwohl sie höhere Privilegien haben), oder auch die Biomediziner, die den Patienten keine Risiken zumuten wollen.

Die Zusammenarbeit wird sich auch auf Büroebene weiterentwickeln, wobei Cloud-Technologien immer mehr an Bedeutung gewinnen. Diese Entwicklung der Nutzung muss begleitet werden, da sie eine echte Herausforderung für die Einarbeitung darstellt.

Die Welt des Gesundheitswesens wird sich neuen Herausforderungen in Bezug auf Governance, Kooperation und Technik stellen müssen, um die Sicherheit der Patienten in einer zunehmend digitalen Umgebung zu gewährleisten.

„Je mehr man sich in Richtung Technologie bewegt, desto mehr muss man die SSI berücksichtigen. Auch wenn die Beziehungen zu den Fachbereichen in der Vergangenheit oft kompliziert waren, müssen CISOs im Gesundheitswesen hartnäckig bleiben, um den anderen Funktionen klar zu machen, dass unsere gemeinsame Herausforderung Vertrauen ist.“

JACQUES LABIDURIE – CISO UNIKLINIKUM LIMOGES

„Das Verständnis der technischen und technologischen Implikationen wird zu einer Pflicht, insbesondere wenn wir jenseits des Atlantiks beobachten, wie unmöglich es ist, den Verbleib der Gesundheitsdaten von Frauen in einem Kontext zu beherrschen, in dem Abtreibung unter Strafe gestellt wird. [...] Mehr denn je liegt es an uns allen, zum Aufbau eines intelligenten und widerstandsfähigen Systems beizutragen, das die Grundrechte und Freiheiten respektiert.“

RAYNA STAMBOLIYSKA – EXPERTIN FÜR DIGITALE DIPLOMATIE, CYBERSICHERHEITSEXPERTIN UND UNABHÄNGIGES MITGLIED DER ENISA-ARBEITSGRUPPE FÜR AUFKOMMENDE UND ZUKÜNFTIGE BEDROHUNGEN

Diese Herausforderungen dürfen jedoch nicht dazu führen, dass der traditionelle Auftrag des Sektors, öffentliche Dienstleistungen zu erbringen und Menschen zu betreuen, in den Hintergrund rückt: es muss möglich sein, „*das Menschliche wieder in die Maschine zu bringen*“, wie es die Rechtsverteidigerin Claire Hédon[33] im Juli 2022 im Gespräch mit France Inter forderte. –

„Nur die Zukunft wird zeigen, ob es dem Gesundheitssektor gelingt, das Cyberrisiko einzudämmen. Aber es ist davon auszugehen, dass die rasante Digitalisierung und der Kompetenzzuwachs der Ransomware-Gruppen es nicht leichter machen werden, die technischen Schwachstellen zu beseitigen.“

JACKY GRISEY – SECURITY OPERATIONS MANAGER FÜR GESUNDHEIT ADVENS

DIE ZUKUNFT DER CYBERSICHERHEIT IM GESUNDHEITSWESEN

INTERVIEW

JACKY GRISEY – SECURITY OPERATIONS MANAGER FÜR GESUNDHEIT ADVENS

„Die Zusammenarbeit im Rahmen eines gemanagten SOC trägt zu einer Form der kollektiven Intelligenz bei, die für den Gesundheitssektor charakteristisch und vorteilhaft ist.“



Die Erwartungen der Industrie an die betriebliche Cybersicherheit betreffen die Automatisierung. Wir setzen bereits Automatisierung bei der Arbeit mit unseren Sicherheitsanalysen ein und können so die Erkennungszeiten optimieren. Es gibt hohe Herausforderungen an eine Vertiefung, da das Ziel darin besteht, die Reaktionszeit so weit wie möglich zu verkürzen. Aus Sicht der Einrichtung ist der erste Schritt der Automatisierung die Delegation der Antwort an den Partner innerhalb eines bestimmten operativen Rahmens. Dann können wir die automatische Ausführung „einfacher“ Reaktionen in Betracht ziehen: Blockierung von IP-Adressen, Blacklists von E-Mail-Domainnamen, Benutzerkonten usw., was möglicherweise auch ein Umdenken der IT-Teams erfordert.

Eine weitere Entwicklung betrifft den biomedizinischen Bereich, insbesondere das Management von Schwachstellen und die Erkennung von Vorfällen durch das SOC. Wir haben einige Kunden, die mit dem Einsatz von dedizierten Sonden begonnen haben, wodurch die Erkennungsfläche erweitert wird. Die Akteure im Bereich der Informationssysteme sind sich in einem Punkt einig: Der Bereich ist eine Grauzone!

Letztendlich wird nur die Zukunft zeigen, ob es dem Gesundheitssektor gelingt, das Cyberrisiko einzudämmen. Im Moment muss man zwischen der technischen Schuld, der Digitalisierung der Berufe, die immer noch mit hoher Geschwindigkeit voranschreitet, und der Industrialisierung der Gruppen von Cyberangreifern jonglieren. Aber die gegenseitige Nutzung im Rahmen eines gemanagten SOC, d. h. die Tatsache, dass die einen von dem profitieren, was für die anderen getan wird (entdeckte Schwachstellen, Hinweise auf Kompromittierungen, Erkennungsregeln oder sogar Integrationsbesonderheiten), trägt zu einer Form der kollektiven Intelligenz bei, die für alle von Vorteil ist. –

QUELLEN UND ANHÄNGE

[1]CERT Santé
[2]https://www.techtarget.com/searchsecurity/news/252521771/Healthcare-breaches-on-the-rise
[3]https://health-trends.co.uk/wi-ga-la-hospitals-confirm-recent-healthcare-cyberattacks/
[4]https://health-trends.co.uk/wi-ga-la-hospitals-confirm-recent-healthcare-cyberattacks/
[5]https://www.cbc.ca/news/canada/newfoundland-labrador/nl-cyberattack-update-march-29-22-1.6401700
[6]lefigaro.fr/secteur/high-tech/covid-19-des-cyberattaques-contre-la-chaine-logistique-des-vaccins-20201203
[7]https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/
[8]https://www.usine-digitale.fr/article/le-gouvernement-injecte-20-millions-d-euros-dans-l-anssi-pour-renforcer-son-accompagnement-des-hopitaux.N2036952
[9]https://www.ssi.gouv.fr/actualite/lanssj-et-le-bsi-alertent-sur-le-niveau-de-la-menace-cyber-en-france-et-en-allemagne-dans-le-contexte-de-la-crise-sanitaire/
[10]https://www.psychiaclic.fr/
[11]https://www.dsih.fr/article/4790/effacer-une-donnee-medicale-d-un-patient-vraiment.html
[12]https://www.france24.com/fr/%C3%A9co-tech/20220705-fuite-de-donn%C3%A9es-il-affirme-mettre-en-vente-la-vie-priv%C3%A9e-des-deux-tiers-des-chinois
[13]https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites
[14]https://www.ibm.com/security/data-breach
[15]https://www.stormshield.com/fr/webinar-sante-face-aux-cybermenaces/
https://www.dsih.fr/article/4790/effacer-une-donnee-medicale-d-un-patient-vraiment.html
[16]https://www.leparisien.fr/faits-divers/coronavirus-le-milieu-medical-nouvelle-cible-des-arnaques-au-president-01-04-2020-8292336.php
[18]https://www.lemondeinformatique.fr/actualites/lire-dedalus-biologie-ecope-d-une-amende-d-1-5-meteuro-par-la-cnil-86527.html
[19]https://www.lemonde.fr/pixels/article/2020/10/27/la-finlande-secouee-par-le-piratage-de-milliers-de-dossiers-de-patients-en-psychotherapie_6057561_4408996.html
[20]https://esante.gouv.fr/sites/default/files/media_entity/documents/mss_ans_rapport_public_observatoire_signalements_issis_2021_vf.pdf
[21]https://www.cyberveille-sante.gouv.fr/sites/default/files/documents/documents-secteur-sante/ACSS_Sensibilisation_s%C3%A9curit%C3%A9_mot_passe.pdf
[22]https://www.esante-centre.fr/portail_pro/services-d-accompagnement/ssi-securite-des-systemes-d-information-131-111.html
[23]https://www.lemagit.fr/etude/Cybersecurite-du-systeme-de-sante-beaucoup-reste-a-faire
[24]https://esante.gouv.fr/sites/default/files/media_entity/documents/webinaires_ie-usagers_2022-05-09_v2.pdf
[25]https://health.ec.europa.eu/publications/proposal-regulation-european-health-data-space_en
[26]https://esante.gouv.fr/actualites/lespace-europeen-des-donnees-de-sante-cest-parti
[27]https://solidarites-sante.gouv.fr/IMG/pdf/190425_dossier_presse_masante2022_ok.pdf
[28]https://esante.gouv.fr/sites/default/files/media_entity/documents/Doctrine_du_numerique_en%20santé_Version%202021_Février%2022_VF.pdf
[29]https://sante-achat.info/performance/charlotte-drapeau-anssi-le-secteur-de-la-sante-est-une-cible-particulierement-vulnerable/
[30]https://sesali.fr/ncpehfr-gui/index.html
[31]https://www.ligence.io
[32]https://www.fondsfhf.org
[33]https://www.francetvinfo.fr/societe/services-publics-il-n-est-pas-possible-d-imposer-a-tout-le-monde-d-avoir-un-smartphone-alerte-la-defenseure-des-droits_5238622.html

DIE EUROPÄISCHE WAHL FÜR CYBERSICHERHEIT

WWW.STORMSHIELD.COM

Jegliche Verbreitung, Vervielfältigung oder Präsentation dieses Whitepapers, auch auszugsweise, auf einem beliebigen Datenträger zu anderen Zwecken als zur privaten Nutzung ist untersagt und kann zivil- und strafrechtliche Folgen für Personen nach sich ziehen, welche dieses Verbot missachten.
Copyright © 2022 Stormshield

STORMSHIELD