

Krankenhaus-IT

JOURNAL

Fakten und Perspektiven der IT im Gesundheitswesen

Kritische Infrastruktur Krankenhaus

**Mit Marktübersicht
Sicherheits-Software**

PRO-KLINIK

KRANKENHAUSBERATUNG



WIR MACHEN KLINIKEN ERFOLGREICHER !

Digitalisierungs-Strategien für Krankenhäuser

Elektronische Patientenakte und digitale Archivierung

Optimierung vorhandener IT-Lösungen

Beschaffung neuer IT-Systeme

www.pro-klinik.de

Kritisch für Geschäftsführung bis Pflegekraft

Die Bedrohungslage für Krankenhäuser hat sich in Sachen Cybersicherheit in den letzten Jahren verschärft. Das Umfeld für Cyber Risiken wird in Zukunft nicht einfacher. Daher bleibt das Thema „IT-Sicherheit“ hochaktuell. Es ist nicht als alleinige Aufgabe der IT-Abteilung zu verstehen. Informationssicherheit liegt im Verantwortungsbereich der Geschäftsführung. Das Krankenhaus-IT Journal erörtert in der vorliegenden Ausgabe Digitalisierung, Sicherheitssoftware und kritische Infrastrukturen.

Kliniken mit ihrer kritischen Infrastruktur (KRITIS) sehen sich einer Reihe von Herausforderungen gegenüber. Cyber-Betriebsunterbrechungen werden kostspieliger, Ransomware-Angriffe nehmen weiter zu, Mega-Datenlecks haben schwerwiegende Folgen aufgrund der verschärften Regulierung und mehr Gerichtsprozessen. Hier gilt es gegenzusteuern. Krankenhäuser sind für die Security-Thematik zunehmend sensibilisiert, auch der Gesetzgeber ist seit einigen Jahren aktiv, um die IT-Sicherheit in Krankenhäusern zu erhöhen. Durch die staatlich finanzierte Digitalisierung im Gesundheitswesen steigen auch die Anforderungen an die Absicherung der eingesetzten Systeme und Prozesse. Krankenhäuser sind seitens des BSI mit besonderen regulatorischen Vorgaben konfrontiert.

Cyber-Angriffe richten sich nicht nur gegen die großen KRITIS-Krankenhäuser, die ihre Vorbeugemaßnahmen regelmäßig gegenüber dem BSI nachweisen müssen. Gefahr droht im gleichen Maß allen Arten von Krankenhäusern, unabhängig von ihrer Größe: ein „zu klein“ gibt es in Zeiten von einfach verwendbarer, baukastenartiger Angriffssoftware und Internetdatenbanken, in denen schlecht gesicherte Systeme einfach auffindbar sind, nicht. Darauf hat auch der Bundesgesetzgeber mit dem §75c Patientendatenschutzgesetz (PDSG) reagiert. Es verpflichtet auch kleine Krankenhäuser, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zum Schutz ihrer IT-Systeme zu treffen.

Um den Herausforderungen effizient zu begegnen, ist es erforderlich, wirtschaftliche, umsetzbare und hochsichere Konzepte prozesskonform und für die Mitarbeiter nachvollziehbar einzuführen. Das erfordert ganzheitliche Lösungsansätze von der Analyse bis hin zum Betrieb. Daher bleibt KRITIS wohl für alle Krankenhäuser ein umfassender Lernprozess.

Ist es nicht Zeit, Erfahrungen über die bessere Absicherung der kritischen IT-Dienstleistungen im Klinikumfeld auszutauschen? Teilen wir doch praktische Tipps, etwa wie Datenverluste oder Systemausfälle durch Angriffe von außen, aber auch durch interne Schwachstellen, vermieden werden können.

Herzliche Grüße

Ihr Krankenhaus-IT Journal Team



Wolf-Dietrich Lorenz



Dagmar Finlayson



Kim Wehrs

Impressum

Antares Computer Verlag GmbH,
Gießener Straße 4, D - 63128 Dietzenbach
E-Mail: info@krankenhaus-it.de, www.krankenhaus-it.de
Verlagsleitung und Herausgeber **Kim Wehrs (kw)**,
stellvert. **Kai Wehrs (kaw)**. Tel.: 0 60 74/25 35 8, Fax: 0 60 74/2 47 86
Redaktion, Chefredakteurin **Dagmar Finlayson (df)** (verantwortlich)
Mitglied der Chefredaktion **Wolf-Dietrich Lorenz**, Freier Journalist **Ralf Buchholz**, **Michael Reiter**
Redaktionelle Mitarbeit **Kai Wehrs** (Fotos und Onlineredaktion) (**kaw**)
Anzeigen + Verkauf **Kim Wehrs**, D - 63128 Dietzenbach, Tel.: 0 60 74/2 53 58 (**kaw**)
Layout, Grafik, & Satz **Nebil Abdulgadir**
Lektorat **Maïke Buchholz**
Druck und Versand: Westdeutsche Verlags- und Druckerei GmbH,
Mörfelden-Walldorf
Erscheinungsweise 6 x jährlich Einzelpreis EUR 12,00 - zzgl. EUR 1,80 Versand
Abonnement: 60,00 zzgl. EUR 11,00 Versand jährlich.
Verbandsorgan des Bundesverbandes der Krankenhaus - IT Leiterinnen/Leiter e. V.
Mitglied im Börsenverein des Deutschen Buchhandels (VK Nr. 14815 Verlag, 32320 Buchhandel)



Fotonachweis

Adobe Stock:

1, 20, 30, 32, 34, 36, 38, 42, 62, 64, 78, 94

Alle Rechte liegen beim Verlag. Insbesondere Vervielfältigung, Mikroskopie und Einspeicherung in elektronische Datenbanken, sowie Übersetzung bedürfen der Genehmigung des Verlages. Die Autoren-Beiträge geben die Meinung des Autors, nicht in jedem Fall auch die Meinung des Verlages wieder. Eine Haftung für die Richtigkeit und Vollständigkeit der Beiträge und zitierten Quellen wird nicht übernommen. „Aus dem Markt“ abgedruckten Beiträgen handelt es sich um Industrieinformationen.

6

Titelstory

Kritische Infrastruktur Krankenhaus 6

Titelthema IT-Sicherheit

Viren, Cyberangriffe und drohender Blackout 12

IT-Sicherheit wird zur Pflichtaufgabe für alle Krankenhäuser 14

Datenschutz ist kein Silo: Warum sich Krankenhäuser mit der DSGVO schwer tun 18

DSGVO-Dauerdruck: Aufwand, Innovationsbremse, Rechtsunsicherheit 20

IT-Sicherheit ohne ISMS ist wie Therapie ohne Behandlungsleitlinie 22

IT-Sicherheit im Krankenhaus: Ab 2022 auch für kleinere Kliniken verpflichtend 24

Nutzerverständnis für digitale Sicherheit stärken 26

Cyber Security im Krankenhaus – auch eine Frage des Managements 30

Das Krankenhaus aus der externen Sicht eines Hackers – ein Lagebild 32

IT für hochsichere Patientenversorgung 34

IT-Sicherheit in der Medizin: Auch an die Zusammenarbeit denken 36

Sicherheitsprioritäten für hybrides Arbeiten: konsolidierte Cloud-Dienste verringern Angriffsflächen 38

Cloud Security 2021: Datendiebstahl gefürchtet – Datensicherheit geschätzt 39

Schieflage bei präventiver Cyberabwehr 40

Hackerangriff: Wie die Universitätsklinik Düsseldorf mitten in der Krise die digitale Kommunikation umstellt 42

Marktübersicht Sicherheits-Software

Menschliche Firewall durch simulierte Phishing-Tests stärken 44

Portfolio-Bundle unterstützt bei der sicheren Digitalisierung der Healthcare-Branche 46

Krankenhäuser schneiden bei der IT-Sicherheit im KRITIS-Branchenvergleich schlecht ab 48

Praxistaugliche IT-Notfallplanung 50

Der ClearPass Policy Manager von Aruba 52

Medigate unterstützt Ihre KRITIS Strategie 53

Wie sich das Gesundheitswesen gegen Cyberangriffe wappnen kann 54

Schutz vor Cyberstürmen 56



KRITIS

Die Sicherheit steht im Fokus	60
5G-Einsatz in Kritischen Infrastrukturen (KRITIS) – Wunsch und Wirklichkeit	62
Handlungsfeld IT-Infrastruktur im Krankenhaus	64
Krisenmanagement in Unternehmen: 9-Punkte-Checkliste	66
IoT-Geräte als Einfallstor: Healthcare-IT-Sicherheit gefährdet	67
IT-Sicherheit und IT-Risikoanalyse: Handlungsbedarf erkennen	68
Cyberfälle: Interne Fehler sind häufig die Auslöser	70

IT-Management

Digitalisierung und Disruption als Nagelprobe für das IT-Management	72
IT-Kooperation Charité/Vivantes: Digitaler Austausch von Behandlungsdokumenten als Teil der eHealth-Strategie	75
IsiK: Standards für Schnittstellen in Krankenhäusern	77

KH-IT Verband

KH-IT: Fels in der Brandung und im Wandel	78
KH-IT-Herbsttagung 2021: Abschied von Compliance as-we-know-it	80

Gesundheitspolitik

Patientenzentriertes Ökosystem – die Zukunft der Gesundheitsversorgung	86
Tech-Unternehmen und die digitale Zukunft der Medizin	88
Gesundheitswirtschaft ist zentrale Branche für Wirtschaftsstandort Deutschland	90
Fusionen verändern die Gesundheitsversorgung	91

Veranstaltungen

Health IT Talk: Spannungsfeld Cyberfront	94
Der 13. KRITISche Stammtisch	97

ENTSCHEIDERFABRIK

15 Jahre ENTSCHEIDERFABRIK – Lösungen für einen reibungslosen Geschäftsprozess	100
---	-----

Aus dem Markt

Mit Wachstum an die Spitze	102
Automatisierte Warenwirtschaft mit RFID – jetzt ganz einfach!	104
Die Reise der Daten	106
Die Architektur der IT im Gesundheitswesen neu überdenken	108
Patientenportal Plus	112
Snom: Wenn das IP-Telefon für lebensrettende Zeitersparnis sorgt	114

Kritische Infrastruktur Krankenhaus



Die Gesundheitswirtschaft ist ein wichtiger Wachstumsfaktor für Gesellschaft und Gesamtwirtschaft. Für die erfolgreiche Weiterentwicklung der Gesundheitsversorgung sind Digitalisierung und deren stabile Sicherheit zentrale Voraussetzungen. Dazu braucht eine komplexe kritische Infrastruktur kompetente Verantwortlichkeiten für die verschiedenen Stakeholder-Gruppen im Krankenhausbetrieb. Fehlt es daran, fehlt es auch an Vertrauen. Dann könnte sich die Perspektive der Krankenhäuser, aber ebenso des IT-Verantwortlichen dramatisch verschlechtern. Von Wolf-Dietrich Lorenz

Die Gesundheitswirtschaft ist und bleibt eine der wichtigsten Branchen für die deutsche Volkswirtschaft. Im Jahr 2020 erwirtschaftete sie 364 Milliarden Euro und damit zwölf Prozent der deutschen Bruttowertschöpfung. Gerechnet auf einen Tag hat die Gesundheitswirtschaft im Jahr 2020 rund 1 Milliarde Euro Bruttowertschöpfung geschaffen. Jeder sechste Erwerbstätige arbeitet in der Gesundheitswirtschaft, insgesamt sind das 7,4 Millionen Menschen.

Doch Gefahr ist im Verzug. Entsprechend dem Bundesministerium für Gesundheit (BMG) ist "für die erfolgreiche Weiterentwicklung unserer Gesundheitsversorgung das Vorantreiben der Digitalisierung die zentrale Voraussetzung. Um im Kampf gegen modernste Cyberangriffe gewappnet zu sein, sollten Maßnahmen über den Standardschutz, wie herkömmliche IT-Sicherheitslösungen, regelmäßige Updates und Patches hinausgehen."

Brisante Herausforderungen für Krankenhäuser im Kontext von IT-Sicherheit wachsen an. Die Welt kämpft derzeit gegen zwei Arten von Viren: Covid-19 und Computerviren. Der Gesundheitssektor ist davon am stärksten betroffen. Er ist eines der Hauptziele besonders von Cyberspionage und Ransomware-Angriffen. So musste das Gesundheitswesen 2020 im Vergleich zum Vorjahr weltweit einen Anstieg der Angriffe um 200 Prozent verzeichnen. Allein von Oktober 2020 bis Januar 2021 betrug die Zunahme aufgedeckter Cyberattacken auf den Gesundheitssektor rund 45 Prozent.

Schutz Kritischer Infrastrukturen

Der Schutz Kritischer Infrastrukturen steht im Zentrum der gemeinsamen Aktivitäten von Staat und Wirtschaft. So formuliert es das Bundesministerium des Innern, für Bau und Heimat zur „Cybersicherheitsstrategie für Deutschland 2021“ in den „Leitlinien der Cyber-Sicherheitsstrategie“. Angesichts der Vernetzung der Systeme kommt dabei dem Schutz der IT-Kritischer Infrastrukturen besondere Bedeutung zu. Dies ist eine ressortgemeinsame und gesamtstaatliche Aufgabe der Cyber-Abwehr und -Verteidigung, da innere und äußere Sicherheit im Bereich Cyber eng zusammenfallen. Bei der Umsetzung der mit dem IT-Sicherheitsgesetz getroffenen Vorgaben müssen Staat und Wirtschaft (unter anderem im Rahmen der öffentlich-privaten Partnerschaft des UP KRITIS) auf allen Ebenen eng zusammenarbeiten und einen vertrauensvollen Informationsaustausch etablieren. Mindeststandards und Meldewege werden gemeinsam mit der Wirtschaft erarbeitet, umgesetzt und fortentwickelt. Zudem wird die Ausweitung solcher Präventions- und Reaktionspflichten auch auf andere Unternehmen von hoher gesellschaftlicher Relevanz geprüft.

Verschärfte Anforderungen für KRITIS

Krankenhäuser zählen ab einer gewissen Größe zu den Kritischen Infrastrukturen (KRITIS) des Landes. Das IT-Sicherheitsgesetz verlangt angemessene Schutzmaßnahmen. Es verpflichtet KRITIS-Betreiber, technische und organisatorische Maßnahmen zu ergreifen, um ihre IT-Systeme und IT-Prozesse nach dem „Stand der Technik“ abzusichern. Entsprechende Nachweise über den „Stand der Technik“ sind alle zwei Jahre dem BSI (Bundesamt für die Sicherheit in der Informationstechnik) gegenüber zu erbringen. Zurecht verschärft angesichts wachsender Cyberbedrohungen und steigender Angriffszahlen der Gesetzgeber die Anforderungen für KRITIS-Einrichtungen und nimmt auch Nicht-KRITIS-Organisationen stärker in die Pflicht. Ab dem 1. Januar 2022 sind alle Krankenhäuser in Deutschland verpflichtet, angemessene Schutzmaßnahmen zur IT-Sicherheit zu treffen.

Jetzt geht es darum, die IT-Sicherheit der für die Patientenversorgung wichtigen Systeme und Prozesse zu gewährleisten. Zusammen mit dem Investitionsbedarf stellt sie insgesamt hohe Anforderungen an den Betrieb und das dafür zuständige Personal in den Krankenhäusern. Die Anforderungen wachsen dabei mit dem zunehmenden Grad an Digitalisierung stetig an. Dabei geht es um mehr als die Umsetzung konkreter technischer Sicherheitsmaßnahmen – Informationssicherheit, die neben der IT-Sicherheit auch Datenschutzanforderungen berücksichtigt, muss auf allen Ebenen wahrgenommen, umgesetzt und in den Prozessen gelebt werden. Dafür müssen die notwendigen Ressourcen, insbesondere die personellen und finanziellen Mittel für die Umsetzung entsprechender Sicherheitsmaßnahmen, bereitstehen. Mit dem Krankenhauszukunftsgesetz KHZG werden wichtige Impulse gesetzt. Eine dauerhafte Finanzierung von IT-Sicherheit im Krankenhaus ist damit aber keinesfalls gewährleistet.



Catharina Richter, globale Leiterin des Allianz Cyber Kompetenzzentrums



Dr. Klaus Rummel, Facharzt für Radiologie, medizinische Informatik

Empfehlung – kontinuierlicher Verbesserungsprozess

Der Leiter Branchenarbeitskreis im UP KRITIS Lars Forchheim rät zum Schutz Kritischer Infrastrukturen, in den kontinuierlichen Verbesserungsprozess einzusteigen, in dem man eine IST-Aufnahme durchführt. Das Ergebnis sollte die Geschäftsleitung zusammen mit allen Beteiligten betrachten und danach gemeinsame Maßnahmen ableiten. Zur Umsetzung empfiehlt sich ein Informationssicherheitsteam zu bilden. Den Vorsitz sollte von der Geschäftsleitung erfolgen und Teilnehmer sind Informationssicherheitsbeauftragter, Datenschutz, Leiter IT, Leiter Haustechnik und Leiter Medizintechnik. Je nach Organisation empfiehlt sich Leiter QM, Innen Revision etc. „Es gibt zwar keine Audit-Pflicht, jedoch sollte man spätestens aller zwei Jahre wieder einen Blick von außen auf diese Organisation werfen. Aus meiner Sicht werden spätestens die Wirtschaftsprüfer die Organisation und Maßnahmen sich immer wieder anschauen.“

IT-Nutzer als menschliche Firewall

Das KHZG bringt Geld und zielt auf eine Verbesserung der Sicherheitslage ab. Krankenhäuser sind dazu aufgerufen, nicht nur ihre IT-Systeme aktuell zu halten, sondern auch das eigene IT-Sicherheitsbewusstsein zu steigern – von der Geschäftsführung bis hin zum Anwender.

Notfallpläne, Notfallübungen, Risikomanagement und die Awareness von Anwendern und Administratoren zählen weiterhin als wichtige Säulen für den sicheren IT-Betrieb. Dr. Klaus Rummel, Facharzt für Radiologie, medizinische Informatik, merkt realistisch an, neben den technischen Sicherheitsrisiken sei der Anwender ein wesentliches Ziel von Attacken, und damit Einfallstor für Schadsoftware. „Mit zunehmend verteilten Arbeitsplätzen und einer technisch und inhaltlich deutlichen Verbreiterung der Angriffsfläche wird es wichtiger,

IT-Nutzern ihre Rolle als eine Art menschlicher Firewall näherzubringen.“ Niemals vorher gab es so viele Berührungspunkte zwischen der beruflichen Tätigkeit und dem privaten Bereich, die eine Stärkung des verhaltensbasierten Ansatzes erfordern. „Die Anleitung von Mitarbeitern und der Erfahrungsaustausch mit den IT-Nutzern sollten den Raum bekommen, der dem Risiko entspricht“, schlussfolgert Klaus Rummel.

Dazu beobachtet Catharina Richter, globale Leiterin des Allianz Cyber Kompetenzzentrums, nämlich mit Sorge: „Obwohl Cyberkriminalität die Schlagzeilen beherrscht, sind es vielfach alltägliche Systemausfälle und menschliche Fehler, die Unternehmen große Probleme bereiten, selbst wenn ihre finanziellen Auswirkungen meistens nicht so gravierend sind. Arbeitgeber und Arbeitnehmer müssen deshalb zusammenarbeiten, um das Bewusstsein für diese Gefahren zu schärfen und die Cyber-Resilienz zu erhöhen.“



Lars Forchheim, Leiter Branchenarbeitskreis im UP KRITIS

Fehlerquellen und kritische Situationen

Der "Faktor Mensch" spielt beim Schutz der Digitalnetze sowie der sensiblen Daten eine wichtige Rolle, um Sicherheitsvorfälle wie Ransomware oder Betrugsversuche zu vermeiden. Neben Tipps zur Konfiguration und Nutzung von geschäftlichen E-Mails und der Software, lohnt es sich für neue wie langjährige Mitarbeiterinnen und Mitarbeiter sich mit der Sicherheit beim digitalen Arbeiten zu befassen.

Durch ihre Komplexität sind Krankenhäuser in besonderem Maße gefordert, Fehlerquellen und kritische Situationen zu analysieren, zu beseitigen und zu deren Vermeidung entsprechende Präventionsmaßnahmen durchzuführen. Zentrale Voraussetzung für das erfolgreiche Implementieren solcher Maßnahmen ist eine gelebte, proaktive Sicherheitskultur. Übergreifende Fehlermeldesysteme haben sich nicht nur in Deutschland, sondern auch international bewährt und sind vom

Gesetzgeber mittlerweile als integrativer Bestandteil des Qualitätsmanagements in Gesundheitseinrichtungen anerkannt. Sie haben zwar unterschiedliche thematische und regionale Schwerpunkte, aber alle bieten eine Chance für Krankenhäuser, einerseits ihre Erkenntnisse aus eigenen interessanten und relevanten Fällen der Öffentlichkeit zur Verfügung zu stellen und andererseits durch das große Lernpotenzial, das in einer solchen Datenbank mit aufbereiteten Fällen und Lösungsansätzen steckt, Fehler nicht selbst zu machen.

Licht am Horizont

Das jährliche Krankenhaus-Rating vom RWI – Leibniz-Institut für Wirtschaftsforschung e. V. ist in der Fachöffentlichkeit etabliert. In einem Szenario „Neustart“ wird vom RWI angenommen, dass das Leistungsvolumen nicht mehr das Vorkrisenniveau von 2019 erreichen wird, sondern auf dem Niveau von 2021 stagniert und bis 2030 nur noch marginal ansteigt, sodass die stationäre Fallzahl im Jahr 2030 rund 6 Prozent unter dem Niveau von 2019 liegt. Kombiniert mit einer weiter sinkenden Verweildauer würde die Auslastung der stationären Kapazitäten infolgedessen stark sinken. In diesem düsteren Szenario würde sich die wirtschaftliche Lage der Krankenhäuser dramatisch verschlechtern.

Doch da scheint Licht am Horizont: Eigentlich ist Grund zur Freude vorhanden. „Durch das Krankenhauszukunfts-gesetz ist nun endlich viel mehr Geld für die Krankenhaus-IT im Spiel, zumindest in einem ersten Wurf, das was wir doch immer wollten und wonach wir IT-Verantwortliche geschrien haben“, meint Horst-Dieter Beha, Vorsitzender Bundesverband der Krankenhaus IT-Leiterinnen/Leiter KH-IT. „Endlich wird die IT-Welt auch per Gesetz immer sicherer, die Sicherheitsgesetze für Kritische Infrastrukturen werden ständig erweitert und verfeinert, auch das eigentlich ein Kernanliegen unter anderem der Krankenhaus-IT schon seit langer Zeit.“ Das sind gute Nachrichten. „Vieles, was wir jahrelang höchstens ansatzweise zu träumen wagten, wird nun vielleicht nach und nach Realität.“



Jörg Asma, Partner, PricewaterhouseCoopers WPG GmbH



**Dr. Benedict Gross, Senior Manager,
PricewaterhouseCoopers WPG GmbH**

Zukunft von Organisation und Position

Technische Lösungen ja, sie allein reichen jedoch nicht aus, um die Informationssicherheit strukturell zu gewährleisten. Genauso wichtig ist es, innerhalb der Organisation Verantwortung und Zusammenarbeit sicherzustellen. Ein Bericht des BSI zur Lage der IT-Sicherheit in Deutschland sieht besonders in diesem Punkt noch Nachholbedarf und fordert Betreiber dazu auf, auch das IT-Risikomanagement in ihr Business Continuity Management (BCM) zu überführen.

Doch dafür fehlt den Häusern vielfach noch eine übergreifende Digitalstrategie. Das macht sie verwundbar für Angriffe von außen. „Wir empfehlen daher die Arbeit mit einem Enterprise-Security-Architekturmodell, das alle Schnittstellen aus technologischer und prozessualer Sicht schematisch abbildet“, raten Jörg Asma und Benedict Gross sind bei PwC Deutschland Ansprechpartner für die Themen Digitalisierung und Sicherheit im Krankenhaus. Ein solches Modell ist die Grundlage für Informationssicherheit und erhöht die Widerstandsfähigkeit einer Organisation. Es stellt sicher, dass ein Krankenhaus seine Unternehmensziele erreichen kann – ein Grund, warum die Sicherheitsarchitektur im Management angesiedelt ist. Diese komplexe IT-Sicherheits-Architektur braucht eine klare Verantwortlichkeit. Im Idealfall ist sie beim Chief Information Security Officer (CISO) angesiedelt oder, in Kliniken, die sich schon deutlicher für die digitale Zukunft aufgestellt haben, beim Chief Information Officer (CIO). Diese Verantwortlichen bündeln die Anforderungen, die sich aus den verschiedenen Stakeholder-Gruppen im Krankenhausbetrieb ergeben.

Diesen Aspekt greift Dr. Uwe Günther auf und vertieft ihn. Er betont die erweiterte Kompetenz des IT-Managements zur Sicherung der Zukunftsfähigkeit. „Weg vom EDV-Leiter, hin zum IT-Manager und strategischen Partner: Das ist die Maxime für die IT-Verantwortlichen, um die Zukunftsfähigkeit der Organisation und auch der eigenen Position zu sichern.“ Für IT-Verantwortliche bringt es der Partner Curacon GmbH Wirtschaftsprüfungsgesellschaft sowie Geschäftsführer Sanovis GmbH auf den Punkt: „Man muss den Anforderungen eines Chief Innovation Officers und des Chief Digital Officers gerecht werden, um nicht eines Tages in der Bedeutungslosigkeit zu verschwinden.“

www.kritis.bund.de



**Dr. Uwe Günther, Partner Curacon GmbH
Wirtschaftsprüfungsgesellschaft, Geschäftsführer Sanovis GmbH**



**Horst-Dieter Beha, Vorsitzender Bundesverband der
Krankenhaus IT-Leiterinnen/Leiter KH-IT**



DIE ZUKUNFT DER DIGITALEN KLINIK.

Das cobas® pulse System.

**Die multifunktionale Lösung für
eine effiziente Patientenversorgung
durch Ärzte und Pflegekräfte.**

Innovatives Blutzuckermanagement.
Mit Apps erweiterbar.
Voll vernetzt. Mobil. Smart.

**Jetzt mehr erfahren
und Termin vereinbaren:
www. Roche.de/cobas-pulse**

Das cobas® pulse System wird bei Launch als Medizinprodukt in den Markt gebracht und mit dem CE-Kennzeichen versehen. Finales Produkt kann von der aktuellen Darstellung abweichen.

COBAS ist eine Marke von Roche.
Roche Diagnostics Deutschland GmbH, Sandhofer Straße 116, 68305 Mannheim
© 2021 Roche Diagnostics. Alle Rechte vorbehalten. www. Roche.de

cobas®

Viren, Cyberangriffe und drohender Blackout

Für die Krankenhäuser waren die vergangenen 18 Monate in vielerlei Hinsicht eine sehr bewegte Zeit. Nach überwiegend erfreulicher Finanzsituation aufgrund großzügig ausgelegter Coronahilfen im vergangenen Jahr, tun sich dieses Jahr vielerorts erstmalig Finanzierungslücken auf, basierend auf anhaltenden Patientenrückgängen und auslaufenden Zuschlagsregelungen. Daneben erschweren die im Rahmen neu entdeckter Varianten regelmäßig prognostizierten Überbelegungssituationen den Krankenhäusern eine verlässliche Planung. Da trifft es sich gut, dass zumindest aus dem IT-Bereich mit den aktuell in Aussicht stehenden Fördermitteln aus dem Krankenhauszukunftsfonds positive Signale für die Zukunft ausgehen. Diese positiven Signale betreffen zum einen die Fortentwicklung der digitalen Transformation im Krankenhaus zum anderen den deutlichen Zugewinn an IT-Sicherheit in den Häusern durch die explizite Schwerpunktlegung der Fördergesetzgebung auf diesen Bereich.

Von Thorsten Schütz, Leiter IT und Betriebsorganisation, Klinikum Itzehoe, Stellvertretender Vorsitzender Bundesverband der Krankenhaus IT-Leiterinnen/Leiter KH-IT

Und IT-Sicherheit ist durchaus dringend geboten, reißen doch die Angriffswellen auf kritische Infrastrukturen und den Gesundheitssektor nicht ab. So wurden allein in diesem Jahr mit einem Angriff auf eine Urologische Klinik in München, ein Krankenhaus im Kreis Soest und eine weitere Klinik in Wolfenbüttel erneut gleich mehrere Krankenhäuser Opfer von Cyberangriffen und Erpressungsversuchen. Europäisch betrachtet war der Krankenhaus-IT nicht einmal eine Sommerpause vergönnt, wie das jüngste Beispiel des Angriffs auf ein Spital in Bukarest im Juli zeigte.

Dabei ist die Informationssicherheit in den Krankenhäusern gemäß ihrer Schutzziele – Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit – nicht allein durch Cyberangriffe bedroht. Die Verfügbarkeit könnte zukünftig ebenso durch Stromausfälle gefährdet sein. Die kontinuierliche Verdrängung verlässlicher Energiereserven aus Kohle

und Atomkraft zugunsten der Quellen aus Windkraft und Solarenergie führt zu zunehmend gefährlichen Schwankungen im Stromnetz abzulesen an den immer häufiger notwendig werdenden Eingriffen der Stromnetzbetreiber in Form sogenannter Redispatche. Die zunehmende Gefahr eines längerfristigen Blackouts stellt alle IT-Verantwortlichen damit vor zusätzliche Herausforderungen.

IT-Systeme sicherer machen

Doch anlässlich der Vorstellung zukünftig wieder papierbasiert aber dafür ausfallsicher zu dokumentieren formiert sich in Krankenhäusern überraschend Widerstand. Also dann doch besser die bestehenden Systeme sicherer machen.

Diesen Weg weisen jedenfalls klar nicht nur die erwähnten Fördermittel aus dem Krankenhauszukunftsfonds mit der verpflichtenden Mindestquote von 15% für die IT-Sicherheit, sondern auch die Vorgaben aus weiteren Gesetzen.

So nimmt das Patientendatenschutz-Gesetz (PDSG) ab dem 01.01.2022 die bislang sicherheitstechnisch nicht regulierten Krankenhäuser mit einem eigenen Paragraphen ins Visier und gibt ihnen mit dem neu geschaffenen § 75c SGB V einen Rahmen vor, wie sie den Stand der Technik in Bezug auf IT-Sicherheit zukünftig sicherstellen mögen. Orientieren sollen Sie sich dabei an den "Großen", den Kritis-Krankenhäusern mit mehr als 30 Tausend vollstationären Fällen pro Jahr, die gemäß IT-Sicherheitsgesetz, jüngst verschärft durch die Neuauflage des IT-Sicherheitsgesetzes 2.0, den Branchenspezifischen Sicherheitsstandard (B3S) einhalten müssen. Dieser B3S ist jetzt ebenfalls vorgesehen als Maßstab für die sog. § 75c-Häuser. Einziger Unterschied, bislang ist für sie keine Nachweispflicht vorgesehen.

Ob diese auf anderen Wegen später nachfolgt, wird sich in den kommenden

Jahren zeigen. So sind bereits in diesem Jahr alle über das KHZG geförderten Krankenhäuser erstmalig verpflichtet, mittels einer Reifegradmessung detaillierte Auskünfte zum Entwicklungsstand ihrer IT offenzulegen. Kriterien und Kennzahlen zur Erfassung des Reifegrades der IT-Sicherheit sind dabei typischer Bestandteil aller gängigen Reifegradmodelle. Liegen solche Daten erst einmal vor, wird man sich möglicherweise über weitere Verwendungsmöglichkeiten Gedanken machen, zumal mit der bereits vorgesehenen Zweitmessung im Jahr 2023 gleich eine Entwicklungstendenz ableitbar wäre.

Vertrauen in den Digitalen Wandel stärken

Dass zur Anwendung kommende IT-Verfahren im Gesundheitswesen regelmäßig risikobehaftet sind, konnten jüngst die IT-Sicherheitsexperten Martin Tschirsch und André Zilch eindrucksvoll zeigen. Kaum waren im Juli die deutschen Apotheken beauftragt worden, digitale Impfnachweise auszustellen, gelang es den beiden IT-Sicherheitsspezialisten, genau solche digitalen Nachweise mit begrenztem Aufwand unter Ausnutzung einer bestehenden Sicherheitslücke erfolgreich nachzubilden. Die ausstellenden Apotheken mussten deshalb bereits nach kurzer Zeit wieder vom Netz bevor erst im zweiten Anlauf die fälschungssichere Vergabe der digitalen Zertifikate gelang.

Es gilt daher auch zukünftig, das Vertrauen in den Digitalen Wandel für Betreiber und Anwender nachhaltig weiter zu stärken und auf der anderen Seite trotzdem jederzeit ausreichend auf ein mögliches Angriffsszenario oder

einen unerwarteten Störfall vorbereitet zu sein, da absolute Sicherheit nicht erreichbar ist.

So bleiben Notfallpläne, Notfallübungen, Risikomanagement und die Awareness von Anwendern und Administratoren weiterhin wichtige Säulen für den sicheren IT-Betrieb. Finden diese Themen Eingang in eine passend angelegte, zukunftsweisende Digitalstrategie, steht der erfolgreichen digitalen Transformation an dieser Stelle nichts entgegen.



Thorsten Schütz, Leiter IT und Betriebsorganisation, Klinikum Itzehoe, Stellvertretender Vorsitzender Bundesverband der Krankenhaus IT-Leiterinnen/Leiter KH-IT:
„Es gilt daher auch zukünftig, das Vertrauen in den Digitalen Wandel für Betreiber und Anwender nachhaltig weiter zu stärken.“



DEEP LEARNING

KI-READY MIT RVC CLINICAL REPOSITORY

Ihre Daten sind Gold wert – machen Sie das Beste daraus! Wir helfen Ihnen, sie richtig zu lesen – mit dem intelligenten Medical Data Management des RVC Clinical Repository:

- ✓ RELATIONALE DATABASE
- ✓ INTELLIGENTE STEUERUNG
- ✓ AUTOMATISIERTE INFORMATIONS-
VERARBEITUNG
- ✓ UNIVERSELLER SPEICHERZUGRIFF
- ✓ DSGVO-KONFORM
- ✓ STATIONÄR, MOBIL & PER APP



Akuter Handlungsbedarf für Krankenhaus-Verantwortliche: IT-Sicherheit wird zur Pflichtaufgabe für alle Krankenhäuser

Angesichts wachsender Cyberbedrohungen und steigender Angriffszahlen verschärft der Gesetzgeber die Anforderungen für KRITIS-Einrichtungen und nimmt auch Nicht-KRITIS-Organisationen stärker in die Pflicht. Dieser Beitrag weist auf aktuelle Themen und Aspekte hin, die Verantwortliche für medizinische Einrichtungen unbedingt beachten sollten, liefert konkrete Handlungsempfehlungen für die Praxis und enthält einen Quick-Check zur Feststellung des KRITIS-Status im Gesundheitswesen. Von Sascha M. Zaczyk, Manager Informationssicherheit & Premium Consultant

Herausforderung 1: IT-Sicherheit wird Pflicht für alle Krankenhäuser

Schon die erste Fassung des IT-Sicherheitsgesetzes (§ 8 BSI-Gesetz) verpflichtete Betreiber von Kritischen Infrastrukturen im Sektor Gesundheit zu technischen und organisatorischen Vorkehrungen, um ihre IT-Systeme nach dem „Stand der Technik“ abzusichern. Die oberste Leitung eines Krankenhauses muss damit ab 30 000 vollstationären Fällen pro Jahr ein Informationssicherheits-Managementsystem in anerkannter Weise betreiben und verantworten.

Mit dem Patientendaten-Schutz-Gesetz (PDSG) wurden im Oktober 2020 erneut Änderungen in Bezug auf die IT-Sicherheit festgelegt und im Sozialgesetzbuch (§ 75c SGB V) konkretisiert. Ab dem 1. Januar 2022 sind alle Krankenhäuser (also auch Nicht-KRITIS-Einrichtungen) in Deutschland verpflichtet, angemessene Schutzmaßnahmen zur IT-Sicherheit zu treffen. Zu vermeiden sind jegliche Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie weiterer Schutzziele der informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind. Dabei sind die informationstechnischen Systeme spätestens alle zwei Jahre an den aktuellen Stand der Technik anzupassen.

Handlungsempfehlung 1:

Um nachzuweisen, dass geeignete organisatorische und technische Vorkehrungen zur IT-Sicherheit getroffen wurden, ist die Anwendung einer anerkannten Methodik obligatorisch:

- ISO/IEC 27001/27002 mit branchenspezifischer Erweiterung nach ISO 27799
- Branchenspezifischer Sicherheitsstandard B3S für die Gesundheitsversorgung im Krankenhaus
- ISO/IEC 27001 auf der Basis von IT-Grundschutz

Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) eignen sich alle drei Methodiken zur Umsetzung der Anforderungen aus dem BSI-Gesetz. Etabliert haben sich besonders die ISO/IEC 27001 und der in weiten Teilen darauf aufbauende, von der Deutschen Krankenhausgesellschaft erarbeitete Standard B3S Gesundheitsversorgung. Der IT-Grundschutz bietet keine branchenspezifischen Bezüge und wäre daher aufwändiger zu implementieren.

Einzuplanen ist ein ausreichend großes Zeitkontingent, da ein komplettes Informationssicherheits-Managementsystem (ISMS) aufgebaut und betrieben werden muss.

Herausforderung 2: Einsatz von Systemen zur Angriffserkennung

Das am 28. Mai 2021 in Kraft getretene „Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ („IT-Sicherheitsgesetz 2.0“) verschärft die ursprünglichen Anforderungen für KRITIS-Krankenhäuser: der Nachweis geeigneter organisatorischer und technischer Vorkehrungen muss binnen zwei Jahren beim BSI erfolgen, danach regelmäßig alle zwei Jahre. Ab dem 1. Mai 2023 umfassen die genannten Vorkehrungen auch den Einsatz von Systemen zur Angriffserkennung, die geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten.

Handlungsempfehlung 2:

Weil das IT-Sicherheitsgesetz nur für KRITIS-Einrichtungen einschlägig ist, muss im Zweifelsfall zunächst der KRITIS-Status ermittelt werden - beispielsweise über den später beschriebenen KRITIS Quick-Check.

Zur Angriffserkennung wird klassischerweise ein IDS (Intrusion Detection System) oder SIEM (Security Incident and Event Management) eingesetzt. Allerdings reicht das oft nicht aus, weil nur ein Teil der potenziell gefährdeten Systemlandschaft überwacht wird.

Auch genügt das bloße Einschalten solcher Systeme formal nicht, da sie laut Anforderung in der Lage sein sollen, fort-

März macht *mobil*



mit
**März-Hosp.IT
Easy Mobility**

Unser Service
für den reibungs-
losen Betrieb
der digitalen
Patientenakte.

Berlin
Chemnitz
Essen
Frankfurt
Hamburg
Karlsruhe
Magdeburg
München

www.maerz-network.de

März. IT, die läuft.

während Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Insbesondere der letztgenannte Punkt erfordert organisatorische/operative Aktivitäten und damit den Einsatz von Personal.

Allerdings lässt sich mangels Zeit und geeigneten Personals eine Reduktion der protokollierten Datenflut auf tatsächlich sicherheitsrelevante Ereignisse in Eigenregie faktisch nicht leisten. Trotz mittlerweile etablierter Künstliche Intelligenz-Algorithmen ist zur finalen Beurteilung von Vorkommnissen menschliche Expertise nötig, die nicht beliebig verfügbar ist. Wesentlich schneller, wirksamer und wirtschaftlicher ist beispielsweise die

Inanspruchnahme eines spezialisierten Managed Security Services. Auf jeden Fall ist ein angemessener zeitlicher Vorlauf für die Start-Konfiguration und Parametrisierung der beteiligten Systeme einzukalkulieren.

KRITIS Quick-Check

Eine Kritische Infrastruktur im Gesundheitswesen bilden Systeme („Anlagen“), die „von hoher Bedeutung für das Funktionieren des Gemeinwesens“ sind und dabei durch das Überschreiten von Schwellenwerten eine bestimmte Größenordnung gegeben ist.

Mit folgendem Quick-Check können Sie ermitteln, ob Sie eine Kritische Infrastruktur im Gesundheitswesen betreiben:

KRITIS Quick-Check Gesundheitsversorgung

Sind Sie Betreiber einer Kritischen Infrastruktur in der Gesundheitsversorgung?
Das ist gegeben, wenn mindestens eine der folgenden Bedingungen gemäß BSI-Kritisverordnung (BSI KritisV), Anlage 5 zutrifft:

Leistung/Dienstleistung	Bedingung	Bedingung trifft zu?
Stationäre medizinische Versorgung: Aufnahme, Diagnose, Therapie, Unterbringung/Pflege und Entlassung in Krankenhäusern	Mehr als 30 000 vollstationäre Fälle pro Jahr	
Versorgung mit lebenserhaltenden Medizinprodukten: Herstellung und Abgabe von Medizinprodukten	Mehr als 90,68 Mio. Euro Umsatz pro Jahr	
Versorgung mit Arzneien und Blut/Plasma: Herstellung, Vertrieb und Abgabe von verschreibungspflichtigen Arzneimitteln und Blut- und Plasmakonzentraten	Mehr als 4,65 Mio. verschreibungspflichtige Arzneimittel pro Jahr bzw. 34 000 Einheiten Erythrozytenkonzentrat, Thrombozytenkonzentrat und Plasma pro Jahr	
Laboratoriumsdiagnostik: Transport und Analytik in Laboren	Mehr als 1,5 Mio. Aufträge pro Jahr	

Als Betreiber einer Kritischen Infrastruktur fallen Sie unter die KRITIS-Regulierung und sind zu einer Reihe von Maßnahmen verpflichtet:

KRITIS Pflichten

Aspekt	Verpflichtende Maßnahme/Aktivität
Identifikation	KRITIS-Relevanz in Eigeninitiative prüfen bzw. feststellen
Registrierung	KRITIS-Anlagen beim BSI bekannt geben und sich als KRITIS-Einrichtung registrieren
Meldung	Informationen zu erheblichen IT-Störungen, Angriffen und Vorfällen an das BSI melden
Geltungsbereich	KRITIS-Anlagen definieren und Anwendungsbereich („scope“) in der Organisation festlegen
Cyber-Security-Maßnahmen (TOMs)	Technische und organisatorische Maßnahmen (TOMs) zum Management von IT- bzw. Informations-Sicherheit (ISMS), Risiken, Kontinuität (BCM) und Technologien festlegen und umsetzen
Audits	Umsetzung der Cyber-Security-Maßnahmen regelmäßig durch Audits nachweisen

Als Betreiber einer Kritischen Infrastruktur gilt ein Krankenhaus, wenn mit seinen IT-Systemen mehr als 30.000 vollstationäre Fälle pro Jahr verarbeitet werden. Bei Einrichtungen mit mehreren Standorten ist die Gesamtzahl aller Fälle, die über gemeinsame IT-Systeme laufen, maßgeblich. Krankenhäuser müssen jeweils bis zum 31. März prüfen, ob sie diesen Schwellenwert im Vorjahr überschritten haben. Falls das zutrifft, gilt das Krankenhaus ab dem 1. April als KRITIS-zugehörig und muss das Bundesamt für Sicherheit in der Informationstechnik (BSI) unverzüglich darüber informieren.

Daueraufgabe mit existenzieller Relevanz

Die hier vorgestellten Beispiele belegen, dass Informationssicherheit als Daueraufgabe anzusehen ist und eine konsequente wie gewissenhafte Behandlung erfordert. Sollten Anforderungen ignoriert oder erforderliche Maßnahmen nicht wirksam umgesetzt sein, können Cyberangriffe durchaus die Existenz einer Einrichtung gefährden. Ähnliches droht, wenn etwa bei Unterlassung durch die Aufsichtsbehörde Strafzahlungen in empfindlicher Höhe verhängt werden. Eine zertifizierte und branchenerfahrene externe Unterstützung kann dabei helfen, Fehleinschätzungen und/oder mangelhafte Umsetzungen zu vermeiden und das erforderliche Sicherheitsniveau dauerhaft zu halten.

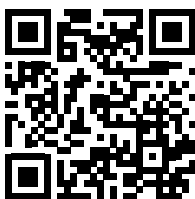


Sascha M. Zaczyk, Manager Informationssicherheit & Premium Consultant, International Certified Lead Auditor ISO 27001, zertifizierter Lead Auditor EN 50600, zertifizierter (Agile) ITIL-Experte & Datenschutzbeauftragter, Professional Scrum Master; EnBW AG, Full Kritis Service, s.zaczyk@enbw.com

Mehr Zeit für die Patienten durch Patientendatenmanagement



DIE RICHTIGE LÖSUNG FÜR IHREN KHZG-ANTRAG!



Die digitale Pflege- und Behandlungsdokumentation ist ein wesentliches Förderkriterium des KHZG zur Förderung von Vorhaben zur Digitalisierung der Prozesse und Strukturen im Verlauf eines Krankenhaus-aufenthaltes von Patientinnen und Patienten. Mit einem elektronischen Patientendatenmanagement-system, wie unserem ICM, kann die Zeit pro Aufnahme im Durchschnitt um fast 50% gesenkt werden. Zusätzlich können Kodierfehler um bis zu 72% reduziert werden, was eine Optimierung der Leistungs-abrechnung ermöglicht. Sprechen Sie uns gerne an.

ERFAHREN SIE MEHR: WWW.DRAEGER.COM/ICM

Datenschutz ist kein Silo:

Warum sich Krankenhäuser mit der DSGVO schwer tun

Datenschutz findet oft noch keinen Eingang in die Arbeitsprozesse, wo Patientendaten tatsächlich verarbeitet werden. Datenschutzmanagement ist nicht als Silo-Organisation zu gestalten, sondern auf die Gestaltung von Prozessen und Organisation zu übertragen. Verantwortlichen fehlt oft noch die Erkenntnis, dass die Bereiche zusammenhängen, die häufig die gleichen Informationen zum Nachweis benötigen und daher nur integriert umgesetzt werden können. Ein Interview mit Stefanie Köhl, Geschäftsführerin, eGovernment Consulting and Development GmbH

Wie schätzen Sie den aktuellen Stand der Umsetzung der Datengrundschutzverordnung DSGVO in deutschen Krankenhäusern ein?

Stefanie Köhl: Der Reifegrad des Datenschutzes in deutschen Krankenhäusern ist vielfach eher noch als mäßig einzuschätzen, was eine kürzlich durchgeführte qualitative Studie der eGovCD (siehe weiterführende Literatur) bestätigte. Über die Jahre ist vielfach nicht bedacht worden, dass durch die zunehmende IT-Nutzung im Krankenhaus das Thema Schutz personenbezogener Daten mehr Aufmerksamkeit gebraucht hätte. Erst durch die tatsächliche Digitalisierung in den Krankenhäusern kommen IT-Sicherheit und Datenschutz in den Vordergrund und es werden die bestehenden Defizite der vergangenen Jahrzehnte sichtbar. Die nächste große Herausforderung kommt mit der Einführung der ePatientenakte. Hier werden die bestehenden Unsicherheiten und fehlenden Kenntnisse die Umsetzung erschweren bzw. im schlimmsten Fall zu zahlreichen Schutzverletzungen führen. Unsere empirische Erfahrung zeigt, dass die verantwortliche Führungsebene in Krankenhäusern die Frage danach, wie hoch das Risiko der Schutzverletzung von Daten in neuen digitalen Prozessen ist, wie Daten in diesen Prozessen geschützt und welche Maßnahmen genau dafür ergriffen werden, häufig nicht zweifelsfrei beantworten können.

Warum tun sich Ihrer Meinung nach so viele Krankenhäuser schwer mit der Umsetzung von Datenschutz?

Stefanie Köhl: Das Thema Datenschutz wird in vielen Organisationen als Fremdkörper und störend wahrgenommen: „zu komplex, zu unverständlich, das ist etwas für Rechtsexperten“. Fakt ist jedoch: die komplexen Datenschutzanforderungen können nur dann erfüllt werden, wenn sie in der gesamten Organisation verstanden und auch als Teil der Kultur gelebt werden. Deswegen kommt man nicht umhin, das Thema stärker in der Organisation zu verankern und nicht auf einzelne und vielleicht sogar noch externe Experten – nach dem Motto: „Aus den Augen, aus dem Sinn.“ – abzuwälzen. Große Defizite in Bewusstsein und Kenntnissen gibt es vor allem

beim Krankenhauspersonal, was insofern problematisch ist, weil dieses täglich den Schutz von Patientendaten gewährleisten muss. Erschwerend kommt hinzu, dass Krankenhäuser generell eine hohe Arbeitsdichte aufweisen, die u.a. aus Personalmangel resultiert. Insgesamt bleibt Datenschutz damit derzeit oft noch auf einer deklaratorischen Ebene und findet keinen Eingang in die Arbeitsprozesse, d.h. dort wo die Patientendaten tatsächlich verarbeitet werden.

Was sollten Krankenhäuser beachten, wenn Sie einen sicheren und nutzerfreundlichen Datenschutz etablieren wollen?

Stefanie Köhl: Mitarbeiter fast aller Bereiche eines Krankenhauses verwenden personenbezogene Daten. Für all diese Tätigkeiten sind datenschutzkonforme Verarbeitungsvorgänge umzusetzen, womit die Arbeitsprozesse im Fokus stehen. Wichtigstes Ziel ist es, dass sich die Mitarbeiter vornehmlich auf den fachlichen Teil ihrer Tätigkeiten konzentrieren können und nicht zuerst überlegen müssen, ob sie gerade datenschutzkonform handeln. Soll das zunächst „sperrig“ anmutende Thema Datenschutz akzeptiert werden, muss es mehr oder weniger „unsichtbar“ in die Arbeitsorganisation integriert werden. Dazu ist vor allem ein niedrigschwelliger Zugang zum Thema Datenschutz für alle zu gewährleisten, zuständigkeitsübergreifende Kommunikationsprozesse zu etablieren, Führungskräfte-Kompetenzen zu verbessern und das Prinzip „Datenschutz durch Technikgestaltung“ auf die Gestaltung von Prozessen und Organisation zu übertragen. Das alles bedarf erheblicher Interaktion und intensiver (organisationaler) Lernprozesse. Ein konkretes methodisches Vorgehen kann helfen, die Herausforderungen bei der Umsetzung des Datenschutzes einfacher zu meistern. Dabei geht es nicht darum, Expertentools für Datenschutzbeauftragte einzukaufen. Vielmehr sind Methoden und Tools zu nutzen, die auch von Nicht-Experten intuitiv anwendbar sind, sodass Datenschutz „nebenbei“ gelernt und nahezu unsichtbar in die Arbeitsabläufe integriert wird.

Wenn Sie methodisches Vorgehen sagen, was genau meinen Sie damit und wie kann das konkret aussehen?

Stefanie Köhl: Es sind unbedingt organisationsweit Informationen darüber zu erheben, bei welchen Geschäftsprozessen (Fach- sowie Querschnittsprozesse) in welcher Art und Weise personenbezogene Daten verarbeitet werden. Hier müssen der DSB, IT-Experten, die Fachebene und ggf. weitere Beauftragte intensiv kommunizieren. Diese kollaborativen Prozesse sind methodisch zu unterstützen und die Datenschutzthematik für alle Bereiche einer Organisation zu vereinfachen, verständlich und nachvollziehbar zu gestalten. Hierfür lassen sich entsprechende Bausteine, bspw. Zweck der Datenerhebung, Verarbeitungsart der Daten, Zugang zu Daten etc, abgeleitet aus den fachlichen Anforderungen der DSGVO, definieren, die einer vordefinierten Systematik folgen. Mittels einfacher haptischer Karten und einer entsprechenden Moderation können auch Nichtexperten durch den DSGVO-Prüfprozess geleitet werden. Dabei werden die Datenschutzanalysen entlang von Fachprozessen vollzogen, um so eine enge Rückkopplung zur Arbeitsebene herzustellen und diese im Weiteren mit IT-Fragen zu verknüpfen. Durch dieses Vorgehen findet bereits bei der Datenerhebung eine fachübergreifende Zusammenarbeit und ein entsprechender Austausch der jeweiligen Experten (IT, Recht, Organisation, Management) statt, so dass es sich hier nicht mehr nur um eine bloße Informationssammlung handelt, sondern bereits Umsetzungs- und Gestaltungsfragen thematisiert werden. Ein nächster wichtiger Schritt ist die Risikobewertung, d.h. es muss eingeschätzt werden, welches Risiko für Schutzverletzungen bei der Verarbeitung personenbezogener Daten besteht. Hier können grundsätzlich Algorithmen – auch analog umgesetzt – unterstützen, indem bspw. auf Basis eines organisationseigenen Kriteriensets Empfehlungen zur Interpretation der erhobenen Informationen und bei der Zuordnung zu Risikoklassen gegeben werden. Sind die Risiken definiert, sind geeignete technische und organisatorische Schutzmaßnahmen (TOM) zu bestimmen.

Welche Erfahrungen haben Sie mit diesem Ansatz bisher gemacht? Welche hilfreichen Tipps haben Sie für Verantwortliche in Krankenhäusern?

Unsere Erfahrungen mit diesem methodischen Vorgehen zeigen, dass Datenschutzanforderungen besser als vorher verstanden und umgesetzt werden können, weil Prozesse von Anfang an datenschutzsensibel gestaltet werden. Ein weiterer Vorteil ist, dass sich durch die prozessnahen Erhebungen datenschutzrelevante Aspekte für das von der DSGVO geforderte Verzeichnis aller Verarbeitungstätigkeiten inkl. entsprechender Prozessdarstellungen, Risikobewertungen und Dokumentation technisch-organisatorischer Maßnahmen nahezu automatisch ergeben, wodurch sich der Aufwand für Datenschutzbeauftragte erheblich reduziert und die Qualität des Datenschutzes maßgeblich erhöht.

Entscheidungsträger und vor allem Verantwortliche für den Datenschutz und Datensicherheit sollten mehr als je zuvor dafür sorgen, Datenschutzmanagement nicht als Silo-Organisation zu gestalten, sondern mit den Bereichen IT/IT-Sicherheit, Prozesse und Organisation sowie weiteren Compliance-Bereichen, wie Qualitätsmanagement und Arbeitsschutz, in Beziehung zu setzen und entsprechend zu verbinden. Hier fehlt bei den Verantwortlichen derzeit oft noch die Erkenntnis, dass die Bereiche zusammenhängen, häufig die gleichen Informationen zum Nachweis benötigen und daher nur integriert umgesetzt werden können. Langfristig können so Aufwände für die gesamte Compliance einer Klinik reduziert werden – eine Investition, die sich lohnt.

Weiterführende Informationen

Um die praktische Umsetzung der Datenschutzanforderungen zu erleichtern, hat die eGovCD – ein SpinOff von Fraunhofer FOKUS – in Zusammenarbeit mit dem SHI Stein-Hardenberg Institut dieses methodisch strukturierte und modulare Vorgehen in ein handhabbares und intuitives Format gebracht: „PRIMO – Datenschutz im Handumdrehen in die Organisation integrieren: Eine Methode für Datenschützer, Entscheider, Mitarbeiter und Verantwortliche“ <https://dsgvo-stressfrei.de>

Hilfreiche Links

Kurzreport „Datenschutz und IT-Sicherheit in deutschen Krankenhäusern – Ergebnisse einer empirischen Untersuchung“ <http://bit.ly/eGovCD-health-report> (Free Download)
Branchenreport „Datenschutz und IT-Sicherheit in deutschen Krankenhäusern – DSGVO trifft oftmals auf (un-)organisierte Verantwortungslosigkeit, gepflegtes Nichtwissen und politisch getriebene Digitalisierung“ <https://bit.ly/3fVO5kO>



Stefanie Köhl, Geschäftsführerin, eGovernment Consulting and Development GmbH (stefanie.koehl@egovcd.de): „Hier fehlt bei den Verantwortlichen derzeit oft noch die Erkenntnis, dass die Bereiche zusammenhängen, häufig die gleichen Informationen zum Nachweis benötigen und daher nur integriert umgesetzt werden können.“



DSGVO-Dauerdruck: Aufwand, Innovationsbremse, Rechtsunsicherheit

Vor allem kleinere Unternehmen kommen bei DSGVO-Umsetzung nur noch langsam voran. 9 von 10 Unternehmen mussten bereits innovative Projekte wegen Datenschutz-Anforderungen stoppen. Kritik über fehlende Unterstützung durch Aufsichtsbehörden ist weit verbreitet. Unternehmen stehen beim Datenschutz unter permanentem Stress.

Ein aufwändiger Prüfprozess vor der Einführung jedes digitalen Tools, regelmäßig neue Entscheidungen der Aufsichtsbehörden und Gerichtsurteile in ganz Europa, die Auswirkungen auf das eigene Unternehmen haben können – die Anforderungen an den Datenschutz setzen Unternehmen in Deutschland unter Dauerdruck. Zugleich bekommen die Aufsichtsbehörden keine guten Noten für ihre Beratung. Die Hälfte der Unternehmen (50 Prozent) sagt, Deutschland übertreibe es mit dem Datenschutz. Zwei Drittel (66 Prozent) sind der Auffassung, dass der strenge Datenschutz sowie die uneinheitliche Auslegung des Datenschutzes in Deutschland die Digitalisierung erschwert. Das sind Ergebnisse einer repräsentativen Befragung von 502 Unternehmen mit 20 oder mehr Beschäftigten in Deutschland im Auftrag des Digitalverbands Bitkom.

Susanne Dehmel, Geschäftsleiterin Bitkom: „Unternehmen stehen beim Datenschutz unter permanenten Stress. Sie wollen dem Datenschutz Genüge tun, aber dazu müssen sie nicht nur europaweit Gerichtsurteile verfolgen und die unterschiedliche Auslegung aus den Mitgliedsstaaten kennen, sondern sich zusätzlich mit 18 verschiedenen Lesarten von Datenschutzaufsichten allein in Deutschland auseinandersetzen. Das ist vor allem für kleinere Unternehmen immer schwerer zu stemmen.“

Aufwand für Datenschutz ist durch die DSGVO gestiegen

4 von 10 (42 Prozent) Unternehmen geben an, dass sie seit der DSGVO-Einführung mehr Aufwand haben – und dieser auch künftig bestehen bleiben wird. Ein weiteres Drittel (32 Prozent) geht sogar davon aus, dass der Aufwand

weiter steigen wird. Nur 19 Prozent erwarten, dass ihr gestiegener Aufwand langsam wieder sinkt, 6 Prozent haben inzwischen keinen erhöhten Aufwand mehr. Zugleich hat mit zwei Drittel der Unternehmen (65 Prozent) die große Mehrheit die DS-GVO vollständig oder größtenteils umgesetzt, aber 3 von 10 (29 Prozent) haben die Umsetzung erst teilweise geschafft und gerade einmal 5 Prozent stehen damit noch ganz am Anfang.

Die Unternehmen, die die DSGVO bislang noch nicht vollständig umgesetzt haben, nennen als Hauptgründe dafür, dass Corona andere Prioritäten erzwingen habe (82 Prozent), aber fast ebenso viele beklagen, dass sich die DSGVO gar nicht vollständig umsetzen lasse (77 Prozent). 61 Prozent fehlt es zudem an den notwendigen personellen Ressourcen. Rund jedes zweite Unternehmen beklagt

fortlaufende Anpassungen wegen neuer Urteile und Empfehlungen der Aufsicht (47 Prozent) und notwendige neue Prüfungen von Datentransfers in Länder außerhalb der EU (45 Prozent). Dehmel: „Es fehlt in kleinen Unternehmen häufig an Datenschutz-Expertise, notwendig sind daher konkrete und umsetzbare Handreichungen, etwa durch die Aufsichtsbehörden.“

Datenschutz hat Innovationen ausgebremst

Aber die DSGVO sorgt nicht nur für Aufwand, sie bremst auch Innovationsprojekte in der deutschen Wirtschaft. So geben drei Viertel aller Unternehmen (76 Prozent) an, dass Innovationsprojekte aufgrund konkreter Vorgaben der DS-GVO gescheitert sind. Und in 9 von 10 Unternehmen (86 Prozent) sind Projekte wegen Unklarheiten im Umgang mit der DS-GVO gestoppt worden. Am häufigsten betroffen war der Aufbau von Datenpools (54 Prozent), dahinter folgen Prozessoptimierungen im Bereich der Kundenbetreuung (37 Prozent), Projekte zur Verbesserung der Datennutzung und der Einsatz neuer Technologien wie Künstliche Intelligenz oder Big Data (je 36 Prozent). Und in jedem dritten Unternehmen (33 Prozent) war der Einsatz von Cloud-Diensten betroffen. „Digitale Technologien sind quer durch alle Branchen die wichtigsten Innovationstreiber. Wir brauchen eine bessere Balance von Datenschutz und Datennutzung“, so Dehmel.

Rechtsunsicherheit bei der DS-GVO-Umsetzung

In den vergangenen Jahren haben die Probleme bei der DSGVO-Umsetzung deutlich zugenommen. So sagen inzwischen mehr als drei Viertel (78 Prozent)

der Unternehmen, dass Rechtsunsicherheit die größte Herausforderung sei, vor zwei Jahren waren es erst 68 Prozent. Zu viele Änderungen bzw. Anpassungen bei den Vorgaben beklagen 74 Prozent, nach 59 Prozent 2019. Die uneinheitliche Auslegung innerhalb der EU behindert 52 Prozent (2019 wurde das nicht abgefragt, 2020: 45 Prozent), fehlende finanzielle Ressourcen nennen 37 Prozent, mehr als doppelt so viele wie noch 2019 mit 18 Prozent. Herausforderungen, auf die die Unternehmen direkt Einfluss nehmen können, gewinnen dagegen nicht an Bedeutung: Eine schwierige technische Umsetzung behindert unverändert 34 Prozent, einen Mangel an qualifizierten Beschäftigten haben nur 33 Prozent (2019: 37 Prozent) und fehlende Unterstützung im Unternehmen sehen nur noch 8 Prozent (2019: 13 Prozent).

Parallel wächst die Unzufriedenheit mit den Aufsichtsbehörden. So kritisieren zwei Drittel (66 Prozent) mangelnde Umsetzungshilfen durch die Aufsicht, vor zwei Jahren lag der Anteil nur bei 53

Prozent. „Wenn Probleme wie Rechtsunsicherheit oder fehlende Umsetzungshilfen durch die Aufsicht immer stärker zunehmen, dann läuft offenkundig etwas falsch“, mahnt Dehmel. „Normalerweise sind die Probleme am Anfang einer neuen Gesetzgebung groß und werden dann mit ersten Erfahrungen, Entscheidungen und zahlreichen Hilfestellungen geringer.“

Und einige meinen gar, die Aufsicht sei gar nicht an Problemlösung interessiert. „Um den Datenschutz in den Unternehmen nachhaltig zu befördern, reicht es nicht, Beschwerden abzuarbeiten und bei nachgewiesenen Verstößen Bußgelder zu verhängen“, so Dehmel. „Für den gelebten Datenschutz könnte viel mehr erreicht werden, wenn die Aufsichtsbehörden präventiv tätig würden und Unternehmen bei der praktischen Umsetzung der Datenschutzvorgaben unterstützten, indem sie konkrete Auskünfte erteilen und praxisnahe Empfehlungen geben.“



Susanne Dehmel, Geschäftsführerin Bitkom: „Unternehmen stehen beim Datenschutz unter permanentem Stress.“



IT-Sicherheit ohne ISMS ist wie Therapie ohne Behandlungsleitlinie

Kliniken rüsten technisch massiv auf, um die IT-Systeme abzusichern. Hochentwickelte Tools bilden jedoch nur ein Teil dessen, was notwendig ist. Technische Maßnahmen können ohne effektive Organisation der Informationssicherheit das geforderte Schutzniveau aus Vertraulichkeit, Verfügbarkeit und Integrität nicht bieten. Informationssicherheit ist ein strategisches Managementthema: Hier kommt das ISMS ins Spiel. Von Thomas Dechant, Opitz Dechant GmbH

Die 90er Jahren waren aus heutiger Sicht idyllisch: Die Rahmenbedingungen in der Krankenhaus-IT waren sehr viel einfacher. Die IT-Landschaft war deutlich weniger Bedrohungen und Vorfällen ausgesetzt. Zu den IT-Services bestand nur eine geringe Abhängigkeit: Eine Klinik funktionierte damals auch ohne IT für einige Tage weitgehend problemlos. Patienten konnten ohne Einschränkung behandelt werden.

Natürlich hingen Verwaltung, Abrechnung etc. und somit die finanzielle Stabilität schon damals an der IT. Aber es reichte im Prinzip, IT-Systeme in einer angemessenen Zeit wiederherzustellen zu können und dabei so wenige Daten zu verlieren wie möglich. Die Ursachen für Probleme waren damals so gut wie immer technische Defekte oder Fehlbedienung von Benutzern und Administratoren. Das waren dann auch

die Themen, die einen IT-Leiter umtrieben: Habe ich ein aktuelles Backup, kann man das auch wieder einspielen, sind die Sicherungsbänder lesbar? Eine idyllische Welt, die es so nicht mehr gibt.

Aber ist es denn nicht immer noch noch so, dass eine der zentralen Fragen lautet: Wie stelle ich im Extremfall meine Systeme mit möglichst geringem Datenverlust schnellstmöglich wieder her? Nun aber in einem Betrieb, der 24/7 von den IT-Systemen abhängig ist. Die zunehmende Digitalisierung vergrößert diese Abhängigkeit weiter.

Technik ist nur ein Baustein

Heute ist nicht nur die Verfügbarkeit der Systeme von essentieller Bedeutung. Inzwischen ist vielen – leider nicht allen! – Verantwortlichen hinreichend bewusst, dass ein Hacker nicht nur Systeme lahmlegen, sondern durch Manipulation der

Daten Menschenleben gefährden oder mit gestohlenen Daten Menschen erpressen kann. Heute muss eine Klinik mit vielfältigen Bedrohungen umgehen, die sich auf die Vertraulichkeit, Verfügbarkeit und Integrität von IT-Systemen und Daten auswirken können. Dabei geht es immer auch um Risiken hinsichtlich der Patientensicherheit, Behandlungseffektivität und der Reputation.

Deshalb wird in vielen Kliniken technisch massiv aufgerüstet, um die IT-Systeme abzusichern: Es werden Firewalls beschafft, Virens Scanner installiert, hochverfügbare Rechenzentren aufgebaut, das Netzwerk redundant ausgelegt, Daten hin- und hergespiegelt, E-Mailanhänge per Sandboxing geprüft und was die Technik sonst noch so hergibt. Das ist alles wichtig – aber nur ein Teil dessen, was notwendig ist. Technische Maßnahmen können ohne effektive

Organisation der Informationssicherheit das geforderte Schutzniveau aus Vertraulichkeit, Verfügbarkeit und Integrität nicht bieten.

Zum Beispiel in Sachen Backups – da ist doch alles klar, denken Sie? Sie gehen schließlich davon aus, dass die IT täglich die Daten sichert. Und damit haben Sie natürlich recht. Aber: Wie machen die Mitarbeiter:innen der IT das? Nicht nur technisch, sondern welche organisatorischen Vorgaben werden dabei berücksichtigt? Als Auditor namhafter Zertifizierer prüfe ich Kliniken hinsichtlich Informationssicherheit und Vorgaben der KRITIS-Gesetzgebung. Oft höre ich bei Prüfungen oder auch in Beratungsprojekten, dass die IT-Abteilung doch am besten wisse, wie Backups zu machen sind. In technischer Hinsicht stimmt das auch. Doch als Prüfer frage ich dann immer: Wie lange darf denn ein Restore z.B. des KIS dauern und wie viele Daten dürfen dabei verloren gehen? Nur wenn diese und andere Vorgaben definiert sind, kann ein angemessenes Backupkonzept entwickelt werden. Das sind Anforderungen aus der Organisation! Die kann nicht die IT-Abteilung festlegen. Dazu müssen Verantwortlichkeiten geklärt, Prozesse z.B. zur regelmäßigen Überprüfung definiert und auch die Kritikalität und der Schutzbedarf von IT-Systemen und der verarbeiteten Daten festgelegt werden. Organisatorische Maßnahmen sind dazu notwendig, technische Maßnahmen angemessen zu planen und zu überprüfen.

Aufbau und Betrieb eines ISMS

Backups sind indes nur ein Aspekt. Um die Sicherheit der IT-Systeme und der darauf gespeicherten und verarbeiteten Daten einer Klinik auf ein angemessenes Niveau zu heben, muss man das Thema

breit angehen. Das schwächste Glied bestimmt die Stärke einer Kette. Das gilt auch für Informationssicherheit. Um sich nicht zu verzetteln, aber auch keinen relevanten Aspekt zu übersehen, bieten sich Standards zur Informationssicherheit zur Orientierung an. Für Kliniken beschreiben ISO 27001 und B3S für Krankenhäuser, wie ein funktionierendes ISMS (InformationssicherheitsManagementsystem) State of the Art aufgebaut sein muss. B3S wurde explizit für Kliniken entwickelt und berücksichtigt deshalb spezielle Gegebenheiten wie z.B. die Geräte der Medizintechnik. Allerdings lehrt die Erfahrung aus KRITIS-Prüfungen, dass einige Anforderungen des B3S zwar gut gemeint, aber in der Praxis nur schwer umzusetzen sind – bei überschaubarem Nutzen. Die ISO 27001 ist hingegen ein flexibles Framework, das man gut an jede Organisation anpassen kann. Natürlich muss man beobachten, dass man dann auch alle Aspekte in einer Klinik wirklich erfasst.

Ob ISO 27001 und B3S – am Aufbau und Betrieb eines ISMS kommt keine Klinik mehr vorbei, wenn sie Sicherheit und Verfügbarkeit der IT-Systeme und Daten auf einem angemessenen Niveau sicherstellen will. Mit § 75c SGB V IT-Sicherheit in Krankenhäusern hat der Gesetzgeber alle Krankenhäuser dazu gesetzlich verpflichtet. Aktuell werden den Kliniken erhebliche Mittel über das KHZG (Krankenhauszukunftsgesetz) zur Verfügung gestellt, um diese gesetzliche Anforderung auch umzusetzen.

Kommunizieren, kommunizieren, kommunizieren

Ist ein ISMS aufgebaut, ist die Arbeit nicht getan, sondern eigentlich fängt sie jetzt erst an: Ein ISMS, das funktioniert, muss im Klinikalltag gelebt werden! Das bedeutet vor allem: kommunizieren,

kommunizieren, kommunizieren. Vom Hausmeister bis zum Chefarzt müssen alle Mitarbeiter:innen ihre Rolle im ISMS kennen, Wissen und notwendige Tools an die Hand bekommen und vor allem verstehen, wozu dies alles notwendig ist. Gerne wird dann neben der Hygiene- und der Brandschutzunterweisung einfach noch eine weitere Schulung in den jährlichen Schulungskalender aufgenommen, frei nach dem Motto: Pflicht erfüllt, Haken dahinter. Aber es geht um viel mehr: wirksame Sensibilisierung der Mitarbeiter:innen, Konfliktmanagement für die IT-Sicherheitsprofis und Übungen für den Ernstfall, wenn Krisenkommunikation notwendig wird.



Thomas Dechant, Geschäftsführer (MD), Lead-Auditor und Consultant, Opitz Dechant GmbH: „Ein ISMS, das funktioniert, muss im Klinikalltag gelebt werden!“

IT-Sicherheit im Krankenhaus:

Ab 2022 auch für kleinere Kliniken verpflichtend

Laut IT-Sicherheitsgesetz müssen bereits seit Juni 2017 Krankenhäuser mit mehr als 30.000 vollstationären Fällen pro Jahr als Betreiber Kritischer Infrastrukturen ihre IT-Systeme stets auf dem neuesten Stand der Technik halten und dies alle zwei Jahre nachweisen. Ab Januar 2022 wird diese Vorgabe auf alle Krankenhäuser erweitert, zunächst noch ohne Nachweispflicht. Von Nadja Götz, Deutsche Gesellschaft zur Zertifizierung von Managementsystemen (DQS GmbH)

Dass nun auch kleinere Krankenhäuser in der Pflicht sind, ihre IT-Systeme auf dem neuesten Stand zu bringen und zu halten, ist vor allem dem im Oktober 2020 in Kraft getretenen Patientendaten-Schutz-Gesetz geschuldet. Die damit einhergehenden Anforderungen an die Informations- und IT-Sicherheit wurden im Sozialgesetzbuch (§ 75c SGB V) konkretisiert und müssen nun zur Sicherung der Patientendaten vollumfänglich umgesetzt werden. Dabei gilt der Grundsatz, dass organisatorische und technische Maßnahmen zur Erreichung von IT- und Informationssicherheit dann angemessen sind, wenn der erforderliche Aufwand für ihre Umsetzung in einem vertretbaren Verhältnis zu den Folgen eines Ausfalls, einer Störung oder einer sonstigen Beeinträchtigung der Klinik oder der Sicherheit von Patienten und den dazugehörigen Informationen steht.

Was für Betreiber Kritischer Infrastrukturen im Gesundheitswesen inzwischen Routine ist, stellt für viele kleinere Krankenhäuser jedoch eine höchst anspruchsvolle Aufgabe dar, wenn nicht sogar Neuland. Die Häuser verfügen aufgrund oft jahrelang ausgebliebener Investitionen nur selten über eigene IT-Abteilungen und können mit den technisch teils veralteten IT-Ausrüstungen und -Strukturen, aber auch in Ermangelung wirksamer Managementsysteme die IT- und Informationssicherheit und damit letztlich auch die Sicherheit der Patienten nicht ausreichend gewährleisten.

Die großen Einrichtungen mit Kritis-Relevanz haben sich bei der Erfüllung der Anforderungen damals mit Erfolg am sog. „B3S Krankenhaus“ orientiert und tun es weiterhin, der Gesetzgeber empfiehlt dieses Vorgehen ausdrücklich auch für kleinere Häuser. Prinzipiell wäre aber auch die Implementierung eines reinen ISMS Informationssicherheitsmanagement-System (ISMS) gemäß ISO/IEC 27001 möglich, wenn krankenhausspezifische Anforderungen zusätzlich integriert werden.

B3S Krankenhaus – geeigneter Standard auch für kleinere Kliniken

B3S Krankenhaus ist ein Ende 2018 von der Deutschen Krankenhausgesellschaft veröffentlichter Standard. Das allgemeine Kürzel „B3S“ bedeutet „Branchenspezifischer

Sicherheitsstandard. Der Standard wurde ursprünglich entwickelt, um großen Krankenhäusern, die unter die Kritis-Verordnung fallen, eine Grundlage zur Einhaltung der gesetzlichen Regelungen und zur Bereitstellung der geforderten Nachweise gemäß IT-Sicherheitsgesetz zu bieten. Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) hat die Eignung des B3S Krankenhaus im Oktober 2019 festgestellt. Nachweise auf der Grundlage des Sicherheitsstandards (z. B. eine Zertifizierung) werden somit anerkannt. Der B3S Krankenhaus kann auf der Internetseite der Deutschen Krankenhausgesellschaft (DKG) kostenfrei heruntergeladen werden.

Die 168 Maßnahmen des B3S Krankenhaus werden nach Muss-, Soll- und Kann-Anforderungen unterschieden, die sich auf sechs Schutzziele konzentrieren. Vier davon sind die klassischen Schutzziele eines (ISMS) nach ISO/IEC 27001, nämlich Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit, ergänzt um die zwei branchenspezifischen Ziele Patientensicherheit und Effektivität der Behandlung.

Verantwortung der obersten Klinikleitung

Im Mittelpunkt steht die Verantwortung der obersten Leitung der Klinik für alle strukturellen und prozessualen Aspekte. Sie ist in diesem Zusammenhang dazu verpflichtet, alle für die Wirksamkeit des ISMS notwendigen finanziellen, organisatorischen und personellen Ressourcen bereitzustellen und dafür zu sorgen, dass alle Informationssicherheitsziele erreicht werden. Grundlage dafür ist die Benennung eines Datenschutzbeauftragten und eines Informationssicherheitsbeauftragten sowie die Besetzung des Postens der Leitung der Krankenhaus-IT. Eine zentrale Rolle spielt auch das Risikomanagement. Zur Bewertung der Kritikalität identifizierter Risiken hält der B3S Krankenhaus 40 Beispiele für Bedrohungsszenarien bereit und benennt dazu mögliche Schwachstellen und Gefahren.

Wichtig ist: Die Digitalisierung betrifft nicht nur die IT. Natürlich stehen im Gesundheitswesen für viele derzeit die IT-Risiken im Mittelpunkt, die Digitalisierung der Prozesse aus ganzheitlicher Sicht schließt aber auch die Chancen mit ein, nämlich dann, wenn die Prozesse der Einrichtungen sicherer,



Nadja Götz ist Expertin der Deutschen Gesellschaft zur Zertifizierung von Managementsystemen (DQS GmbH) für Gesundheitsmanagementsysteme und BSI-KRITIS-Prüfungen, Auditorin und Produktmanagerin für diverse Qualitätsstandards der Rehabilitation sowie der stationären und ambulanten Versorgung.

flexibler, schneller, ressourceneffizienter und damit auch kostengünstiger werden. Stichworte hier sind Geltungsbereiche samt Schnittstellen, Prozesslandschaften und Gefährdungsanalysen auch mit Blick auf die Patientensicherheit und die Behandlungseffektivität.

Umsetzung des B3S Krankenhaus in die Praxis

Kleinere Kliniken, die bislang noch keine oder nur wenig Erfahrung mit Managementsystemen und deren Implementierung gemacht haben, stehen vor dem Problem, wie sie an die Sache herangehen sollen, zumal die Zeit mit Blick auf den Stichtag 01.01.2022 drängt. Dazu kommt möglicherweise fehlendes Know-how über den aktuellen Stand der IT-Technik und den Umgang damit. Zwar müssen Kliniken „nur“ ihre IT-Systeme auf den neuesten Stand bringen und dort halten sowie angemessene Informationssicherheit gewährleisten. Dass laut IT-Sicherheitsgesetz (noch) kein regelmäßiger Nachweis über die Wirksamkeit des implementierten ISMS (z. B. nach B3S Krankenhaus) verlangt wird, bedeutet jedoch nicht, dass ein solcher Nachweis im Fall der Fälle nicht eventuell doch erbracht werden muss, zum Beispiel aus Haftungsgründen o. ä. Es bietet sich also geradezu an, für die Implementierung der Anforderungen des B3S Krankenhaus auf professionelle Hilfe externer Partner zurückzugreifen. Dabei sollte jedoch beachtet werden, dass solche Leistungen nur von Stellen erbracht werden sollten, die eine ausgewiesene Expertise vorweisen können. Diese wird meist auf ausgiebige Erfahrung bei der Unterstützung oder Zertifizierung großer Kliniken zurückgehen, die den Sicherheitsstandard aufgrund der Kritis-Verordnung einführen mussten.

Hilfreich: Workshops & Co.

Eine entsprechende Unterstützung kann z. B. in Workshops erfolgen, in denen die Teilnehmer erfahren, wie sie den Geltungsbereich des B3S definieren, wie sie die Informationssicherheitspolitik ihrer Klinik entwickeln und wie die für sie relevanten Compliance-Anforderungen des B3S ermittelt werden können. Hier wird in der Regel auch vermittelt, wie an die Verteilung von Rollen und Verantwortlichkeiten herangegangen werden kann.

Nutzbringend sind grundsätzlich auch Self-Assessments, deren Ergebnis z. B. in Form einer GAP-Analyse bereitgestellt werden kann. Solche Analysen zeigen, wo die Klinik mit Blick auf den B3S Krankenhaus steht, welche Maßnahmen erforderlich sind, um den aktuellen Stand der IT-Technik zu erreichen und welcher Zeit- und Kostenaufwand dafür in etwa nötig ist.

Veröffentlichungen zum Thema

§ „Handlungsempfehlungen zur Verbesserung der Informationssicherheit an Kliniken“, Branchenarbeitskreis (BAK) medizinische Versorgung, 2017

§ „Handlungsempfehlung Digitalisierung und Patientensicherheit“, Aktionsbündnis Patientensicherheit (APS), 2018

Eine wichtige Rolle kommt schließlich den Beschäftigten zu. Die Oberste Leitung ist in der Pflicht, Mitarbeiter abzuholen und mitzunehmen auf Ihrem „Segelturn in die Zukunft“ – über Jahre und Jahrzehnte gewachsene, teils wie in Stein gemeißelte Rollen und Handlungen können in den seltensten Fällen mit einem Handstreich verändert werden.

Welche Fördermöglichkeiten es gibt

Im Jahr 2020 wurde im Rahmen des Krankenhauszukunftsgesetzes der sog. Krankenhauszukunftsfonds eingerichtet, der Fördergelder für kleinere Kliniken, die nicht unter die Kritischen Infrastrukturen fallen, bereithält. Dabei geht es um die Förderung der Digitalisierung in Krankenhäusern, eine Bewilligung ist konkret mit Maßnahmen zur Verbesserung der IT-Sicherheit verbunden. Anträge können jedoch nur noch bis Ende 2021 gestellt werden.

Fazit

Kliniken, die von der neuen Regelung betroffen sind, sollten ihre IT-Systeme zeitnah auf den neuesten Stand bringen und sich dabei am besten am B3S Krankenhaus orientieren. Es empfiehlt sich, zur Implementierung des ISMS externe Hilfe in Anspruch zu nehmen und die Ende 2021 auslaufende Förderung für entsprechende Maßnahmen schnellstens zu beantragen.

Nutzerverständnis für digitale Sicherheit stärken

IT-Sicherheit für Kliniken hat für Dr. Klaus Rummel hohe Bedeutung. Der Facharzt für Radiologie, medizinische Informatik betont im Interview mit dem Krankenhaus IT Journal: Für verantwortliche Nutzer ist der verhaltensbasierte Ansatz zu stärken.

Welches sind die wichtigsten Herausforderungen der IT-Sicherheitslage im Krankenhaus durch die Corona-Pandemie?

Klaus Rummel: Eine Herausforderung durch die Corona-Pandemie ist sicher der schnelle Wechsel in den Anforderungen. Die notwendige Flexibilität darf hierbei keine Lücken in den Sicherheitsbarrieren erzeugen, weder im Haus noch bei neu geschaffenen mobilen Arbeitsplätzen oder den Nutzern. Ein anderes Thema ist das Krankenhauszukunftsgesetz, das eine Vielzahl digitaler Innovationen in die Krankenhäuser bringen wird. Das Gesetz sehe ich als große Chance, die kurze, zur Verfügung stehende Zeit für die jeweils individuelle Rahmenplanung aber auch als große Herausforderung. Die jetzt eingesteuerten Veränderungen werden über Jahre wirken. Besonderes Augenmerk muss daher der IT-Sicherheit gelten, um diese vom historisch bedingten Baustein in ein Fundament medizinischer IT-Nutzung umzuwandeln.

Welche besonderen Handlungsempfehlungen können Sie zur Bewältigung neuer Risiken für die IT-Sicherheit geben?

Klaus Rummel: Neben den technischen Sicherheitsrisiken ist der Anwender ein wesentliches Ziel von Attacken, und damit Einfallstor für Schadsoftware. Mit zunehmend verteilten Arbeitsplätzen und einer technisch und inhaltlich deutlichen Verbreiterung der Angriffsfläche wird es wichtiger, IT-Nutzern ihre Rolle als eine Art menschlicher Firewall näherzubringen. Niemals vorher gab es so viele Berührungspunkte zwischen der beruflichen Tätigkeit und dem privaten Bereich, die eine Stärkung des verhaltensbasierten Ansatzes erfordern. Die Anleitung von Mitarbeitern und der Erfahrungsaustausch mit den IT-Nutzern sollten den Raum bekommen, der dem Risiko entspricht.

Welche Botschaft ist für Verantwortliche aus Krankenhäuser vor allem wichtig?

Klaus Rummel: IT-Audits, Penetrationstests und Vorträge zu IT-Sicherheit und Datenschutz durch Dritte boomen. Dadurch entsteht eine immer länger werdende Liste an Vorgaben und Checklisten von externen Quellen, wohingegen die eigentlichen Wissensträger die Krankenhäuser selbst sind. Ich kann mich an keine Zeit erinnern, in der

die Digitalisierung im Gesundheitssektor derart gefördert und herausgefordert wurde, wie dies momentan geschieht. Andererseits war die IT-Sicherheit noch nie so bedroht wie heute, und die Regeln des Datenschutzes waren noch nie so präzise. Dies ist eine exzellente Zeit, um über Wege nachzudenken, die eine zunehmende Vernetzung mit den Anforderungen des Datenschutzes und einer mitwachsenden IT-Sicherheit in Einklang bringen können. Eine nachhaltige digitale Zukunft in den Krankenhäusern kann aber nur entstehen, wenn hierbei nicht Technologien handlungstreibend sind, sondern digitale Lösungen, die die Abläufe rund um den Menschen und Patienten weiter verbessern. Verlässliche Daten aus multiplen Quellen am Ort der Behandlung sind dafür nur eine Basis.

Dr. med. Klaus Rummel, Informationstechnologie, Medizinisches Prozessmanagement: „Eine nachhaltige digitale Zukunft in den Krankenhäusern kann aber nur entstehen, wenn hierbei nicht Technologien handlungstreibend sind, sondern digitale Lösungen, die die Abläufe rund um den Menschen und Patienten weiter verbessern.“



Malware - Ein Blick aus medizinischer Perspektive

Wenn jede Malware eine Erkrankung wäre, könnte man sie nach dem auslösenden Agens (z.B. Virus) einordnen und nach der Art der Verbreitung (z.B. Netzwerk) und Vermehrungsart (Sporenbildend). Wir wüssten, dass Abstand und Hygiene helfen.

Wir würden unser Verhalten auf das Risiko selektiv abstimmen. Wir würden bereits bei einem Verdacht zum „Arzt“ gehen ... und es gäbe neben einer Impfung (spezifische Antikörper) auch selektive Medikamente und Breitbandtherapeutika.

- Die Abläufe von Diagnostik und Therapie wären Fachrichtung zugeordnet, weil das Gebiet immer größer geworden war.
- Es gäbe globale Forschung.
- Vielleicht würde eine Pandemie ausgerufen. Aber immer noch würde gelten: Es gibt keine abrechenbare DRG für ein gesundes IT-System.

Das digitale Krankenhaus – aber mit Sicherheit

Digitale Anwendungen setzen sich in deutschen Kliniken immer stärker durch, beschleunigt durch das Krankenhauszukunftsgesetz und die Covid19-Pandemie. Das macht Krankenhäuser zugleich angreifbarer für Attacken von außen. Wie können sich die Häuser am besten schützen – worauf kommt es beim Thema Informationssicherheit an? Ein Überblick von Jörg Asma und Benedict Gross, PwC Deutschland. Beide sind Ansprechpartner für die Themen Digitalisierung und Sicherheit im Krankenhaus.

„Digitalisierung beschleunigen“ – das besagt eine Forderung aus einem Positionspapier zur 20. Legislaturperiode des künftigen Bundestags. Denn der Einsatz von Technologien wie E-Health, Künstlicher Intelligenz, Robotik und Big Data ist vielversprechend: Sie können die Versorgung in Kliniken verbessern und das medizinische Personal entlasten, etwa bei administrativen Aufgaben oder der Entscheidungsfindung. Entsprechend dynamisch entwickelt sich die digitale Transformation in Krankenhäusern weiter.

Gleichzeitig braucht die Digitalisierung in Krankenhäusern eine belastbare und sichere Infrastruktur. Denn die Gefahr durch Cyberangriffe in Deutschland ist groß – jährlich entstehen nach Schätzungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) branchenübergreifend Schäden in zweistelliger Milliardenhöhe. Gerade für Krankenhäuser hat sich die Bedrohungslage verschärft; sie stehen im Visier von Cyberkriminellen, wie beispielsweise der Angriff auf das Universitätsklinikum Düsseldorf gezeigt hat.

ZWISCHEN IT-SICHERHEIT & INNOVATION PASST KEIN „ODER“



Dell Latitudes der 9000 Serie
Premium-Notebooks mit integrierter KI

Digitalisierung und IT-Compliance stellen wachsende Herausforderungen an das Management von Krankenhäusern und Kliniken. Spezialisiert auf zertifizierte IT-Lösungen für regulierte Branchen, entwickelt die Ratiodata maßgeschneiderte Konzepte, die auf dem Einsatz neuester Technologien basieren.

Die Ratiodata ist Premium-Partner der weltweit führenden IT-Hersteller. Die Hardware von Dell ist fester Bestandteil unserer Multivendor-Strategie.

Als mehrfach ausgezeichnetes Systemhaus und prämierter „Bester Managed Service Provider“ integriert und serviciert die Ratiodata IT-Hardware und -Lösungen mit höchster Effizienz und Zuverlässigkeit. Mit 20 Kompetenzzentren und 2.300 Mitarbeitern in drei Ländern erreichen wir partner-schaftliche Kundennähe.



Einfach per QR-Code den
Dell Latitude 2-in-1
auf dem Weg zum Kunden erleben.

Ratiodata AG
Lyoner Straße 9 | 60528 Frankfurt a. M.
Tel. +49 69 38076-0 | www.ratiodata.de

Das Fundament für Resilienz: ein Security-Architekturmodell

Keine Frage – Digitalisierung und Sicherheit müssen Hand in Hand gehen, gerade in Krankenhäusern, die zu den Kritischen Infrastrukturen zählen und in denen es um die Gesundheit und das Leben von Menschen geht. Was heißt das in der Praxis für die Informationssicherheit von Kliniken? In zahlreichen Krankenhäusern ist die IT historisch gewachsen und zum Teil veraltet, zusätzlich gibt es eine Fülle von Datenquellen, Endgeräten und Schnittstellen. Vielfach fehlt den Häusern noch eine übergreifende Digitalstrategie. Das macht sie verwundbar für Angriffe von außen.

Wir empfehlen daher die Arbeit mit einem Enterprise-Security-Architekturmodell, das alle Schnittstellen aus technologischer und prozessualer Sicht schematisch abbildet. Ein solches Modell ist die Grundlage für Informationssicherheit und erhöht die Widerstandsfähigkeit einer Organisation. Es stellt sicher, dass ein Krankenhaus seine Unternehmensziele erreichen kann – ein Grund, warum die Sicherheitsarchitektur im Management angesiedelt ist. Mit einem systematischen Vorgehen durch ein Architekturmodell ist dafür gesorgt,

dass einerseits die organisatorischen und technischen Sicherheitsanforderungen des Krankenhauses erfüllt werden, andererseits aber der operative medizinische Betrieb rund um die Uhr reibungslos laufen kann, um Patientensicherheit zu gewährleisten.

Die verschiedenen Nutzergruppen von Anfang an einbinden

Diese komplexe IT-Sicherheits-Architektur braucht eine klare Verantwortlichkeit. Im Idealfall ist sie beim Chief Information Security Officer (CISO) angesiedelt oder, in Kliniken, die sich schon deutlicher für die digitale Zukunft aufgestellt haben, beim Chief Information Officer (CIO). Diese Verantwortlichen bündeln die Anforderungen, die sich aus den verschiedenen Stakeholder-Gruppen im Krankenhausbetrieb ergeben. Es ist wichtig, die verschiedenen Abteilungen wie Ärzteschaft, Pflegekräfte, Hygienebeauftragte, IT-Spezialisten, Verantwortliche für Krankenhauslogistik etc. in die Planung einzubeziehen. Durch die interdisziplinäre Zusammenarbeit ist sichergestellt, dass alle Interessen einbezogen werden und Fragen der Sicherheit von Anfang an mitgedacht werden. Dabei können durchaus verschiedene Interessen aufeinandertreffen, etwa die Ziele der Usability und der Sicherheitsanforderungen wie beim Thema Passwortsicherheit oder der Verschlüsselung von Mails.

Interdisziplinäre Zusammenarbeit ist auch ein entscheidender Faktor, wenn es um die Wahl des richtigen Dienstleisters geht. Derzeit kommen viele Anbieter im Zuge des Krankenhauszukunftsgesetzes auf Kliniken zu. Dabei fällt es vielen Häusern schwer, das richtige Angebot auszuwählen. Wir empfehlen in jedem Fall, auf einen integrierten Anbieter zu setzen, der Digitalisierung und Sicherheit nicht nur in Einzelteilen denkt, sondern auch in einen Kontext der Gesamtarchitektur stellen kann. Nur so kann die Komplexität des Themas gefasst werden.



Dr. Benedict Gross, Senior Manager,
PricewaterhouseCoopers WPG GmbH,
benedict.gross@pwc.com

Erste Hilfe für den Ernstfall

Grundsätzlich geht es auch darum, für das Thema Informationssicherheit ein Bewusstsein zu schaffen. Viele Krankenhäuser sind sich noch immer nicht im Klaren darüber, wie schnell sie aus wirtschaftlichen oder politischen Interessen zum Angriffsziel werden können und wie verwundbar sie sind. Medizinische Sicherheit wird im Krankenhaus zwar großgeschrieben, eine IT-spezifische Sicherheitskultur hingegen noch vernachlässigt. Auch nach unserer Erfahrung ist Informationssicherheit in vielen Krankenhäusern noch immer ein erschreckend blinder Fleck – die IT ist in den Krankenhausnotfallplänen vielfach gar nicht abgebildet. Dabei kommt es gerade im Ernstfall auf eine gute Vorbereitung an. Entscheidend ist dabei aus unserer Sicht, dass Krankenhäuser ein Notfallszenario in der IT einmal pro Jahr üben. Entscheidend ist auch ein Krisenstab, der einen strategischen Krisenreaktionsplan erstellt. Wie unsere PwC-Studie „Global Crisis Survey 2021“ zeigt, können Unternehmen mit solch einer Vorbereitung ihren Betrieb schneller wieder aufnehmen. Das belegt: Informationssicherheit ist immer auch ein strategisches Thema.



Jörg Asma, Partner, PricewaterhouseCoopers
WPG GmbH, joerg.asma@pwc.com

Sicher aufgestellt
für die **digitale**
Krankenhauszukunft
dank **interoperabler**
Patientenakten.



Lesen Sie die
ArchivAktiv
jetzt als ePaper





Cyber Security im Krankenhaus – auch eine Frage des Managements

Der vermehrte Einsatz von IT-Lösungen sowie die Verwertung und Speicherung sensibler Gesundheitsdaten stellt Kliniken vor eine grundlegende Sicherheits-Herausforderung.

IT-Systeme müssen mit der rasanten technischen Weiterentwicklung Schritt halten.

Krankenhäuser sind dazu aufgerufen, nicht nur ihre IT-Systeme aktuell zu halten, sondern auch das eigene IT-Sicherheitsbewusstsein zu steigern – von der Geschäftsführung bis hin zum Anwender. Von Bjoern Wolf und Michael Happ, Unity AG

Die Mehrzahl der Cyber-Angriffe findet auf bekannte Sicherheitslücken statt, für die es Patches gibt. Weiterhin wird bei der Implementierung von IT-Sicherheitsmaßnahmen häufig das Client Management außer Acht gelassen. Da es die Durchführung von Sicherheitsupdates für Betriebssysteme und Anwendungen sowie Software-Aktualisierungen gewährleistet, ist es jedoch von hoher Bedeutung für die IT-Sicherheit eines Krankenhauses. Es gilt: Informationssicherheit ist ein kontinuierlicher Prozess, der nie endet.

Gefahren erkennen und reduzieren

Gegenwärtig häufen sich Angriffe, bei denen IT-Systeme der Kliniken von sogenannter Ransomware befallen werden und der Betrieb zeitweilig eingestellt

werden muss. Kliniken können die Auswirkungen eines Ransomware-Angriffs deutlich reduzieren, indem sie aktuelle Sicherheitstechniken einsetzen und das Backup entsprechend anpassen. Ransomware verschlüsselt Datenbestände und kann Backups ausschalten, um den Zugriff auf gespeicherte Daten zu verwehren. Dennoch lassen sich derartige Erpressungsangriffe nicht als Hack des Systems auffassen: Denn die beispielsweise per Mail eingeschleusten Schadprogramme nutzen lediglich die Berechtigungen aus, die der betroffene Anwender ohnehin hat. Krankenhäuser sind also dringend dazu aufgerufen, nicht nur ihre IT-Systeme aktuell zu halten, sondern auch das eigene IT-Sicherheitsbewusstsein zu steigern – von der Geschäftsführung bis hin zum Anwender. Um einen wirksamen Schutz zu

erreichen, muss der betroffenen Organisation bewusst sein, an welcher Stelle ein erhöhtes Risikopotenzial besteht. Für die meisten Krankenhäuser stellt das Mapping der Unternehmensrisiken auf die IT-Systeme eine signifikante Herausforderung dar.

Kernsteuerungselement ist das Risikomanagement

Im Rahmen einer Risikoanalyse sollten zunächst konkrete Risiken identifiziert und auf ihre Eintrittswahrscheinlichkeit sowie das mögliche Schadensausmaß geprüft werden. Dabei sollten sich die IT-Sicherheitsrisiken eng an den Unternehmensrisiken orientieren. Aus dem entstehenden Risikocluster lassen sich Handlungsbedarfe und Maßnahmen zur Eindämmung möglicher Gefahrenpotenziale ableiten und im Hinblick auf

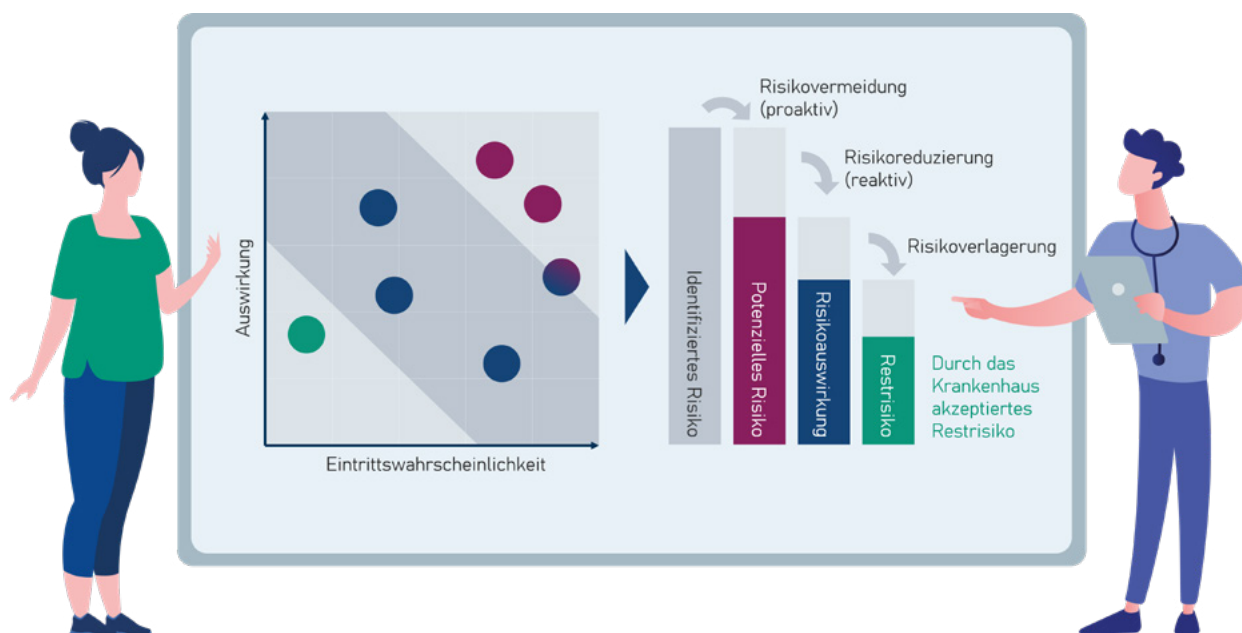


Abb: Vom Risiko zum Restrisiko

Kosten und Nutzen bewerten. Die individuelle Bewertung der kritischen Komponenten der IT-Systeme ist ratsam, da ein hohes Schutzniveau für die gesamte IT-Infrastruktur in der Regel nicht kosteneffizient ist. Für die Umsetzung empfiehlt sich das Vorgehen nach einem klassischen PDCA-Zyklus (Plan, Do, Check, Act). In einer iterativen Schleife werden die strategischen Themen festgelegt, umgesetzt, geprüft und bei Bedarf korrigiert.

Wirksame Leitlinien und gesetzliche Vorgaben

Mit dem Patientendatenschutzgesetz (kurz: PDSG) sind ab dem 1. Januar 2022 alle Krankenhäuser in Deutschland



Björn Wolf, Leiter IKT, Unity AG

gesetzlich dazu verpflichtet, angemessene Schutzmaßnahmen zur IT-Sicherheit zu treffen. Bisher betraf dies nur Krankenhäuser, die zur kritischen Infrastruktur (kurz: KRITIS) gehören.

Gleichzeitig hat der Bund mit dem Krankenhauszukunftsgesetz (kurz: KHZG) einen 4,3 Milliarden Euro starken Fond zur Digitalisierung deutscher Kliniken zur Verfügung gestellt. Ein Anteil von mindestens 15% der Förder-summe muss dabei für die Verbesserung der Informationssicherheit eingesetzt werden. Auch hier wird der Aufbau eines Management-Rahmens fokussiert – das Information Security Management System (kurz: ISMS) soll anhand definierter Abläufe und Richtlinien die Informationssicherheit in der Organisation sicherstellen. Es wird deutlich: Informationssicherheit betrifft nicht nur die IT-Abteilung, sondern wesentlich die Führung, das Managementsystem und die Mitarbeiter. Hier stellt beispielsweise die Rückführung sogenannter Schatten-IT eine wesentliche Herausforderung dar. Die eigenständige Beschaffung und Nutzung von IT-Diensten und Geräten durch Ärzte und Fachbereiche scheint zwar einfach und schnell – sie verursacht



Michael Happ, Produktmanager Cyber Security, Unity AG

jedoch ein erhöhtes Risiko in den Bereichen Informationssicherheit, Datenschutz und Integrierbarkeit. Hier stehen die Krankenhausverantwortlichen in der Pflicht, die IT-Sicherheit entlang eines klaren Managements zu verankern und die IT zu befähigen, die gewünschten und erforderlichen Services zur Verfügung zu stellen.

Zusätzlich zur internationalen Norm zur IT-Sicherheit (ISO 27001) setzt die Deutsche Krankenhausgesellschaft den branchenspezifischen Standard (B3S), um eine prozessorientierte und risikobasierte Herangehensweise zum Erreichen der gesetzten Informationssicherheitsziele bereitzustellen.



Das Krankenhaus aus der externen Sicht eines Hackers – ein Lagebild

Bei einer Analyse von im Internet öffentlich zugänglichen Systemen und Informationen von deutschen Krankenhäusern zeigten sich zahlreiche Cybersecurity-Schwachstellen. Merke: Gerade nicht beachtete Systeme werden von Angreifern als Eintrittsvektor in das Netzwerk genutzt – auch bei größeren KRITIS-Krankenhäusern. Von Johannes Klick, Alpha Strike Labs, Internet Scanning Expert

Durch die Covid-19-Pandemie wurde uns in der Gesellschaft wieder bewusst, welchen Stellenwert Krankenhäuser und deren Einsatzbereitschaft haben. Gleichzeitig häufen sich die Meldungen über erfolgreich angegriffene Krankenhäuser zunehmend. So wurde im Herbst 2020 der Anbieter Universal Health Services Inc. von einem Ransomware-Angriff getroffen. Mit Ryuk wurden die Dienste von 250 US-Krankenhäusern und Kliniken lahmgelegt und Einrichtungen im ganzen Land in Mitleidenschaft gezogen. In Düsseldorf musste das Universitätsklinikum im Oktober letzten Jahres seine Notaufnahme abmelden, weil es schwer von einem Ransomware-Angriff getroffen wurde.

Das deutsche Sicherheitsforschungsunternehmen Alpha Strike Labs hat diese Cyber-Angriffe auf Krankenhäuser als Anlass genutzt, um die öffentlich über das Internet erreichbaren Netzwerkdienste auf Schwachstellen zu untersuchen. Ein Drittel der analysierten Krankenhäuser weist Schwachstellen auf. Werden diese systematisch von Cyberkriminellen missbraucht, kann das zu einem nationalen Sicherheitsrisiko werden.

Alpha Strike Labs scannt regelmäßig und weltweit das Internet (2,8 Milliarden IPv4 Adressen) nach verwundbaren Netzwerkdiensten mit Hilfe einer selbst entwickelten Suchmaschine und fortgeschrittenen Big-Data Algorithmen. Als Basis für die Analyse wurde das DIVI-

Register verwendet, welches ca. 1300 Krankenhäuser mit COVID-19 Intensivstationen namentlich beinhaltet

Die Datenauswertung von mehr als 89 verschiedenen globalen Internetscans mit einem analysierten Datenvolumen von 1483 GB ergab, dass 1555 Krankenhäuser über 13.000 extern erreichbare Netzwerkdienste verfügen. 32 Prozent der analysierten Dienste wurden in unterschiedlichem Ausmaß als verwundbar eingestuft. Jedes Dritte Krankenhaus weist eindeutige Angriffspunkte auf. Insgesamt konnten mehr als 900 kritische Schwachstellen identifiziert werden.

Die Abbildung 1 zeigt eine Karte, welche auf der linken Seite die Standorte der DIVI-Krankenhäuser darstellt. Auf der rechten Seite der Abbildung befindet sich eine Karte mit schwachstellenbehafteten DIVI-Krankenhäusern. Es lässt sich gut erkennen, dass schwachstellenbehaftete Krankenhäuser sowohl im ländlichen als auch im städtischen Bereich gleichermaßen betroffen sind.

Unter der Berücksichtigung der Bettenkapazitäten der einzelnen Krankenhäuser zeigen sich weitere interessante Ergebnisse. So stellt Abbildung 2 dar, dass die Anzahl der Schwachstellen proportional mit der Anzahl der Betten je Krankenhaus steigt.

Dies war zu erwarten, denn die zunehmende Größe eines Krankenhauses führt zu mehr Abteilungen, mehr IT-Systemen und erhöhter Komplexität und somit meist auch zu mehr Schwachstellen. Jedoch würde man meinen, dass Krankenhäuser mit mehr als 30.000 vollstationären Behandlungen im Jahr und somit in die KRITIS-Verordnung fallen, besser aufgestellt sind als Krankenhäuser, die nicht unter die KRITIS-Verordnung fallen. Abbildung 2 zeigt allerdings ein gegenteiliges Ergebnis. Es lässt sich sehr gut erkennen, dass insbesondere die Mehrheit der größeren KRITIS-Krankenhäuser sicherheitstechnisch nicht besser aufgestellt sind als die nicht KRITIS-Krankenhäuser.

Der aufmerksame Leser mag nun argumentieren, dass es sich bei vielen der verwundbaren Systeme wahrscheinlich eher um weniger wichtige oder vergessene Legacy-Systeme handelt. Doch gerade diese nicht beachteten Systeme werden von Angreifern als Eintrittsvektor in das Netzwerk genutzt. Um dies zu verhindern, empfiehlt es sich, ein Netzwerk in verschiedene Sicherheitssegmente aufzuteilen. So wie die Schottsegmente in der Schifffahrt, ermöglichen verschiedene Sicherheitssegmente einen Angriff auf einen lokalen Teil eines Netz-

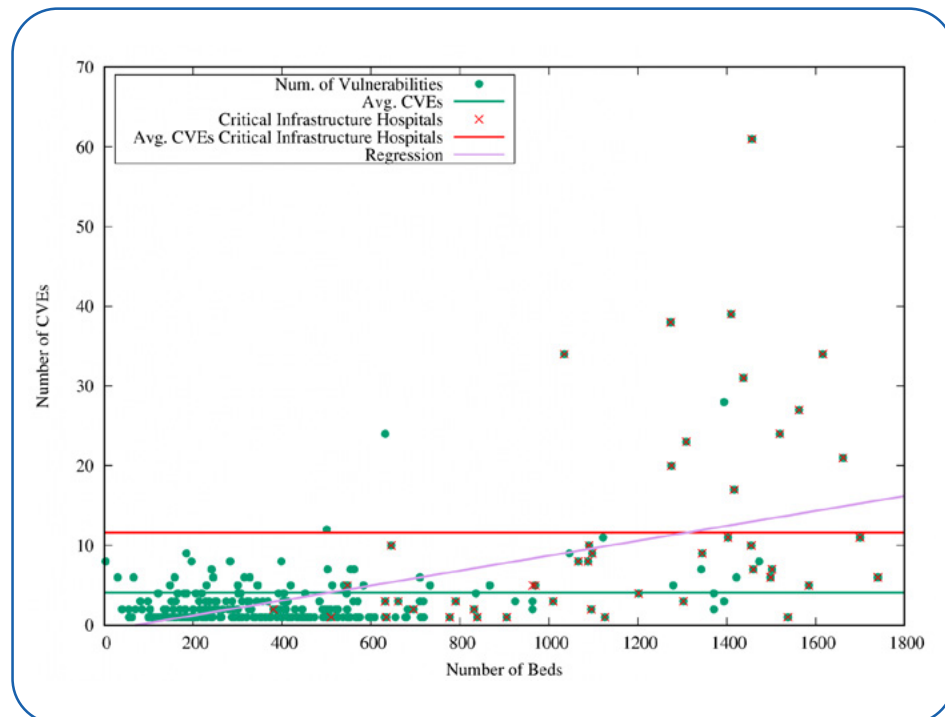


Abb.1

werkes zu begrenzen. Oft wähnen sich Unternehmen sicher, wenn sie eine § 8a Prüfung gemäß BSI-Gesetz oder eine ISO27001-Zertifizierung durchlaufen haben. Die Praxis zeigt, dass bei diesen Prüfungen oft nur die Papierdokumentation der Sicherheitsprozesse überprüft werden. Technische Prüfungen von z.B. Firewall- und Routerkonfiguration oder Aktualität der letzten Security-Patches für eingesetzte Netzwerkkomponenten und Serverbetriebssysteme oder -applikationen werden oft nicht durchgeführt. Neben technischen Maßnahmen fehlen häufig auch ausreichende Personalressourcen und grundlegende gelebte Prozesse, die für ein gut funktionierendes Asset-, Patch- und Schwachstellenmanagement notwendig sind.

Viele Organisationen wissen gar nicht, welche ihrer Systeme im öffentlichen Internet erreichbar sind. Mit der Open Source Intelligence (OSINT)-Plattform, die auch für die Erstellung der Studie verwendet wurde, kann sehr schnell Transparenz geschaffen werden, um mögliche Ziele von Angreifern fernzuhalten.



Johannes Klick, CEO & Co-Founder von Alpha Strike Labs, Internet Scanning Expert. Alpha Strike Labs bildet eine eigene F&E-Einheit innerhalb der Limes Security mit dem Fokus auf Schwachstellenforschung, neuen Angriffsmethoden, besserer Angriffserkennung mit Honeypots und OSINT/Threat Intelligence. Außerdem fungiert Alpha Strike Labs als Inkubator für Produkt- und Service-Ideen.



IT für hochsichere Patientenversorgung

Herausforderungen für Krankenhäuser im Kontext von IT-Sicherheit, Impulse und Handlungsempfehlungen gibt Markus Holzbrecher-Morys. Der Geschäftsführer, Dezernat III / IT, Datenaustausch und eHealth, Deutsche Krankenhausgesellschaft e.V., Berlin, richtet seine Tipps an die Verantwortlichen der Krankenhaus IT. Credo: Die IT-Sicherheit der wichtigen Systeme und Prozesse für die Patientenversorgung ist unbedingt zu gewährleisten.

Welches sind die wichtigsten Herausforderungen für Krankenhäuser im Kontext von IT-Sicherheit, besonders bei branchenspezifischen Sicherheitsstandards?

Markus Holzbrecher-Morys: Die IT-Sicherheit der für die Patientenversorgung wichtigen Systeme und Prozesse zu gewährleisten, stellt neben dem Investitionsbedarf insgesamt hohe Anforderungen an den Betrieb und das dafür zuständige Personal in den Krankenhäusern. Die Anforderungen wachsen dabei mit dem zunehmenden Grad an Digitalisierung stetig an. Dabei geht es um mehr als die Umsetzung konkreter technischer Sicherheitsmaßnahmen – Informationssicherheit, die neben der IT-Sicherheit auch Datenschutzerfordernungen berücksichtigt, muss auf allen Ebenen wahrgenommen, umgesetzt und in den Prozessen gelebt werden. Dafür müssen die notwendigen Ressourcen, insbesondere die personellen und finanziellen Mittel für die Umsetzung entsprechender Sicherheitsmaßnahmen, bereitstehen. Mit dem Krankenhauszukunftsgesetz werden hier wichtige Impulse gesetzt. Eine dauerhafte Finanzierung von IT-Sicherheit im Krankenhaus ist damit aber keinesfalls gewährleistet. Besondere Sorge bereitet zudem die Fachkräftesituation, denn es bedarf eben vor allem der entsprechend geschulten Mitarbeiter, um IT-Sicherheit im Krankenhaus umzusetzen. Aber auch konkrete Anforderungen des Gesetzgebers, wie beispielsweise die erwartete Verpflichtung für die Umsetzung von Einbruchserkennungssystemen (Intru-

sion Detection) im IT-Sicherheitsgesetz 2.0, erhöhen die Herausforderung an die Umsetzung. Dafür bedarf es einer entsprechenden Umsetzungszeit, die nicht kürzer sein kann, als der Gesetzgebungsprozess selbst.

Welche hauptsächlichen Handlungsempfehlungen können Sie geben?

Markus Holzbrecher-Morys: Zunächst ist es wichtig, das Thema „IT-Sicherheit“ nicht als Aufgabe der IT-Abteilung zu verstehen. Informationssicherheit liegt im Verantwortungsbereich der Geschäftsführung, wir empfehlen daher im branchenspezifischen Sicherheitsstandard (B3S) die Benennung eines Informationssicherheitsbeauftragten, welcher direkt der Geschäftsführung unterstellt ist. Seine Aufgabe besteht ja gerade auch in der Überprüfung der Aufgabenerfüllung der Informationstechnik, er sollte in alle relevanten Prozesse, welche die Informationssicherheit betreffen, eingebunden sein - beispielsweise auch in Beschaffungsprozesse, um auf wesentliche Merkmale, wie „security by design“ oder „privacy by design“ hinweisen zu können.

BSIG-Gesetz §8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen Zusammenfassung

Betreiber sind nach §8a Abs. 1 BSIG zur Umsetzung von angemessenen Sicherheitsmaßnahmen verpflichtet („Stand der Technik“).

Betreiber müssen nach §8a Abs. 3 BSIG die Umsetzung entsprechender Maßnahmen regelmäßig (spätestens alle 2 Jahre) nachweisen.

Das BSI nimmt nach §8b BSIG die Aufgabe einer zentralen Meldestelle für sicherheitsrelevante Informationen wahr.

**Betreiber haben nach §8b Abs. 2 BSIG ein Informationsrecht gegenüber dem BSI.
Betreiber müssen nach §8b Abs. 4 BSIG IT-Störungen an das BSI melden.**

Weiter ist es erforderlich, die relevanten Prozesse und Systeme einmal vollständig zu erfassen und zu hinterfragen, ob diese im Einzelnen sinnvoll ausgestaltet sind. Dies kann schnell aufwendig werden und „den Berg an Arbeit“ zu groß erscheinen lassen. Hier sollte man im Zweifel iterativ vorgehen und dabei mit den wichtigsten Prozessen zuerst anfangen. Dafür bedarf es jedoch einer Einschätzung dieser Prozesse – hier ist klassisches Risikomanagement gefragt. Der B3S schlägt hier einen Standardrisikomanagementprozess vor.

Ist Informationssicherheit erst einmal als Querschnittsaufgabe auf allen Ebenen „angekommen“, bedarf es auch regelmäßiger Awareness- und Schulungsmaßnahmen, um die Mitarbeitenden in den Krankenhäusern in der täglichen Arbeit regelmäßig zu sensibilisieren.

Was wollen Sie den Verantwortlichen aus Krankenhäusern vor allem mitgeben?

Markus Holzbrecher-Morys: Verstehen Sie Informationssicherheit als wesentliche Voraussetzung für die Digitalisierung im Krankenhaus. Begreifen Sie dies als Querschnittsaufgabe, welche die Unterstützung von der Geschäftsführung des Klinikverbundes bis zur Pflegekraft auf Station benötigt, um die tägliche Patientenversorgung so sicher wie möglich zu machen.



Markus Holzbrecher-Morys. Der Geschäftsführer, Dezernat III / IT, Datenaustausch und eHealth, Deutsche Krankenhausgesellschaft e.V., Berlin: „Zunächst ist es wichtig, das Thema „IT-Sicherheit“ nicht als Aufgabe der IT-Abteilung zu verstehen.“



E-Health-Wachstum bedeutet auch KI, Big Data, Robotik und vernetzte OPs.

IT-Sicherheit in der Medizin: Auch an die Zusammenarbeit denken

Durch die zunehmende Verbreitung informationstechnischer Systeme in den Kliniken wachsen die Anforderungen an den sicheren Austausch von Daten. Technische Lösungen allein reichen nicht aus, um die Informationssicherheit strukturell zu gewährleisten. Genauso wichtig ist es, innerhalb der Organisation Verantwortung und Zusammenarbeit sicher zu stellen.

Von Philipp Michael, Business Support, Drägerwerk AG & Co. KGaA

Die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der IT-Systeme und Daten wird durch Maßnahmen gemäß des branchenspezifischen Sicherheitsstandards (B3S) gewahrt. [1] Vor diesem Hintergrund hat sich die Implementierung eines Informationssicherheits- und Managementsystems (ISMS) und zusätzlich ein Risikomanagement (RM) nach DIN EN 80001-1-Norm „Risikomanagement für medizinische IT-Netzwerke“ bewährt. Dadurch werden Sicherheitsmaßnahmen nicht allein auf technischen IT-Lösungen wie Sicherheit Gateways, Absichern der beteiligten IT-Komponenten oder einer sicheren Zugangsverwaltung reduziert. Ein Bericht des BSI zur Lage

der IT-Sicherheit in Deutschland sieht besonders in diesem Punkt noch Nachholbedarf und fordert Betreiber dazu auf, auch das IT-Risikomanagement in ihr Business Continuity Management (BCM) zu überführen. [2] Das Betriebliche Kontinuitätsmanagement oder auch BCM soll betriebliche Tätigkeiten oder Abläufe schützen, ohne die erhebliche Schäden beim Betreiber entstehen würden.

Eine integrierte Herangehensweise berücksichtigt neben der technischen Sicherheit auch die Zusammenarbeit innerhalb der Klinik: Das ISMS gehört klassisch in den Aufgabenbereich der IT, während der Risikomanager MIT das Risikomanagement verantwortet. Die

Geschäftsführung steht jedoch in der Generalverantwortung für die Umsetzung des ISMS und des Risikomanagements. Im Projektteam für das Implementieren eines ISMS arbeiten also neben den IT-Verantwortlichen, Risikomanagern und Prozessverantwortlichen auch die Krankenhausleitung sowie Mitarbeiter einzelner Fachabteilungen ja nach Bedarf mit. [3] Der Funktion des Medical IT-Riskmanagers kommt zusätzlich die Rolle eines Moderators zu, der die Kommunikation im Sinne der MIT-Norm zwischen Anwender, Medizintechnik, IT, Einkauf bis hin zum Lieferanten initiiert und dokumentiert. [4]



Integrierte Herangehensweise

Das BSI-Gesetz verpflichtet Betreiber kritischer Infrastrukturen angemessene organisatorische und technische Vorkehrungen zu treffen, um die Funktionsfähigkeit dieser Infrastrukturen zu schützen.^[5] Entsprechend verweist der branchenspezifische Sicherheitsstandard (B3S) auf die Normen DIN EN 80001 und ISO 27001 sowie „gültige technische Standards“. Das bedeutet keine einseitige Anforderung nur auf Seiten der Betreiber. Auch die Hersteller von Medizintechnik stehen in der Verantwortung ihren Teil für den sicheren Betrieb im Krankenhaus beizutragen. Die DIN EN ISO 14971:2020 regelt das Risikomanagement für Medizinproduktehersteller. Diese Norm bezieht sich auf ein abgeschlossenes Netzwerk eines Herstellers. Erst in Kombination mit der DIN EN 80001 erweitert sich der Rahmen, da diese Benchmark das Risikomanagement für die Medizinprodukte unterschiedlicher Hersteller integriert in ein IT-Netzwerk regelt. Während

die ISO 27001 Sicherheit von Medizintechnik integriert in die Infrastruktur der Organisation, also auch Abläufe und Prozesse zusätzlich in den Fokus nimmt und Rollen definiert. Durch das integrierte Vorgehen bei der Bekämpfung von IT-Sicherheitslücken sowohl auf technischer Seite als auch organisatorisch ist ein „Plan B“, sollte es zu einem Vorfall kommen, automatisch immer mitgedacht. Denn Verantwortliche und Abläufe sind für den Störfall bereits etabliert.



Philipp Michael,
Business Support, Dräger

Quellen:

- [1] Deutsche Krankenhaus Gesellschaft (Hrsg.): Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus, Berlin, 02.04.2019, S.6,9
- [2] BSI: Die Lage der IT-Sicherheit in Deutschland 2020, p.53
- [3] BSI: Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT – Leitfaden, 2013, p. 9f.
- [4] Tarras B., Universitätsklinikum Regensburg: IT-Infrastruktur – Risikomanagement bei der Beschaffung von vernetzter Medizintechnik, in: Klinik Einkauf, 2019, Thieme (<https://www.klinik-einkauf.de/aktuelles/beschaffung/detail/risikomanagement-bei-der-beschaffung-von-vernetzter-medizintechnik-a-41018>)
- [5] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG): § 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen



Sicherheitsprioritäten für hybrides Arbeiten: konsolidierte Cloud-Dienste verringern Angriffsflächen

Cyberattacken und Bedrohungen haben zugenommen, da Hacker die Verlagerung zu Remote- und Hybrid-Arbeit ausnutzen. Eine Umfrage bestätigt, dass es eine wachsende Verlagerung hin zu cloudbasierten Sicherheits- und SASE-Lösungen gibt.

Die Verlagerung zu dezentralem und hybridem Arbeiten ist eine der wichtigsten Veränderungen, die als Folge der Covid-19-Pandemie stattgefunden haben. Viele Unternehmen mussten in ihren verteilten Umgebungen Kompromisse bei der Netzwerkleistung und dem Schutz eingehen, weil sie mehrere verschiedene Produkte einsetzen, was zu einer komplexen Verwaltung und einer fragmentierten Bedrohungsübersicht führt. Unternehmen ermöglichen ihren Mitarbeitern den Remote-Zugriff auf Unternehmensressourcen. Dabei spricht das SASE-Modell die Einschränkungen traditioneller Netzwerkarchitekturen an und führt Netzwerk und Sicherheit in der Cloud zusammen.

Eine Umfrage ⁽¹⁾, an der 450 IT- und Sicherheitsexperten aus aller Welt teilgenommen haben, zeigt, inwieweit sich die Remote-Arbeit auf die Sicherheitslage der Unternehmen, die Betriebskosten und die Auswirkungen auf die Benutzer auswirkt:

Remote-Arbeit bringt ein erhöhtes Risiko mit sich: Laut 45 % aller Befragten sind Unternehmen mit der Umstellung auf Remote-Arbeit einem höheren Risiko von Cyberangriffen ausgesetzt. Die Branchen, die das höchste Maß an Cyberangriffen meldeten, waren das Finanzwesen (54 %), Versorgungsunternehmen (52 %) und die Fertigungsindustrie (47 %).

Herausforderungen in der Verwaltung: Die drei wichtigsten Probleme, mit denen sich IT- und Sicherheitsexperten auseinandersetzen müssen, sind die Skalierung der Leistung (46 %), die Bewältigung von Problemen mit dem Datenschutz und der Datenhoheit (42 %) sowie die Unterstützung des Fernzugriffs für nicht verwaltete Geräte der Mitarbeiter (40 %).

Strategien zur Skalierung des Fernzugriffs: Um die steigende Nachfrage nach Remote-Arbeiten zu befriedigen, geben 69 % der Sicherheitsexperten an, dass sie On-Prem-Kapazitäten hinzufügen; 66 % wechseln zu cloudbasierter Sicherheit und überraschenderweise tun 36 % beides.

Schutz von Apps, auf die aus der Ferne zugegriffen wird: Bei der Ermöglichung des Fernzugriffs auf Unternehmens-Apps halten 70 % die Sicherheit der Anwendungen gegen Cyberattacken und Zero-Day-Bedrohungen für sehr wichtig.

Einführung der SASE-Technologie: 94 % sind mit dem Secure Access Service Edge-Framework vertraut, aber die Akzeptanz nimmt langsam zu. 9 % haben es bereits implementiert und 21 % planen dies.

In diesem Rahmen zeigt die Umfrage eine doppelte Nutzung von Cloud- und On-Prem-Security. Aus Gründen der Zweckmäßigkeit ist es möglicherweise einfacher, Kapazitäten zu aktuellen Lösungen hinzuzufügen, als sie herauszureißen und durch komplett neue zu ersetzen. Möglicherweise ist dies aber auch Ausdruck eines schrittweisen Ansatzes bei der Einführung von cloudbasierten Diensten oder ein Ergebnis von Überlegungen zur Datenresidenz.

Dennoch nutzen 66 Prozent cloudbasierte Sicherheitsdienste, um den Fernzugriff zu skalieren, und 61 Prozent dieser Befragten halten cloudbasierte Sicherheitsdienste für die Skalierung des Fernzugriffs für entscheidend (darunter 83 Prozent der Führungskräfte). Aufgrund der langfristigen Auswirkungen, die das Arbeiten per Fernzugriff auf die Anforderungen an die Datensicherheit und die Architektur haben wird, gewinnen cloudbasierte Sicherheitsdienste und Secure Access Service Edge (SASE)-Technologie heute mehr denn je an Interesse, da sie die dringende Notwendigkeit lösen, schnelle Konnektivität und zuverlässige Sicherheit für jeden Benutzer unabhängig von Gerät, Standort oder Zielressource bereitzustellen. Da Benutzer überall arbeiten können, verbessern Cloud-Dienste die Leistung und Verfügbarkeit auf globaler Ebene.

(1) Hybrid workplaces need new security paradigms, checkpoint.com

Cloud Security 2021: Datendiebstahl gefürchtet – Datensicherheit geschätzt

Die Ergebnisse der Studie „Cloud Security 2021“ zeigen, dass die „Wolken“-Technologie in der öffentlichen Wahrnehmung zugelegt hat. Dies betrifft verschiedene Aspekte der Cloud-Sicherheit. Marktforscher von IDG und TÜV Süd befragten IT-Verantwortliche dazu in der DACH-Region.

Das Risiko eines Datendiebstahls in der Cloud ist die mit 35,5 Prozent meistgenannte Sorge der Studienteilnehmer. Dieses Ergebnis überrascht kaum, schließlich fungiert die Cloud quasi als Bank für die Daten der Nutzer. Etwas auffälliger hingegen ist das zweite zentrale Kriterium, auf welches die Befragten neben der weltweiten Verfügbarkeit von Daten besonderen Wert legen: Datenschutz liegt mit 38,9 Prozent an erster Stelle der schätzenswerten Vorteile der Cloud.

Datendiebstahl vs Datensicherheit: Nur auf den ersten Blick paradox

Dieses vermeintliche Paradoxon löst sich jedoch auf den zweiten Blick auf: Selbstverständlich sind Cloud-Nutzer um die Sicherheit ihrer Daten besorgt, schließlich sind diese häufig wertvoll und damit besonders schützenswert. Die Sorge hat folglich weniger mit der statistischen Wahrscheinlichkeit eines

Datendiebstahls zu tun, sondern vielmehr mit der Vorstellung eines Worst-Case-Szenarios. Denn vertrauliche oder gar geschäftskritische Daten möchte man nach Möglichkeit nicht in den falschen Händen wiederfinden.

Der Schutz personenbezogener Daten, insbesondere von Patienten- und Mitarbeiterdaten, hat große Auswirkungen auf das Vertrauen in ein Unternehmen. Da Cloud-Anbieter oft verschiedenen Rechtssystemen unterliegen und die Regelungen teilweise kollidieren, ist ein stärkerer Fokus auf Datenschutzkriterien bei der Auswahl von Cloud-Diensten angebracht.

Die Ergebnisse der Cloud Security-Studie zeigen, dass die Cloud in der öffentlichen Wahrnehmung deutlich an Zuspruch gewonnen und viel von ihrer anfänglichen Obskurität verloren hat. Denn die meisten Menschen in Deutschland haben mittlerweile Erfahrungswerte im Umgang mit der Cloud sammeln können.

rein medical
a JVCKENWOOD Company



Ergonomisch



Hygiene

24/7

Sicherheit



Qualität

Jeder OP ist anders - und wir sind darauf eingestellt. Neben technisch und hygienisch hochwertigen Wandeinbaukonsolen, OP-Feld-Monitoren und All-In One-Computern bieten wir eine skalierbare Software-Suite, mit deren Hilfe wir maßgeschneiderte Lösungen für den Bereich Medical IT realisieren.

Unser Team vereint Forschung und Entwicklung, Produktion und Vertrieb sowie Projektplanung und Service unter einem Dach.

Wir stehen mit über 20 Jahren Erfahrung im Medizin-Markt für Qualität, Innovation und zuverlässigen Service.



reinmedical.com

Schiefelage bei präventiver Cyberabwehr

Bei Maßnahmen gegen Cyberattacken scheint das deutsche Gesundheitswesen Nachholbedarf zu haben. So glaubt nur ein Drittel der Healthcare-IT-Entscheidungssträger in Deutschland, über genügend Tools und das Know-how im präventiven Kampf gegen Cyberbedrohungen zu verfügen. Dennoch sind zwei Drittel der Meinung, ihr Budget für IT-Sicherheit sei für die Anforderungen der nächsten zwei Jahre ausreichend. Dreiviertel der Healthcare-Organisationen haben während der Pandemie einen Cyberangriff verzeichnet.

Der wachsende Einsatz von - zum Teil auch komplexen - IT-Systemen legt allerdings auch die technologischen Schwachstellen im Gesundheitssystem offen. Insbesondere in Zeiten verstärkter Digitalisierungsinitiativen müssen Kliniken, Labore, Forschungseinrichtungen und Arztzentren verstärkt für die IT-Sicherheit ihrer Infrastruktur sorgen und entsprechend adäquate sowie nachhaltige Maßnahmen ergreifen.

Es gibt derzeit eine akute Bedrohungslage und viele Cyberangriffe auf das Gesundheitswesen [1]. Über ein Viertel (26 Prozent) der in Deutschland befragten Organisationen haben während der Pandemie mehr Attacken auf ihre IT-Infrastruktur erlebt. Insbesondere Spear-Phishing (43,5 Prozent) als Einfallstor stellt hierbei eine Gefahr dar. Ebenfalls sind Mitarbeiter, die über zu geringe Kenntnisse hinsichtlich digitaler Sicherheit verfügen oder die Sicherheitsvorschriften wissentlich ignorieren, ein Risiko, sagen 30 Prozent der in Deutschland befragten IT-Entscheidungssträger. Die Sorge, dass Patientendaten gefährdet seien, teilt mehr als ein Viertel (28 Prozent) aller Umfrageteilnehmer.

Laut der Studie haben mit 72 Prozent fast drei Viertel der deutschen Unternehmen im Gesundheitssektor während der Pandemie mindestens einen Cyberangriff verzeichnet. Ein leistungsstarker und proaktiver Cyberschutz ist demnach

für die zum Teil äußerst vulnerablen Systeme in Krankenhäusern, Pflegeeinrichtungen oder in anderen Organisationen des Gesundheitssektors wichtig.

Entsprechend dem Bundesministerium für Gesundheit (BMG) [2] ist für die erfolgreiche Weiterentwicklung unserer Gesundheitsversorgung das Vorantreiben der Digitalisierung die zentrale Voraussetzung. Um im Kampf gegen modernste Cyberangriffe gewappnet zu sein, sollten Maßnahmen über den Standardschutz, wie herkömmliche IT-Sicherheitslösungen, regelmäßige Updates und Patches hinausgehen.

Empfohlene Maßnahmen und Status Quo in Deutschland

- Für den Ernstfall einen Business Continuity Plan beziehungsweise einen Disaster Recovery Plan aufsetzen, der auch regelmäßig einer Prüfung hinsichtlich Sinnhaftigkeit und korrekten Mechanismen unterzogen wird. 67,3 Prozent der in Deutschland befragten IT-Entscheidungssträger im Gesundheitswesen verfügen über derartige Pläne für den Notfall.
- Unternehmen sollten ein dediziertes Budget für IT-Sicherheit bereithalten. Jedoch sind lediglich knapp zwei Drittel (63,3 Prozent) der Befragten der Auffassung, ihr IT-Sicherheitsbudget sei für künftige Anforderungen ausreichend.

Deutschland	Österreich	Schweiz
• Spear-Phishing: 43,5 • Spyware: 31,5 • Generische Malware-Angriffe: 27,8	• Spyware: 41,1 • Spear-Phishing: 38,4 • DDoS: 37,0 • Ungepatchte Programme: 30,1	• Spear-Phishing: 42,3 • Ransomware / ungepatchte Programme: jeweils 39,7
• Gezielter Angriff: 25,9 • Ransomware: 25,0 • DDoS: 22,2 • Ungepatchte Programme: 18,5	• Ransomware/Gezielter Angriff/ Gen. Malware: jeweils 26,0	• Gezielter Angriff/ DDoS: jeweils 37,2 • Spyware: 32,1 • Gen. Malware: 31

Rangfolge Cybersicherheitsherausforderung DACH

- Cloud-Software und -Aktivitäten über spezielle Sicherheits-Tools oder -Services schützen: In Deutschland setzt dies gemäß der Studie nicht einmal die Hälfte (46,7 Prozent) der Unternehmen im Healthcare-Sektor um.
- Unterstützung durch externe Sicherheitsexperten suchen und Threat Intelligence wie ein externes Cyber Security Operations Center (SOC) nutzen. Solche Managed Detection and Response-Services sind nicht nur für Großunternehmen interessant, sondern auch für den Mittelstand. Gerade einmal ein Drittel (37,3 Prozent) greift bislang auf derartige Expertise zurück und nur jedes fünfte Unternehmen (20,7 Prozent) aus dem deutschen Healthcare-Bereich setzt bisher auf ein eigenes SOC.
- Bestehende Sicherheitslösungen evaluieren und/oder nach einer (neuen) Lösung suchen. Immerhin ein knappes Drittel (32 Prozent) der Healthcare-Unternehmen in Deutschland machen sich hierzu aktuell Gedanken.
- Netzwerksegmentierung durchführen, das heißt kritische Systeme (wie Röntgengeräte, Computertomographie etc.) von der Büro-IT-Infrastruktur trennen: Diese wichtige Sicherheitsmaßnahme zum Schutz beispielsweise vor dem Verlust von Patientendaten setzen in Deutschland gerade einmal 28,7 Prozent um.
- Security Information and Event Management (SIEM) einsetzen. 27,3 Prozent der in Deutschland Befragten haben bereits ein SIEM.
- Die Schulung der Mitarbeiter ist von entscheidender Bedeutung für Cybersicherheit, denn menschliches Versagen aufgrund mangelnder Kenntnisse und mangelnden Bewusstseins sind die Hauptursachen für Cyber-Vorfälle. In Deutschland werden nur bei 26,7 Prozent der Unternehmen im Gesundheitssektor Cybersicherheitsschulungen abteilungsübergreifend für alle Mitarbeiter durchgeführt.

[1] Kaspersky-Studie "Patient Krankenhaus: zur IT-Sicherheitslage im Gesundheitswesen in Deutschland, Österreich und der Schweiz". Die Umfrage wurde von Arlington Research im Auftrag von Kaspersky im Mai 2021 durchgeführt.

[2] <https://www.bundesgesundheitsministerium.de/e-health-initiative.html>



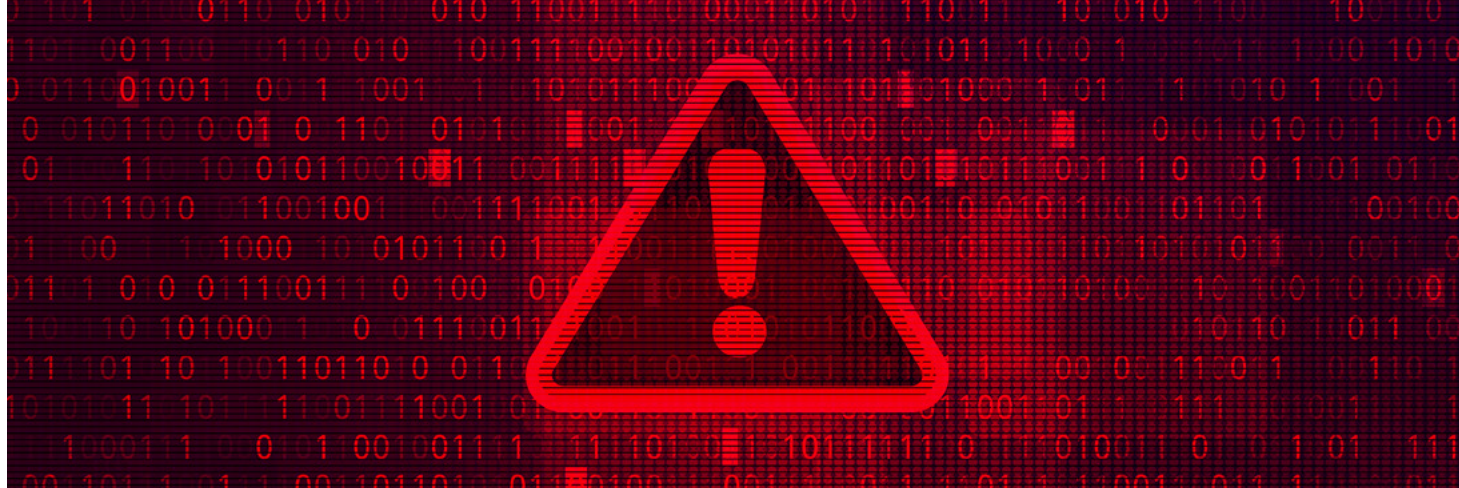
Der Konnektor für Krankenhäuser

Sicher und leistungsstark in die Telematikinfrastruktur

Wo Kommunikation zwischen Kliniken und der Telematikinfrastruktur geschützt werden muss, steht secunet bereit. Als IT-Sicherheitspartner der Bundesrepublik Deutschland bieten wir mit dem secunet konnektor die entscheidende und hoch performante Sicherheitskomponente zur vertrauensvollen Anbindung an die Telematikinfrastruktur.

secunet.com/konnektor protecting digital infrastructures

secunet



Hackerangriff: Wie die Universitätsklinik Düsseldorf mitten in der Krise die digitale Kommunikation umstellt

Kriminelle Cyberangriffe auf Kliniken häufen sich zunehmend. In einer Nacht im September 2020 ist es auch beim Universitätsklinikum Düsseldorf so weit: Plötzlich fallen weite Teile der Systeme aus. Nach einer Überprüfung wird klar: Das Klinikum ist Opfer eines Hackerangriffs und muss sich zunächst digital isolieren.

Die gewohnten Wege der Kommunikation funktionieren anschließend nicht mehr und insbesondere der Austausch von Befunden muss neu organisiert werden. Die Klinik findet eine Lösung, die auch vor dem Ausfall schon hilfreich gewesen wäre. Dr. Iris Santowski, Fachärztin für Anästhesiologie und Dr. Rainer Kram, Oberarzt der Anästhesiologie, Leiter der Operativen Intensivstation sowie Leiter der Stabsstelle Katastrophenschutz, berichten von ihrem Weg aus der Krise.

In der Intensivmedizin ist selten ein Tag wie der andere. Doch der 10. September 2020 wird uns und unseren Kollegen aus dem Universitätsklinikum Düsseldorf nachhaltig in Erinnerung bleiben. Als wir am Morgen nichtsahnend die Klinik erreichen, stellt sich schnell heraus: Die IT ist lahmgelegt und die vernetzten Computersysteme tun nicht mehr, was sie sollen. Innerhalb weniger Stunden findet unsere IT-Abteilung den Grund: Cyberkriminelle haben sich in das System der Klinik gehackt. Sofort wird die digitale Verbindung zur Außenwelt unterbrochen. Mit Unterstützung vom Landeskriminalamt, dem Bundesamt für Sicherheit in der Informationstechnologie und Spezialunternehmen starten aufwendige Ermittlungen. Die Unterbrechung der IT von

der Außenwelt betrifft in der Folge auch die interne und externe Kommunikation: Wir können keine E-Mails mehr versenden oder abrufen und über das Netz keine Befunde austauschen.

Kreative Lösungsfindung: Not macht erfinderisch

Die Stabsstelle Katastrophenschutz ist einige Stunden lang damit beschäftigt, eine Lösung für das Kommunikationsproblem zu finden. Um überhaupt alle Beschäftigten des Klinikums über den Vorfall zu informieren, greifen wir zunächst auch zu analogen Methoden und setzen neben dem guten alten Faxgerät einen Botendienst ein, der schriftliche Informationen an Wände der verschiedenen Stationen pinnt sowie auf Tischen auslegt.

Zeitgleich arbeiteten wir neben der Informationsverbreitung über Flugblätter in der Krankenhauseinsatzleitung an der Entwicklung weiterer Kommunikationsformen. So wird auch eine Internetseite als Informationszentrale innerhalb weniger Stunden aufgebaut. Glück im Unglück haben unsere Stationen dadurch, dass bei einem Großteil noch keine computerbasierte Patienten- und Befundenmanagementsysteme vorhanden sind oder sie schnell auf analoge Systeme (schriftliche Medikamenten Anordnun-

gen und Befunde etc.) umstellen können, sodass der Betrieb aufrechterhalten werden kann. Darüber hinaus sind die medizinischen Geräte, wie Beatmungsgeräte, Perfusoren und Monitore, auch unabhängig vom IT-Netz funktionstüchtig, sodass das Wohl der Patienten zu keiner Zeit gefährdet ist.



Dr. Iris Santowski

Dennoch verhängen wir einen temporären Aufnahmestopp und verschieben alle nicht lebenswichtigen Operationen. Da auch der Rettungsdienst unsere Klinik nicht mehr anfährt, reduziert sich die Patientenzahl nach und nach. Glück haben wir auch beim Labor-System, das auf einem anderen Betriebssystem läuft. Es funktioniert problemlos weiter. Ein entscheidender Faktor für uns: Wäre das Labor ausgefallen, hätten wir unsere Dienste gänzlich einstellen müssen.

Ein zentrales Problem stellt jedoch die Übermittlung von Befunden und Informationen zu Organisation, Dienstplanung und Dienstweisungen dar. Hier müssen wir schnell eine Lösung finden, um effektiv weiterarbeiten zu können. Zunächst bauen wir einen Verteiler aus externen E-Mail-Adressen auf. Nach und nach stellen wir auf die E-Mail-Adressen der Universität um, da der Server der Universität von dem Angriff nicht betroffen ist. Doch auch dies kann sich nicht als Standardweg in der Kommunikation durchsetzen, da immer wieder vereinzelte Mitarbeiterinnen und Mitarbeiter keinen Zugriff auf jene E-Mails haben. Mit verschiedenen Parallelsystemen sowie dem Einsatz von Faxgeräten versuchen wir zu gewährleisten, alle Beschäftigten bestmöglich zu erreichen.

Ein sicherer Messenger für die Ad-Hoc-Kommunikation

Die Kommunikation per E-Mail-Adressen der Universität funktioniert nur eingeschränkt und sie kostet Zeit – Zeit, die in einer Krise niemand hat. Faxe zu versenden, dauert ebenfalls und sie müssen an Ort und Stelle abgerufen werden. Auf der Suche nach einer effektiven Ad-Hoc-Kommunikationslösung, die auch den Austausch größerer Dateien wie zum Beispiel Röntgenbilder ermöglicht, stoßen wir schließlich auf den Messenger Siilo. Die App aus den Niederlanden wurde speziell für das Gesundheitswesen entwickelt und bietet eine DSGVO-konforme Alternative zu Messengerdiensten,

wie z.B. WhatsApp, die im klinischen Bereich aus Datenschutzgründen nicht gestattet sind. Innerhalb von nur wenigen Tagen nach dem Hackerangriff installieren sich über 500 Ärzte des Universitätsklinikums die Siilo-App auf die Smartphones. Der Messenger bietet uns in der Krisenzeit vor allem eins: eine schnelle und sichere, digitale Kommunikation und Vernetzung, die von unseren anderen Systemen völlig unabhängig funktioniert.

Auch nach der Krise bewährt sich die App Siilo

Nachdem der Server der Universitätsklinik wieder funktionstüchtig ist, bleibt Siilo bei uns weiterhin im Einsatz. Obwohl wir seit der Wiederherstellung aller IT-Funktionen wieder vorrangig E-Mails und die Patienteninformationssysteme nutzen, fungiert der Messenger nun als zusätzliches Tool und Parallellösung der Kommunikation. In einigen Fällen hat die Anwendung sich inzwischen sogar zur bevorzugten Kommunikationsform entwickelt. Insbesondere wenn es um kurzfristige Absprachen geht, hat sich gezeigt: Die Beschäftigten antworten über den Messenger deutlich schneller. So sind inzwischen auch unsere Dienstpläne in der App einsehbar und ein spontaner Austausch, etwa bezüglich eines Schichtwechsels, ist problemlos möglich.

Ein weiterer Vorteil der Anwendung, von der wir erst seit wenigen Wochen profitieren: Es besteht die Möglichkeit, die Beschäftigten des Klinikums in institutioneller Form zentral und zeitgleich über den Messenger anzuschreiben, ohne ihre privaten Kontaktdaten kennen zu müssen. Dies ist besonders aus Krisensicht eine entscheidende Funktion, die wir gerne schon zu Zeiten des Hackerangriffs genutzt hätten. Daher wünschen wir uns eine Ausweitung der Siilo-Nutzung auf möglichst viele Mitarbeiterinnen und Mitarbeiter.

Eine der wichtigsten Lehren, die wir aus dem Hackerangriff des vergangenen



Dr. Rainer Kram

Jahres gezogen haben, ist jedoch: Selbst wenn im Ernstfall eine Lösung ausfällt, müssen wir handlungsfähig bleiben. Daher können wir nur dazu raten, sich nicht nur auf eine IT-Infrastruktur zu verlassen, sondern auch Kommunikationsformen zu etablieren, die gänzlich unabhängig von der Krankenhaus-eigenen Infrastruktur sind.

Die Corona Pandemie hat uns allen noch einmal verdeutlicht: Es geht nicht nur um die Anzahl an Intensivbetten, sondern vorwiegend um das Personal. Die Digitalisierung kann hier einen wichtigen Beitrag leisten, um die Medizin in Zukunft effizienter zu gestalten. Wir betrachten sie als eine notwendige Entwicklung, die stattfinden muss. Alle Anwendungen, die dazu beitragen, Prozesse besser zu gestalten, Kommunikation zu erleichtern oder abzukürzen sowie redundante Prozesse zu vermeiden, sollten wir nach und nach in unseren klinischen Alltag integrieren. Nur so kann die Versorgung auch insgesamt besser werden.



Menschliche Firewall durch simulierte Phishing-Tests stärken

Die Cyber Samurai GmbH bietet IT-Security Dienstleistungen zum Schutz vor drohenden Gefahren durch Cyberattacken an. Die Berater für IT-Sicherheit zeigen, wie das Sicherheits-Risiko in der jeweiligen Organisation reduziert werden kann und unterstützen bei der konkreten Umsetzung

Gerade der Mensch dient als Angriffsfläche, so dass die menschliche Firewall eine immer größere Bedeutung bekommt. Durch interaktive Security Awareness Trainingseinheiten, gepaart mit simulierten Phishing-Tests, werden die Mitarbeiter für Cyber-Risiken sensibilisiert.

Eine erfolgreiche Security Awareness Kampagne entwickelt die Mitarbeiter zum aktiven Mitglied der Verteidigung. Relevante Trainingsinhalte sind der Schlüssel zum Lernerfolg und der Trainingsakzeptanz. Das Ziel ist eine nachhaltige Verhaltensänderung, die nur durch die Kombination von IT-Security Trainings und simulierten "Real Life Phishing-Tests" samt inhaltsbezogenen Lernvideos bewirkt wird.

Umfassender IT-Security Service

Die Cyber Samurai GmbH bietet einen umfassenden Service, wie Beratung zur Standortbestimmung der IT-Security, Security Awareness Kampagnen und Phishing Tests, Einführung von Information Security Management Systemen, IT-Security Checks, Livehacking, Cyber Security Vorträge und Webinare sowie Vulnerability Scans und Pentesting.

Erfahrungsgemäß ist die Personaldecke in vielen Organisationen dünn, wobei die Kosten über das Krankenhauszukunftsgesetz übernommen werden. Ideale Voraussetzungen für den Security Awareness Service von Cyber Samurai. Das Krankenhaus muss lediglich einen Projektleiter bestimmen sowie ein paar Servereinstellungen vornehmen. Anschließend wird von Cyber Samurai ein bedarfsgerechtes Phishing und E-Learning ausgerollt und die Ergebnisse sowohl kommuniziert als auch im ISMS dokumentiert. Bereits nach kurzer Zeit kann eine Phishing Anfälligkeit der Mitarbeiter um 50% gesenkt und ein aktiver Beitrag zur Sicherheitskultur geleistet werden.

Security Awareness Kampagne

Die Cyber Samurai GmbH steht für eine produktunabhängige Full-Service Dienstleistung, um die jeweilige Organisation, insbesondere beim Faktor Mensch, so sicher wie möglich zu machen. So werden die eigenen Ressourcen geschont. Die Beratung erfolgt durch zertifizierte IT-Sicherheitsexperten, die je nach Kundenanforderung eine individuelle Lösung erarbeiten.

Fundierte Experten Know-How hinsichtlich der Security Awareness Tools und Trainingsinhalte erlaubt ein zielgerichtetes Ausrollen der Trainingsinhalte je nach Kenntnisstand der Mitarbeiter.

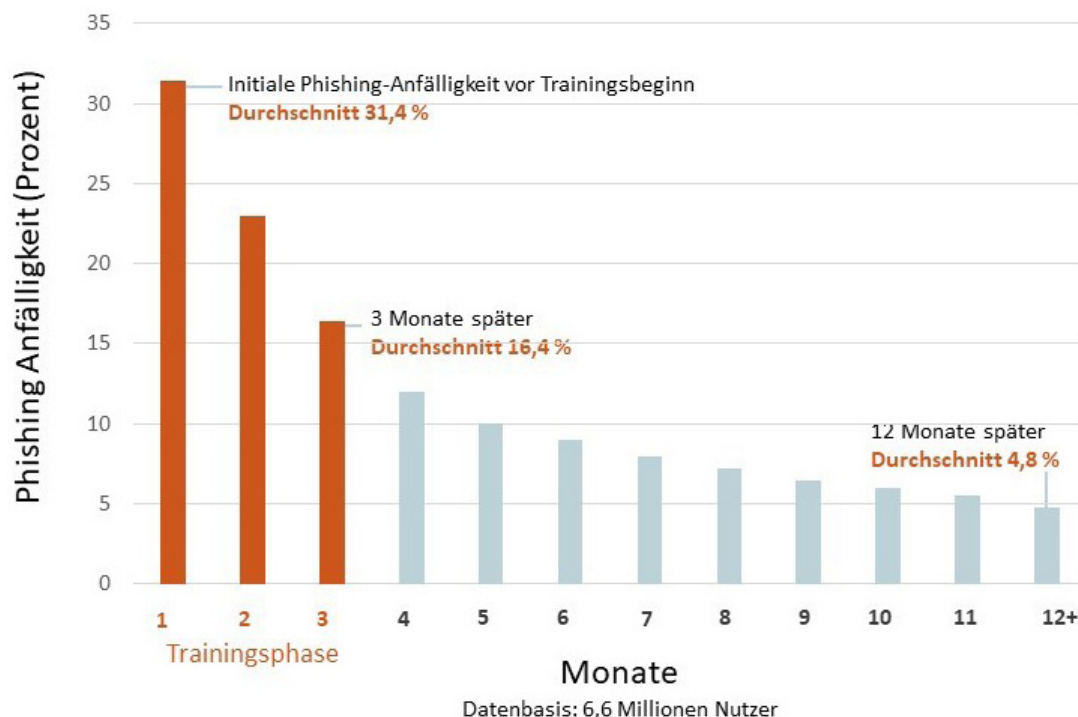
Durch professionelle Planung und Durchführung samt transparentem Reporting sowie einer effizienten Umsetzung werden Zeit- und Kostenersparnis im Kampagnenverlauf erreicht.

Zielgruppen und Einsatzgebiete

Die Dienstleistungen sind branchenübergreifend in mittelständischen und großen Organisationsformen im Einsatz. Zielgruppen sind Chief Information Security Officer, Chief Information Officer, Informationsbeauftragte, IT-Leiter und die Geschäftsführer.

Die Trainings wurden bedarfsgerecht ausgerollt, sodass jeder Beschäftigte, das für ihn relevante Trainingsangebot erhält.

Den Kunden wird höchste Vertraulichkeit garantiert.



Im Schnitt fallen 31,4% der ungeschulten Nutzer auf einen simulierten Phishing-Versuch rein. Bereits nach einem Jahr fortlaufendem Security Awareness Training und regelmäßigen simulierten Phishing-Tests hat sich die Anfälligkeit der Mitarbeiter signifikant reduziert. Die durchschnittliche Verbesserung liegt dabei im Durchschnitt bei 84%.

Proof of Concept

Im Rahmen eines Proof of Concept erhalten interessierte Organisationen einen ersten Eindruck zu den Dienstleistungen im Rahmen einer Security Awareness Kampagne. Schulungsinhalte werden zielgruppengerecht ausgewählt, beispielhaft ausgerollt, dokumentiert und reportet, damit der Kampagnenerfolg entsprechend analysiert werden kann.

Phishing Test

Ein kostenloser Phishing-Test ermöglicht es herauszufinden, wie anfällig Mitarbeiter für Phishing-Mails sind.

Die Basis des Phishing-Tests sind ungefährliche Phishing-Simulationen. Diese unschädlichen Phishing-Mails werden an die zuvor definierten Empfänger verschickt. Diese überprüfen, ob im Arbeitsalltag solche Angriffe erkannt werden können – ganz ohne echtes Risiko.

So kann die Gefährdung des Unternehmens anhand fundierter Kennzahlen richtig eingeschätzt werden. Eine Beratung erfolgt basierend auf den Ergebnissen. Bei weiterem Handlungsbedarf können die Mitarbeiter durch gezielte Schulung unterstützt werden, damit sie nicht zum Einfallstor für Hacker werden.

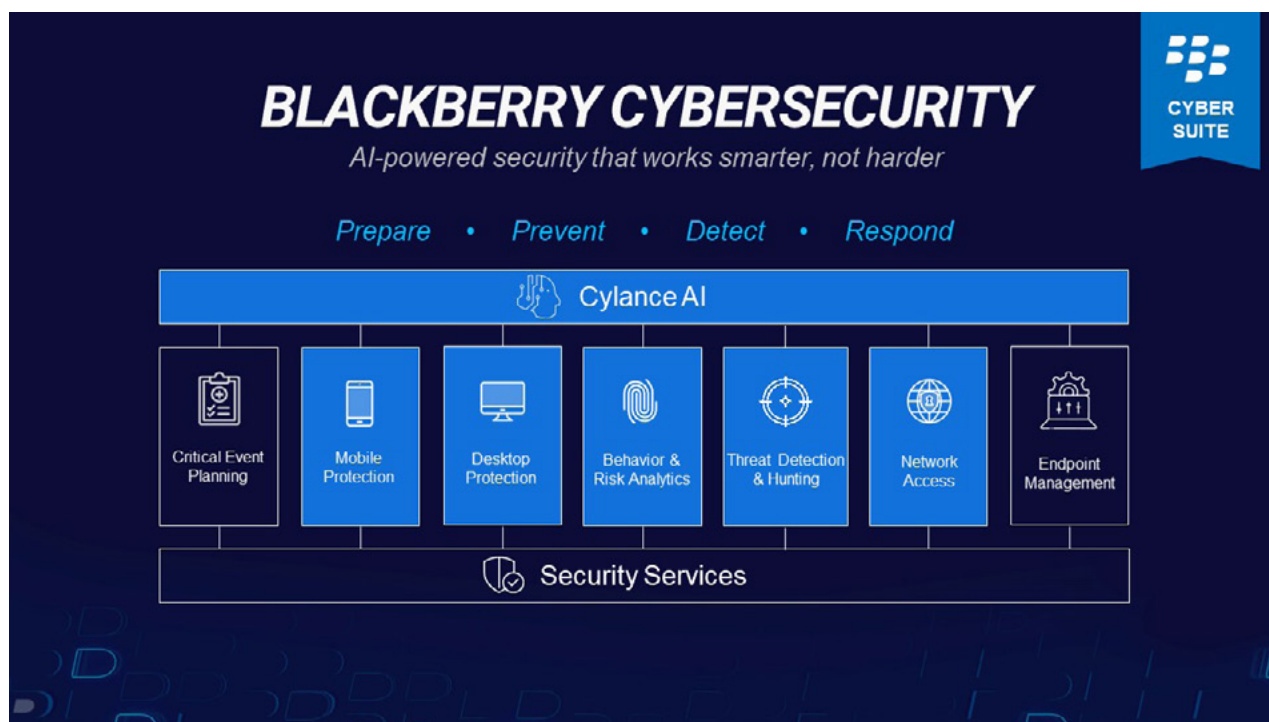


Cyber Samurai GmbH

Brahmsstrasse 9
85591 Vaterstetten
<https://cyber-samurai.net>

Nicolas Leiser, Geschäftsführung
nicolas.leiser@cyber-samurai.net
Telefon: 01 73 / 70 37 33 6

Elke Dieckröger-March, Vertrieb
elke.dieckroeger-march@cyber-samurai.net
Telefon: 08 10 6 / 39 80 05 2



Portfolio-Bundle unterstützt bei der sicheren Digitalisierung der Healthcare-Branche

Die jahrelange, erfolgreiche Partnerschaft von BlackBerry und der ISEC7 Group bietet Organisationen und Unternehmen innovative Lösungen und Dienstleistungen für eine sichere, digitale Kommunikations-Infrastruktur. Im Rahmen des Krankenhauszukunftsfonds (KHZG) bieten BlackBerry und die ISEC7 Group fundierte Unterstützung rund um digitale Arbeitsplätze, Kommunikation, Monitoring & erhöhte Verfügbarkeit, Cybersecurity, Alarmierung und digitale SAP-Prozesse.

ISEC7

Die ISEC7 Group ist ein global agierender Anbieter von Dienstleistungen und Software-Lösungen mit Sitz in Hamburg. Das Unternehmen unterstützt Sie mit tief spezialisiertem Wissen rund um sichere Digitale Arbeitsplätze, Kommunikation, Monitoring & erhöhter Verfügbarkeit, Cybersecurity, Alarmierung und digitale SAP-Prozesse.

Als **zertifizierter Partner für den Krankenhauszukunftsfonds** liefert Ihnen ISEC7 ein Konzept und die Profilskizze für die (optimierte) Digitalisierung Ihrer Einheit – direkt in einer einreichbaren Form.

BlackBerry

BlackBerry, vielen noch als Markenname für Smartphones bekannt, hat sich in den letzten Jahren zu einem der weltweit führenden Softwareanbieter im Bereich der Verwaltung und Absicherung von Endgeräten, IoT und über die QNX-Plattform Anwendungen für autonom fahrende Autos entwickelt. Insbesondere im Bereich der Cybersecurity-Lösungen kann der kanadische Hersteller zahlreiche Auszeichnungen vorweisen und gehört auch hier zu den weltweit führenden Anbietern.

Künstliche Intelligenz und Machine Learning

Die BlackBerry Unified Endpoint Security (UES) Lösung ist mit einem Ende-zu-Ende-Ansatz für Cybersicherheit tief in künstlicher Intelligenz (KI) und maschinellem Lernen (ML) verwurzelt. Durch diesen gesamtheitlichen Ansatz können alle Endpunkte gegen Cyberangriffe geschützt werden. BlackBerry Protect ist die einzige Lösung am Markt, welche auch unter anderem alte Windows Betriebssysteme (XP, Windows 7), Windows Embedded und Server mit KI schützen kann. Durch den „Vorhersage-Vorteil“ können aktuelle Bedrohungen ohne Signaturen, täglichem Updates und sogar im Offline-Modus erkannt und geblockt werden. Dabei wird auch keine On-Premise Infrastruktur benötigt.

Das Lösungs-Portfolio von BlackBerry umfasst mehrere Bausteine, um auf Cyberangriffe besser vorbereitet zu sein, d.h. Angriffe frühzeitig zu identifizieren und präventiv zu agieren und um anschließend optimal reagieren zu können.

So bieten die Lösungen verbesserte Transparenz und optimalen Schutz vor aktuellen und künftigen Cyberbedrohungen.

Neben der Plattform zur Absicherung der Endgeräte, bietet BlackBerry auch Professional Services und Managed Services an. Das weltweit agierende 24x7x365 SOC Team hat hier bereits mehrere Auszeichnungen erhalten, unter anderem auch den Weltmeister-Titel.

Breites Lösungs-Portfolio

Einsatzgebiete der Lösungen sind Desktop PCs und Server (Windows, MAC OS, Linux), sowie mobile Endgeräte mit den Betriebssystemen iOS, Android oder Chrome. Das Portfolio umfasst:

- **BlackBerry Protect:** Alle Arten von Cyberangriffen voraussagen und somit verhindern. Menschliches Eingreifen ist nicht erforderlich.
- **BlackBerry Optics:** Der umfassende Schutz besteht auch im Offline-Modus.
- **BlackBerry Persona:** Dynamische Anpassung an die Cybersicherheitsrichtlinien geschieht mittels prädiktiver KI – in Echtzeit und auf Basis von Benutzerstandort, Gerät und anderen Faktoren.

- **BlackBerry Gateway:** Bietet mehr Sicherheitskontrollen und gleichzeitig hohe Benutzerfreundlichkeit, verbessert den Fernzugriff für Mitarbeiter.

- **BlackBerry Guard:** Cybersecurity Service, nutzt sowohl KI, als auch den 24-Stunden Support durch das BlackBerry Incident Response (IR) Team.

Softwarelizenzen und Services

Bestehende devicebasierte Subscription CALs mit einer Mindestlaufzeit 12 Monate sind: BlackBerry Protect Desktop, BlackBerry Protect Mobile, BlackBerry Optics, BlackBerry Persona, BlackBerry Gateway, BlackBerry Guard. Als weitere Services stehen zur Verfügung: Professional Service für Consulting, Professional Service für Incident Response, Professional Service für Compromise Assessment, Professional Service für Red Team Services und Managed Services für Detection and Response.

Zielgruppen und Kundenreferenzen

Die Zielgruppen des Portfolio-Bundles sind Unternehmen und Organisationen im privaten und öffentlichen Bereich, welche eine moderne KI-basierte Absicherung aller Endgeräte möchten. Kunden sind Krankenkassen, Krankenhäuser auf der ganzen Welt, Unternehmen in der Healthcare-Branche sowie Verbände und Stiftungen.



Weitere Informationen und Kontakt:

<https://bit.ly/KH-IT>

Ein Gastbeitrag von Tim Berghoff, Security Evangelist bei G DATA CyberDefense

Krankenhäuser schneiden bei der IT-Sicherheit im KRITIS-Branchenvergleich schlecht ab

Niemand wird bestreiten wollen, dass Krankenhäuser mit Recht zu den zentralen Betrieben der KRITIS zählen. In keinem anderen Bereich unserer Gesellschaft besteht ein so unmittelbarer Zusammenhang zwischen reibungslosem Betrieb und dem Wohlergehen der Bevölkerung. Daher ist es nur richtig, dass Krankenhäuser zur Einhaltung der strengen KRITIS-Anforderungen des BSI verpflichtet sind. Demnach sind die Verantwortlichen dazu verpflichtet „geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.“

Die Planung eines wasserdichten IT-Sicherheitskonzepts ist heute jedoch komplexer denn je. Sicherheitsbeauftragte befinden sich in einem stetigen Katz-und-Maus-Spiel mit Cyberkriminellen und finden sich nicht selten in einer passiven Position des Reagierens wieder. Sie müssen Schwachstellen in der Krankenhaus-IT identifizieren und Sicherheitslücken schließen, bevor potenzielle Angreifer sich diese zunutze machen können. Doch die IT-Sicherheitsbeauftragten kämpfen hier einen ungleichen Kampf: Auf der einen Seite bedienen sich Cyberkriminelle neuester Tools aus dem Darknet und nutzen die florierende Malware as a Service – Branche. Gut gepflegte Datenbanken mit den aktuellen Schwachstellen runden das Paket ab. Auf der anderen Seite kämpfen IT-Sicherheitsbeauftragte von Krankenhäusern mit Legacy-Software auf vielen ihrer medizinischen Geräte und müssen eine unübersichtliche Schatten-IT in ihrem Netzwerk überwachen. So nutzen viele Kliniken beispielsweise noch immer MRTs mit veralteten Betriebssystemen, die seit Jahren keine Sicherheitsupdates mehr erhalten. Ebenso problematisch sind private Endgeräte wie Smartphones, Tablets oder mitgebrachte Laptops von Mitarbeitern, die mit dem WLAN des Krankenhauses verbunden sind – ganz abgesehen davon, dass teilweise Patienteninformationen über Messenger-Plattformen wie WhatsApp kommuniziert werden. All diese Endpunkte stellen ein

schwer kontrollierbares Risiko für die IT-Infrastruktur dar: Entweder weil sie über keine aktuellen Updates verfügen oder bereits mit Malware infiziert sind. Das Problem ist um so problematischer, wenn ein Netzwerk ohne eine langfristige Strategie und über einen langen Zeitraum gewachsen ist.

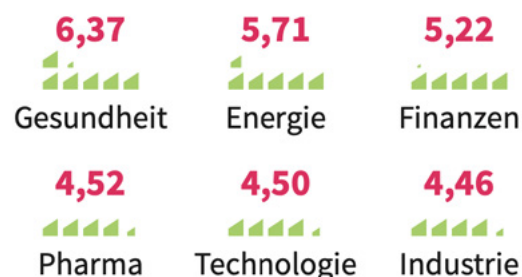
Der Gesundheitssektor erleidet die größten finanziellen Schäden durch Datenpannen

Die Vergangenheit hat uns eindrücklich bewiesen, wie schnell ein Krankenhaus von einer Cyberattacke getroffen werden und wie schwer sich ein solcher Vorfall auf den Betrieb auswirken kann. Ein Ransomware-Angriff auf die Uniklinik Düsseldorf im September 2020 führte dazu, dass Tagelang keine OPs stattfinden konnten und Notfälle auf andere Krankenhäuser in der Umgebung ausgelagert werden mussten. Vier Jahre zuvor quittierten im Lukaskrankenhaus Neuss rund 500 Rechner und 150 Server ihren Dienst, weil ein unvorsichtiger Mitarbeiter einen Mailanhang geöffnet hatte und damit einen Trojaner ins Netzwerk gelangen ließ. Im Lichte dieser Vorfälle sollte man meinen, dass die Verantwortlichen unseres Gesundheitssystems gewarnt sind und die notwendigen Gegenmaßnahmen gegen Cyberangriffe umgesetzt haben. Doch die Realität sieht anders aus. In einer großangelegten Studie „Cybersicherheit in Zahlen“ betrachtete G DATA die Cybersicherheit in

Deutschland, sowie im internationalen Vergleich und über alle Branchen hinweg. Eine der Erkenntnisse der Studie ist, dass der Gesundheitssektor weltweit den größten monetären Schaden durch Datenpannen erleidet. Im Durchschnitt betragen die Kosten eines Vorfalls 6,37 Millionen Euro. Doch die gesundheitlichen Schäden, die entweder mittelbar oder unmittelbar durch die empfindliche Störung des Regelbetriebs verursacht werden, kann kein Geld der Welt rückgängig machen. Daher muss eine gewissenhafte IT-Abwehrstrategie eine viel höhere Priorität erhalten, als dies bisher der Fall ist. Denn eine funktionierende IT ist für die moderne Medizin ebenso wichtig, wie gut geschultes Personal.

Addiert

Durchschnittliche Gesamtkosten von Datenpannen in ausgewählten Branchen; weltweit; 2019 / 2020; in Millionen Euro



Gesundheitssektor vermeldet innerhalb der KRITIS die meisten Vorfälle

Zahl der Meldungen von KRITIS-Unternehmen nach Sektoren; Deutschland; 2020

Gesundheit	134
Information & Kommunikationstechnik	75
Energie	73
Finanzen und Versicherungen	65
Transport & Verkehr	56
Ernährung	9
Wasser	7
kerntechnische Anlagen	0

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Das Gesundheitssystem ist innerhalb der KRITIS mit Abstand am häufigsten von Cyberangriffen betroffen. Alleine 2020 gingen 134 Meldungen beim BSI ein; mit 75 Meldungen und großem Abstand auf Platz zwei folgt die Branche der Information & Kommunikationstechnik. Die Gründe dafür sind mannigfaltig. Zum einen sind Unterbrechungen im Gesundheitsbetrieb mit großer Dringlichkeit und im wahrsten Sinne des Wortes mit großen Leidensdruck verbunden. Daher bleibt keine Zeit zu zögern, bevor man sich Hilfe von den Experten des BSI anfordert. Ein weiterer, wichtiger Punkt ist jedoch die Konkurrenz um die knappen finanziellen Mittel. Damit die IT-Sicherheit nicht zur Verhandlungsmasse in der Finanzplanung von Krankenhäusern wird, werden seit 1. Januar 2021 drei Milliarden Euro vom Bund bereitgestellt, die Krankenhäusern eine Modernisierung und Absicherung ihrer IT ermöglichen sollen. Das „Krankenhauszukunftsgesetz“ eröffnet nun also Krankenhäusern die Möglichkeit, sich Bundesmittel zur Modernisierung der IT zu sichern, ohne Abstriche beim Personal oder der medizinischen Versorgung machen zu müssen. Diese Mittel sollten daher auch dazu genutzt werden, die bestehenden IT-Sicherheitslücken zu stopfen. Um sicherzustellen, dass die Bundeshilfen auch zielführend und effizient zum Ausbau der IT-Sicherheit genutzt werden, empfiehlt es sich, die drei Säulen der IT-Sicherheit im eigenen Krankenhaus auf Investitionslücken abzuklopfen.

Die 3 Säulen der IT-Sicherheit

An welchen Stellen es fehlt, ist eine Einzelbetrachtung, die jedes Krankenhaus in einer individuellen Bestandsaufnahme selbst klären muss. Krankenhäuser, die unter die KRITIS-Verordnung fallen, müssen laut §8a des BSI-Gesetzes alle zwei Jahre nachweisen, dass ihre Maßnahmen dem Stand der Technik entsprechen. Richtlinie für diese Maßnahmen sind die „B3S“ (Branchenspezifische Sicherheitsstandards). Als generelle Orientierungshilfe ist es sinnvoll, die IT-Sicherheitsstrategie grob in drei Bereiche aufzuteilen: Sicherheits-Software, Mitarbeiter-Sensibilisierung und Vorsorge.

1. Technische Maßnahmen: Firewall, Antivirus und starke Authentifizierungs-Maßnahmen sind das A und O und sollten als Mindestanforderung betrachtet werden. Ohne sie stehen Angreifern Tür und Tor offen.

2. Sensibilisierung aller Mitarbeiter: Selbst mit besten Schutzmaßnahmen ist man noch nicht vollumfänglich gegen raffinierte Phishing-Attacken oder Social Engineering gewappnet. Mit 24,3 Prozent der Mitarbeitenden, die sich „große bis sehr große Kompetenz bei der IT-Sicherheit“ zuschreiben sind Beschäftigte im Gesundheitssektor auf dem drittletzten Rang aller Branchen in Deutschland. Bedenkt man, dass die meisten IT-Vorfälle durch ungeschulte Mitarbeiter begünstigt oder verursacht werden, sind Mitarbeitertrainings eine der wirksamsten Maßnahmen für eine Verbesserung der IT-Sicherheit.

3. Vorsorge: Datenbackups, Incident Readiness & Response helfen, den Betrieb nach einem Angriff schnell wieder in geregelte Bahnen zu führen. Datenbackups schützen gegen Ransomware-Angriffe, damit die verschlüsselten Daten schnell wiederhergestellt werden können. Incident Readiness bedeutet, gut auf Notfälle vorbereitet zu sein und schnell reagieren zu können. Notfallpläne sind dabei genauso wichtig, wie die Einbeziehung und Schulung der Mitarbeitenden. Auch (übersichtliche & verständliche) Checklisten helfen Angestellten dabei, Schäden abzuwenden.

Weiterhin sollte man die Netzwerksegmentierung im Auge behalten. Unzählige Logins von teilweise unregistrierten Endgeräten führen schnell zum Kontrollverlust über die Integrität der IT-Infrastruktur.

Wenn alle Dämme brechen, hilft als letztes Bollwerk nur noch die Incident Response. Am besten man schließt im Vorfeld einen Vertrag mit Sicherheitsexperten ab. Daraufhin nehmen diese die gesamte IT-Infrastruktur des Krankenhauses unter die Lupe und können im Notfall schnell eingreifen.

Fazit: Das Gesundheitssystem und dessen Rückgrat – die Krankenhäuser – reagieren so sensibel wie kaum eine andere KRITIS-Branche auf Betriebsstörungen. Denn Notfälle bieten keinen Spielraum für zögerliches Handeln oder schlechte Vorbereitung. Umso wichtiger ist es, keine Kompromisse bei der IT-Sicherheit einzugehen, da ein Cyberangriff die fachgerechte Behandlung von Patienten empfindlich stören oder im schlimmsten Fall über Wochen unmöglich machen kann.



Tim Berghoff, Security Evangelist bei G DATA CyberDefense

Praxistaugliche Einführung des B3S Krankenhaus (ISMS)

In wenigen Monaten tritt das Patientendaten-Schutz-Gesetz (PDSG) in Kraft. Um die Anforderungen des PDSG zu erfüllen, wurde der branchenspezifische Sicherheitsstandard B3S als geeignetes Rahmenwerk bestätigt. Was in der Theorie vielleicht einfach klingt, ist in der Praxis im Healthcare Bereich eine Herausforderung.

Praxistaugliche Einführung des B3S Krankenhaus (ISMS)

In wenigen Monaten tritt das Patientendaten-Schutz-Gesetz (PDSG) in Kraft. Um die Anforderungen des PDSG zu erfüllen, wurde der branchenspezifische Sicherheitsstandard B3S als geeignetes Rahmenwerk bestätigt. Was in der Theorie vielleicht einfach klingt, ist in der Praxis im Healthcare Bereich eine Herausforderung.

Passende Lösungen für Informationssicherheit

Die Softwarelösungen von CONTECHNET verfolgen hier eine strukturierte und vor allem praxistaugliche Vorgehensweise. Diese Transparenz im Projektverlauf ermöglicht realistische Planungen hinsichtlich Softwarekosten, der Einführungsdauer und Nutzung als auch der Überführung in den täglichen Betrieb.

Eine gemeinsame Datenbasis für Informationssicherheit, Notfallplanung und Datenschutz minimiert die Datenpflege innerhalb Ihrer Organisation: Personal, Infrastruktur und Prozesse.

Folgende Lösungen stehen zur Verfügung:

- **INDITOR® BSI / ISO:** Softwarelösung zum Aufbau und Betrieb eines ISMS nach der IT-Grundschutz-Methode oder der Methode des ISO/IEC 27001, B3S Krankenhaus, sowie weiterer Standards
- **INDART® Professional:** Softwarelösung zum Aufbau und zur Pflege einer prozessorientierten Notfallplanung (erforderlicher Teilbereich der Informationssicherheit – Kontinuitätsmanagement)
- **INPRIVE®:** Softwarelösung zur Dokumentation des Datenschutzes gemäß EU-DSGVO

Zielgruppen und Referenzen

Zielgruppen der CONTECHNET-Lösungen sind insbesondere Krankenhäuser und Kliniken. Beispielhafte Ansprechpartner innerhalb dieser Organisationen sind: IT-Leiter, Informationssicherheitsbeauftragte, Risiko-Manager, Geschäftsführer, Qualitätsmanager und Datenschutzbeauftragte.

Mit mehr als 450 umgesetzten Projekten und über 100 Fachspezialisten aus unserem Partnernetzwerk sind die Lösungen der CONTECHNET im Bereich Krankenhaus der Marktführer.

Wie also vorgehen?

Bevor Sie unnötig Zeit und Geld in Beraterstunden investieren oder unzählige Listen in Word und Excel erstellen: Nehmen Sie sich die Zeit, Ihre Optionen zu prüfen, um das Projekt schneller, einfacher und sicherer durchzuführen.

Mithilfe der Lösung INDITOR® B3S können die Anforderungen des Standards B3S Krankenhaus schnell und nachhaltig umgesetzt werden. Dabei bietet die Lösung eine Umsetzungshilfe mit vorgegebener Struktur. Auf diese Weise lassen sich die geforderten Maßnahmen dokumentieren und bestehende Dokumente beispielsweise aus der ISO 9001 oder den KTQ-Katalogen einbinden. Über Importer und Schnittstellen können zudem bereits vorhandene Daten problemlos in die Lösungen von CONTECHNET importiert und dort automatisiert und zentral gepflegt werden.

Denn B3S und die geforderten Maßnahmen – wie ein Informationssicherheitsmanagementsystem (ISMS) – sind keine einmaligen Prozesse. Es gilt, sie langfristig zu integrieren und für sich selbst die Vorteile und Chancen daraus zu nutzen.

Als bisher einziger Softwarehersteller gibt CONTECHNET Anwendern eine Lösung an die Hand, mit der sie den Sicherheitsstandard B3S Krankenhaus selbstständig und in kurzer Zeit umsetzen können.

Technische Anforderungen und voller Leistungsumfang

Systemvoraussetzungen sind MS Windows Betriebssystem & MS SQL-Server / MS SQL Express.

Zur Verfügung stehen eine Vielzahl an Import- & Schnittstellenanbindungen – beispielhaft: Docusnap/Matrix42/i-doit/Excel...)

Zugriff auf das Partnernetzwerk der CONTECHNET mit mehr als 45 Partnerunternehmen und über 100 Fachspezialisten für die Themen Notfallplanung / Informationssicherheit / Datenschutz.

Speziell für die Leser:innen des Krankenhaus IT-Journals bietet die CONTECHNET einen Webcast-Workshop zur praktikablen Umsetzung des B3S an. In diesem Workshop gehen wir auf die empfohlene Methode ein und geben einen direkten Einblick in die Vorgehensweise innerhalb und außerhalb unserer Lösungen. Sie erfahren unter anderem, worauf es beim Projektstart, bei der Projektdurchführung und bei internen oder externen Audits ankommt.

Anmeldung einfach und unkompliziert über unsere Homepage: www.contechnet.de/de/b3s-veranstaltungen
Seien Sie dabei!

Das MEDIX-CARE Patientenportal

Beliebt und überraschend intelligent



MEDIX-CARE[®]
Intelligent Patient Engagement

Das MEDIX-CARE Patientenportal basiert auf den Erfahrungen von tausenden Patienten im In- und Ausland und kombiniert digitale Best-Practice mit intelligenter Prozessautomatisierung, damit Kliniken einfacher ihre Ziele erreichen: Optimale Behandlungsergebnisse und zufriedene Patienten.



Netzwerkzugriffskontrolle für Gesundheitseinrichtungen

Der ClearPass Policy Manager von Aruba

Der ClearPass Policy Manager von Aruba bietet eine sichere rollen- sowie gerätebasierte Netzwerkzugriffskontrolle für IoT-, BYOD- und Unternehmensendgeräte. Somit stehen den Mitarbeitern in Gesundheitseinrichtungen und Kliniken sowie den Patienten und Gästen kabelgebundene, drahtlose und VPN-Infrastrukturen für einen sicheren Zugang mit ihren Geräten zur Verfügung.

Der ClearPass Policy Manager ist Teil der Aruba Edge Services-Plattform (ESP) und adressiert die Konnektivitätsanforderungen für das digitale Krankenhaus. Die ESP besteht aus drei Ebenen: Die Ebene „Unified Infrastructure“ bietet die Möglichkeit kabelgebundene und kabellose Endgeräte einheitlich und standortübergreifend zu vernetzen. Dieser Ansatz erleichtert den IT-Betrieb durch seine durchgängige einheitliche Infrastruktur über Klinikcampus, Außenstelle, Rechenzentrum und Heimarbeitsplätze hinweg. Die zweite Ebene „Zero-Trust-Security“ stellt sicher, dass alle Geräte im Netzwerk erkannt werden und kann jedem Benutzer, Gerät und medizinischem IoT-Device im Netzwerk eine bestimmte Rolle kontextbasiert zuweisen. Die dritte Ebene, die „AIOps“ Lösung, mit ihren Funktionalitäten ist exakt auf die Bedürfnisse von Kliniken zugeschnitten, da künstliche Intelligenz Fehler in Anwendungen frühzeitig sowie automatisiert erkennt, proaktiv informiert und konkrete Handlungsempfehlungen benennt. Zudem können Softwareaktualisierungen während des laufenden Betriebs vorgenommen werden – eine wichtige Voraussetzung für den Non-Stop IT-Betrieb im Gesundheitswesen.

Referenz: Universitätsklinikum Schleswig-Holstein,
<https://bit.ly/39sCPsb>

Mehrwerte der Lösung im Gesundheitswesen

- Rollenbasierte, einheitliche Durchsetzung des Netzwerkzugriffs in drahtlosen, kabelgebundenen und VPN-Netzwerken verschiedener Hersteller
- Intuitive Konfigurationsvorlagen für Richtlinien und Tools zur Fehlerbehebung
- Unterstützung verschiedener Authentifizierungs- und Autorisierungsquellen (AD, LDAP, SQL)
- Self-Service-Geräte-Onboarding mit integrierter Zertifizierungsstelle (CA) für BYOD
- Individualisierte Gastzugänge in punkto Personalisierung und Unternehmensbranding

- Integration mit zentralen UEM-Lösungen für detaillierte Geräteprüfungen
- Umfassende Integration mit dem Aruba 360 Security Exchange Programm
- Die Unterstützung von Single Sign-On (SSO) ist mit Ping, Okta und anderen Identitätsmanagementlösungen kompatibel, um die Benutzerfreundlichkeit von SAML 2.0-basierten Anwendungen zu optimieren

Lizenzmodelle:

- Unbefristete Volllizenzen oder subscriptionbasiert – es werden nur Endgeräte lizenziert, die mit dem Netzwerk verbunden sind

ClearPass ist als Hardware oder als virtuelle Appliance verfügbar - abhängig von der Anzahl der Endgeräte und den Kundenanforderungen.

Hardware Appliances:

- JZ508A Aruba ClearPass C1000 S-1200 R4 HW-Based Appliance
- R1V81A Aruba ClearPass C2010 DL20 Gen10 HW-Based Appliance
- R1V82A Aruba ClearPass C3010 DL360 Gen10 HW-Based Appliance

Virtuelle Appliance:

- Virtual Appliances JZ399AAE Aruba ClearPass Cx000V VM-Based Appliance E-LTU

Hewlett-Packard GmbH
 arubanetworks.com/de/
 digitales-krankenhaus@hpe.com
 Herrenberger Str. 140
 71034 Böblingen
 Deutschland

Medigate unterstützt Ihre KRITIS Strategie

Krankenhäuser, Labore und Arztpraxen sind systemrelevant – das haben wir alle in den zurückliegenden Monaten sehr deutlich erfahren. Digitalisierung ist das Rückgrat moderner Gesundheitseinrichtungen und damit grundsätzlich Angriffsobjekt für Viren und andere Cyber-Attacken. Um den Organismus Gesundheitswesen widerstandsfähig zu halten, bedarf es effizienter Verfahren zur Prävention, zur Früherkennung und zur Behandlung.

Wir verfügen über diese Mittel und Methoden, die notwendige Erfahrung und den Willen, die kritischen Infrastrukturen in unserem Gesundheitswesen zu schützen.

Wir, die globits GmbH in Berlin, die Netzwerk-Kommunikationssysteme GmbH in Barleben und die cano systems GmbH in Recklinghausen sind das Geschäftsfeld Digital Infrastructure Services (DIS) der Fernao Networks Holding und bieten neue Lösungen zum effizienten Schutz Ihrer vernetzten medizintechnischen Geräte (IoMT).

Verantwortliche in Kliniken für diese besondere Gruppe von IT-Geräten beklagen in Diskussionen mit unseren Consultants sehr deutlich die fehlende Transparenz bezüglich Patch- und Release-Status, Kommunikationsverfahren, Inventarisierung, Abstellort und Gesundheitszustand.

Gemeinsam mit unserem Partner Medigate verfügen wir über die Lösung für diese und weitere Ihrer Herausforderungen im Alltag digitaler Gesundheitseinrichtungen.

Medigate liefert ein komplettes Inventarverzeichnis aller vernetzter medizintechnischer Geräte, identifiziert anomale Kommunikationsvorgänge, hilft bei der Durchsetzung von Sicherheitsrichtlinien und liefert wertvolle Erkenntnisse für das Management Ihrer Medizintechnik - bis hin zur Nutzungsintensität Ihrer Geräte. Das liefert wertvolle Informationen zur Optimierung künftiger Beschaffungsentscheidungen und hilft Kosten zu senken.

Die Lösung von Medigate erzeugt zu jedem erkannten Device detaillierten Informationen zu Schwachstellen des Gerätes, dem genauen Gerätetyp, der installierten Software-Version, der Betriebsdauer, dem Standort, den Kommunikationsbeziehungen und der Auslastung des jeweiligen Gerätes.

Medigate informiert weiterhin nicht nur über die Herkunft des medizinischen Datenverkehrs, sondern auch über dessen Ziel und warnt bei Anomalien bzw. bei ungewünschten Zielen. Medigate bietet Schnittstellen zu unterschiedlichen Herstellern von NAC-Systemen, Firewalls, Asset Management, Vulnerability Management, SIEM, Monitoring, EMR, IPAM und lässt sich einfach in die IT-Systemlandschaft integrieren.

Medigate: Die Highlights

- Erstellt komplettes, exaktes Inventar aller vernetzten medizinischen Geräte
- Erkennt Anomalien in der Gerätenutzung und im Datenverkehr
- Unterstützt die Durchsetzung der Sicherheitsrichtlinien
- Verhindert zusammen mit Firewall-Lösungen illegitimen Datenabfluss
- Liefert direkt verwertbare Erkenntnisse über Auslastung der Geräte und weitere Management-Informationen
- Erhöht die Sicherheit für komplexe standortübergreifende Netzwerke von Krankenhäusern
- Liefert die Basis für zukünftige Digitalisierungsinitiativen

Mit der mehrfach ausgezeichneten Medigate-Plattform können Sie, als Verantwortlicher für die Sicherheit Ihrer IT und IoMT präventiver arbeiten, früher agieren und schneller reagieren.

Sie wünschen mehr Informationen oder eine Präsentation zu unserer Lösung mit Medigate und den Möglichkeiten zur Förderung durch das Krankenhauszukunftsgesetz?



Nehmen Sie mit uns Kontakt auf.
Herr Hendrik Ahlburg (h.ahlburg@globits.de)
ist Ihr kompetenter Ansprechpartner.

Wie sich das Gesundheitswesen gegen Cyberangriffe wappnen kann

Zwischen Januar und November 2020 gab es laut Bundesregierung 43 Cyberangriffe auf wichtige Einrichtungen des Gesundheitsbereichs. Das zeigt, wie groß die Gefahrenlage für Deutschland ist. Insbesondere Kliniken und deren Betreiber müssen sich vermehrt gegen Ransomware-Attacken wehren. Bei einem solchen Angriff werden Daten verschlüsselt und Lösegeld erpresst. Dies kann jedoch direkte Auswirkungen auf die Versorgung der Patienten haben, wie ein Fall im Dezember 2020 aus Nordrhein-Westfalen zeigt. Ein Rettungswagen musste abgewiesen und umgeleitet werden; die Patientin verstarb – möglicherweise auf Grund des durch den Cyberangriff notwendig gewordenen längeren Transports.

Ein Problem sind digitale Geräte und Anwendungen, die zum Teil erhebliche Schwachstellen aufweisen. Das haben Studien des BSI ergeben, bei denen verschiedene Medizinprodukte zur Behandlung und Pflege von Patienten auf ihre Sicherheit überprüft wurden – und rund 150 Schwachstellen gefunden wurden.

Wie kann sich das Gesundheitswesen schützen?

Gegen Cyberbedrohungen hilft der medizinische Leitsatz „Vorbeugen ist besser als Heilen“. Dabei sind es vornehmlich Präventivmaßnahmen, die für mehr Sicherheit sorgen:

Alle Geräte berücksichtigen

Jedes Gerät mit Zugang zum Unternehmensnetz und Internet muss geschützt werden. Neben Computern sind das auch Mobiltelefone, Tablets, Terminals und medizinische Geräte. Sicherheitsanbieter bieten dedizierte Lösungen zum Schutz dieser an.

Updates

Die Software aller Geräte muss stets auf dem neuesten Stand sein. Dies ist für medizinische Hardware gar nicht so leicht zu erfüllen, weswegen bereits bei der Anschaffung neuer Geräte berücksichtigt werden muss, ob und wie lange die Hersteller Updates garantieren.

Sicherheit für E-Mails

E-Mails sind im Gesundheitswesen eine tragende kommunikative Säule. Umso wichtiger ist es, Spam-Mails mit gefährlichen Anhängen und Links unschädlich zu machen. Ein effektiver E-Mail-Schutz ist ausschlaggebend für die Sicherheit der elektronischen Kommunikation.

Mitarbeiter schulen

Jeder Mitarbeiter, der mit Technologie in Berührung kommt, sollte über die damit verbundenen grundlegenden Sicherheitsrisiken in speziellen Schulungen wie Kaspersky Security Awareness Trainings informiert werden.

Angriffe mit Expertenwissen blockieren

Cyberangriffe werden zielgerichtet durchgeführt; Geräte und Server sowie Institutionen und einzelne Mitarbeiter werden konkret ausgewählt und angesprochen. Einmal im System wird dieses nach den wertvollen Daten durchsucht, bevor der Diebstahl oder eine Blockade erfolgen. Solche Angriffe sind schwer zu erkennen, können aber durch einen umfassenden Schutz wie Kaspersky Managed Detection and Response abgewehrt werden.

Mehr IT-Sicherheit im Gesundheitswesen ist ebenso unabdingbar wie umsetzbar. Die Sicherheitsindustrie bietet professionelle Lösungen und tiefgehende Expertise, von der alle Institutionen des Gesundheitswesens profitieren können. Wenn – wie von der Bundesregierung geplant – vier Milliarden Euro in die Digitalisierung von Krankenhäusern fließen werden, sollten Betreiber die Gelegenheit nutzen und in die Sicherheit der digitalen Infrastruktur investieren.



Autor: Christian Milde, Geschäftsführer DACH bei Kaspersky



enovacom

Saving time for care

Kümmern wir uns um
diejenigen, welche sich um
die medizinische Versorgung
kümmern.

#BiomedizinischeInteroperabilität #Interoperabilität
#vernetzteGesundheit #Gesundheitsdaten
#AustauschvonGesundheitsdaten #Datenlager

Haben sie Fragen oder Projekte ?

Fabrice Treziny - Enovacom Deutschland
ftreziny@enovacom.com

www.enovacom.de/



Stormshield bietet Kliniken wirksame IT-Sicherheit

Schutz vor Cyberstürmen

„Sturmhaube, Sturmschutz“, so lässt sich Stormshield übersetzen. Und das trifft auch recht genau, was das Tochterunternehmen von Airbus Cybersecurity tut: Unternehmen schützen, die potenziell dem Sturm eines Cyberangriffs ausgesetzt sind. Stormshield ist 2013 aus dem Zusammenschluss von NETASQ, gegründet 1998, und ARKOON, gegründet 2000, entstanden. Mehr verrät uns Uwe Gries, Country Manager DACH, im Interview.

Herr Gries, in welchen Bereichen kommen Ihre Lösungen zum Einsatz?

U. Gries: Wir konzentrieren uns auf die Branchen, die ein erhöhtes Sicherheitsbedürfnis haben, namentlich Regierungsbehörden, Militäreinrichtungen und generell kritische Infrastrukturen. Dazu gehören für uns seit langer Zeit auch schon Gesundheitseinrichtungen.

In welchen Ländern ist Stormshield aktiv?

U. Gries: Das Unternehmen agiert weltweit mit dem Fokus auf Europa. Das ist unsere DNA. Wir sind ein rein europäisches Unternehmen, die Forschung und Entwicklung finden komplett in Europa statt und hier sind wir auch vom Vertriebs- und Servicenetz äußerst gut aufgestellt. Zudem genießen wir hier durch die Verbindung mit Airbus ein großes Renommee.

Und wie sieht es in Deutschland aus?

U. Gries: Hier operieren wir vom Münchener Technologiepark Messestadt West aus. Neben eigenen Mitarbeitern setzen wir auf ein eng gewobenes Partnernetzwerk, mit dem wir auch regional sehr gut aufgestellt sind und unsere Kunden vor Ort betreuen können. Genauso ist es in Österreich und der Schweiz.

Welche Aufgaben übernehmen die Partner?

U. Gries: Sie übernehmen Vertrieb, Service und Support unserer Lösungen. Unsere Organisation unterstützt sie dabei, übernimmt aber durchaus auch Präsentation und Beratungsleistungen bei großen Einrichtungen.

Was kann ich mir unter Beratungsleistungen vorstellen?

U. Gries: Nicht die klassische Beratung auf jeden Fall, sondern eher ein Sparring. Wir sprechen mit den IT-Abteilungen der Häuser über Sicherheitsrisiken und erkennen dann, wo gegebenenfalls noch Schutzbedarf besteht. Uns geht es darum, dass sich der Kunde noch sicherer fühlt.



Uwe Gries, Country Manager DACH

Welche Lösungen bieten Sie Gesundheitseinrichtungen?

U. Gries: Unser Lösungsportfolio ist relativ breit. Im Bereich KRITIS sehen wir im Wesentlichen zwei Lösungen: zum einen das Unified Threat Management, kurz UTM, das umgangssprachlich Firewall genannt wird. Das betrifft den Schutz der physischen IT, des internen und externen Netzverkehrs. Komplexer ist unsere sogenannte Stormshield Endpoint-Security, die zusätzlich zum Anti-Virenschutz installiert wird. Die hilft, Zero Day-Attacken abzuwehren, also Hackerangriffe, die unbekannte Schwachstellen in Software-Programmen ausnutzen. Dabei handelt es sich um eine verhaltensbasierte Erkennung, gepaart mit einem umfangreichen Berichtswesen. Wenn eine Attacke also teilweise erfolgreich war, können wir zum Beispiel nachvollziehen, wann und wo sie stattgefunden hat, und dann gezielte Maßnahmen einleiten.

Maßnahmen heißt also, vorhandene Sicherheitslücken zu schließen?

U. Gries: Das wäre erst der letzte Schritt. Zuerst einmal kann man nachvollziehen, welche Bereiche überhaupt betroffen sind. In der Regel müssen nach einem Angriff alle Systeme neu installiert und aufgesetzt werden. Das sind die Fälle, von denen man dann in der Zeitung liest, dass die Einrichtung ein, zwei Wochen gar nicht mehr in der Lage war zu arbeiten. Wenn eine Attacke nur teilweise erfolgreich war, reicht es oft schon, Segmente, Abteilungen oder Unternehmensbereiche zu isolieren, so dass der Rest relativ normal weiterarbeiten kann. Das ermöglichen wir mit unserer Lösung. In letzter Konsequenz werden dann die Sicherheitslücken geschlossen.

Was ist für Stormshield am deutschen Gesundheitsmarkt so interessant?

U. Gries: Nun, wir sehen, dass – bedingt auch durch die Corona-Pandemie – das Bewusstsein für die Notwendigkeit einer guten Gesundheitsversorgung geschärft ist. Das bedeutet aber auch, dass die Medizingeräte und IT in den Krankenhäusern ausreichend geschützt sein müssen. Und da wollen wir unseren Beitrag leisten.

Es war in den letzten Jahren für uns überraschend zu beobachten, dass gerade im Bereich IT-Sicherheit sehr gespart worden ist. Gesundheitseinrichtungen haben teilweise hohe Millionenbeträge in Röntgengeräte investiert, sich dann aber häufig schwer damit getan, auch Geld in die Sicherheit der IT zu stecken. Und jetzt nehmen wir da einen Mindshift wahr, also dass Kliniken durchaus bereit sind, auch in entsprechende Schutzmechanismen zu investieren.

Worauf führen Sie das zurück, Herr Gries?

U. Gries: Das liegt sicher an den zahlreichen, teils verheerenden Vorfällen, die gerade im letzten Jahr publik geworden sind, auch im Gesundheitswesen. Da ist schlicht die Wahrnehmung gestiegen. Jeder konnte sehen, welche dramatischen Auswirkungen ein derartiger Angriff haben kann, bis hin zur kompletten Lahmlegung der gesamten IT. Viele Krankenhäuser sind auf dem Weg in die Digitalisierung bereits relativ weit. Und da möchte man sich das Szenario der Rückkehr zur Zettelwirtschaft nicht vorstellen, weil das den Betrieb sehr nachhaltig stören und einen immensen Arbeitsaufwand nach sich ziehen würde. Damit geht mittlerweile dann auch eine Anhebung der Budgets für IT-Sicherheit einher.

Wie viele Krankenhäuser arbeiten europaweit schon mit der Stormshield-Lösung?

U. Gries: Hochgerechnet sind es ein paar Hundert, doch zum Gesundheitssektor gehören auch Kunden wie der Pharmakonzern sanofi aventis oder Mercator Medical, ein großer Hersteller medizinischer Einwegmaterialien.

Warum sollten Krankenhäuser mit den Lösungen von Stormshield arbeiten?

U. Gries: Wir sind ein europäisches Unternehmen. Wir sind äußerst erfahren, weil wir unser Geschäft bereits sehr lange betreiben. Die Lösungen sind voll durchentwickelt. Wir investieren nach wie vor sehr viel in Forschung und Entwicklung. Wir haben eine flächendeckende und schlagkräftige Vertriebs- und Serviceorganisation im deutschsprachigen Bereich. Wir sind vor Ort vertreten. Und wir können unsere Krankenhäuser, die wir bedienen, auch immer vollumfänglich unterstützen.

Wo sehen Sie das deutsche Gesundheitswesen in fünf bis sieben Jahren?

U. Gries: Hoffentlich voll digitalisiert. Ich bin sehr häufig in Krankenhäusern unterwegs und sehe dort bereits teilweise wirklich gute Ansätze und Umsetzungen. Das ist nicht so schlecht, wie es häufig dargestellt wird. Deshalb bin ich auch zutiefst davon überzeugt, dass wir in fünf, sechs oder sieben Jahren – nicht zuletzt durch die Lektionen, die wir aus der Pandemie gelernt haben – vollständig digital aufgestellt sein werden. Und dass die medizinischen Mitarbeiter der Krankenhäuser, auch davon bin ich überzeugt, dann viel mehr Zeit für ihre Patienten haben werden.

Damit wird dann auch der Bedarf an Sicherheitslösungen steigen, speziell wenn man an den intersektoralen Informationsaustausch denkt.

U. Gries: Nun, grundsätzlich sind die Kommunikationswege ja bereits sicher. Wenn es Probleme gibt, dann häufig durch die Fehlkonfiguration eigentlich sicherer Geräte. Manchmal trifft man unverschlüsselte Kanäle an, das ist aber zum Glück die Ausnahme. Schließlich sind die Produkte und Lösungen dafür im Wesentlichen ja auch auf dem Markt. Hier mangelt es dann doch eher am Gefahrenbewusstsein der Anwender. Verständlich, dass die Kernkompetenz eines Arztes oder einer Pflegekraft nicht die IT-Sicherheit ist. Da ist aus meiner Sicht der Gesetzgeber gefordert, Vorschriften zu erlassen, die die IT-Industrie dann auch sicher umsetzen muss.

Vielen Dank für das interessante Gespräch, Herr Gries.

Das Interview führte Ralf Buchholz.





Digitalisierung und Vernetzung im Gesundheitswesen

#teamedalus
#together4success
#healthcareIT

dedalusgroup.de

Die Sicherheit steht im Fokus

Digitalisierung der Krankenhäuser erfordert viele Veränderungen, die meisten von ihnen aber nicht in der IT selbst, sondern in den Prozessen. Dabei steht die Sicherheit im Fokus. Führungskräfte des Krankenhauses, aber auch Krankenhausgesellschaften, Eigentümer und auch Kostenträger sind gefragt, um Krisenvorsorge und Krisenbewältigung - und Finanzierung - erfolgreich stemmen zu können. Von Lars Forchheim, KH-IT Vorstand - Beisitzer

Gerade während einer Pandemie bzw. Krisensituation des Gesundheitssystems steht die Patientenversorgung im Mittelpunkt. Gerade dann sind Kennzahlen für die Steuerung des Geschehens entscheidend.

Für die Patientenversorgung selbst, aber auch für die Steuerung der Abläufe über Kennzahlen ist die Abhängigkeit von IT-Werkzeugen bereits heute sehr hoch. Im weiteren digitalen Wandel wird diese Abhängigkeit noch steigen. Die Sicherheit solcher Systeme, vor allem aber der damit verarbeiteten Informationen, spielt damit für den Alltag eine ganz entscheidende Rolle.

Trotzdem ist das Thema Informationssicherheit in der Öffentlichkeit und vor allem im Krankenhaus nur schwer zu vermitteln. Der Begriff Sicherheit wird im englischen Raum mit den beiden Wörtern „Safety“ und „Security“ beschrieben. Am Beispiel des Autos lassen sich die unterschiedlichen Bedeutungen gut aufzeigen: da steht „Safety“ z.B. für den Sicherheitsgurt – wir können uns ja kaum noch ans Auto ohne Sicherheitsgurt erinnern. Ebenso ist „Security“ im Auto eine Selbstverständlichkeit – das Auto wird mit der passenden Funkfernbedienung geöffnet, bzw. geschlossen und bedankt sich mit einem Blinken. „Safety“, also die Sicherheit in der

medizinischen Versorgung kann nur mit regelmäßigen Updates von Systemen in der vernetzten Umgebung innerhalb vereinbarter Wartungsfenster erreicht werden. Das wird aber nur selten tatsächlich umgesetzt. Die „Security“-Funktion des An- und Abmeldens an den Systemen ist den meisten Mitarbeitern lästig und zu aufwändig.

Überträgt man die Anforderungen der Informationssicherheit in der medizinischen Versorgung mit etwas Ironie in die Analogie zum Auto, könnte das so aussehen:

- Warum benötige ich für meinen ganzen Fuhrpark immer einen extra Autoschlüssel. Kann ich nicht einen Schlüssel für alle Fahrzeuge nutzen?
- Warum kann ich meinen 4-Türer nicht einfach zum Transporter umrüsten? Der Tuning-Händler des Vertrauens kann das in wenigen Sekunden.
- Warum muss mein Auto nach einem Dauereinsatz (7*24h) zur Inspektion (Systemupdate)?

Informationssicherheit als eigenständige Disziplin

Die Informationssicherheit als eigenständige Disziplin ist aufgrund schlechter Erfahrungen aus der Krisenvorsorge und Krisenbewältigung entstanden. Im Katastrophenfall kümmern sich üblicherweise Experten um die Bewältigung und Schadensbegrenzung. Um nicht nur zu reagieren, sondern proaktiv die Eintrittswahrscheinlichkeit zu reduzieren oder wenigstens den dabei entstehenden Schaden, kümmern Experten sich um den Eintritt der „Krise“ bevor sie passiert. Damit wird die „Feuerwehr“ verbessert. Durch die Betrachtung der Risiken gehen wir in die Vorsorge, der „Brandenschutz“ wird verbessert.

Die Informationssicherheit übernimmt genau diese Aufgabe – im Vorfeld eines Schadensereignisses prüfen, welche Risiken existieren und wie mit ihnen am besten umgegangen wird. Der Aufwand für die Durchführung dieser Analysen ist beträchtlich, denn es ist nicht damit erledigt, sich einige Gedanken zu machen und ein paar Workshops durchzuführen. Regelmäßige Übungen von Störungen, auch IT-Störungen, sollten zum Regelbetrieb des Krankenhauses oder der Arztpraxis gehören. Diese Übungen helfen Abläufe zu testen, sowie Fehler zu erkennen und zu beheben.

Entscheidend ist dabei, die Komplexität der Systeme und der Prozesse den voraussichtlich schwierigen Rahmenbedingungen anzupassen. In der Praxis wird überwiegend zentralisiert, im Krisenmodus ist aber die Resilienz der kleinen Organisationseinheiten, also lokalen Systeme, entscheidend. Dieser Ansatz kann nur durch regelmäßige Übungen getestet und gelernt werden.

Anwendung der Branchen Sicherheitsstandards (B3S)

Die gesetzlichen Anforderungen unterscheiden zwischen Häusern gleich/über dem Schwellenwert für KRITIS-Häuser und solche unter dem Schwellenwert. Beide „Gruppen“ müssen kontinuierlich an der Verbesserung der Informationssicherheit und damit der Ausrichtung am „Stand der Technik“ arbeiten. Am besten lässt sich dieser erreichen durch die Anwendung der Branchen Sicherheitsstandards (B3S). Er wurde und wird von der DKG mit Einbeziehung des Branchenarbeitskreises medizinische Versorgung ständig weiterentwickelt. In der medizinischen Versorgung gelten folgende Schritte:

- Strukturelle Analyse
- Risikobewertung / Risikomanagement
- Compliance Management / Rechtliche Rahmenbedingungen
- Prozessorganisation
- Aktionsplan - Maßnahmen verfolgen / Projektmanagement / Changemanagement
- Implementierung/Integration - Projektmanagement / Changemanagement
- Ständige Verbesserung/Messung
- Sicherheitsinfrastruktur Prüfung / Bewertung
- und damit wieder Start der Struktureller Analyse ...

Die Handlungsempfehlungen aus Sicht des Branchenarbeitskreises medizinische Versorgung sind mit dem B3S als „Was?“ beschrieben. In der Praxis wird aber oft

nach den „Wie?“ gesucht. Die Universität der Bundeswehr hat mit Smart Hospitals einen sehr gut geeigneten Maßnahmenkatalog für Informationssicherheit herausgebracht. Die DKG erarbeitet zurzeit eine entsprechende Handlungsempfehlung für alle Krankenhäuser. In der Praxis ist es erforderlich, die Kernpunkte der obigen Liste immer wieder zu durchlaufen.

KHZG - Signal für die Bedeutung der IT-Sicherheit

Im Rahmen des KHZG wird zwar primär die Digitalisierung im Krankenhaus gefördert, aber mindestens 15% der Fördersumme müssen in die IT-Sicherheit investiert werden. Diese Maßnahme ist ein sehr gutes Signal für alle und zeigt die Bedeutung der IT-Sicherheit.

Die weitere Finanzierung der Betriebskosten für die über das KHZG beschafften Systeme ist nach wie vor unbefriedigend gelöst. Im Moment müssen die Häuser die zu erwartenden Pönnen für die unzureichende Digitalisierung gegen die künftigen Betriebskosten rechnen.

Aber auch ein paar kritische Fragen bringen Bewegung in die Gedankenwelt: Was kostet mich ein Ausfall eines OP-Tages? Wie kann ich nach einem Brand wieder anfahren? Diese Szenarien zeigen den Wertbeitrag, und aktuelle Beispiele zeigen immer wieder, dass die Prozesse in Papier viel mehr Ressourcen benötigen. Daher sind die 15% aus meiner Sicht ein guter Wert. Jede Umsetzung von KHZG-Projekten sollte die Betriebskosten in der Kalkulation ausweisen, dann bleiben sie auch im Blick.

Während für die KHZG-Projekte wenigstens die Finanzierung der Umsetzung geklärt ist, bleiben die Betriebskosten und vor allem die zahlreichen Projekte außerhalb des KHZG, die im Rahmen der Digitalisierung in den nächsten Jahren umgesetzt werden müssen.

Aus meiner Sicht ist dies nur durch Abschaltung von Alt-Systemen sowie die effektive und effiziente Nutzung neuer IT-Systeme zu schaffen.

All diese Veränderungen erfordern nicht nur eine klare Vision, eine solide Strategie und gutes Projektmanagement – die Veränderungen können nur dann wirklich umgesetzt werden, wenn sie durch ein strukturiertes Änderungsmanagement begleitet werden.

Digitalisierung erfordert viele Veränderungen, die meisten von ihnen aber nicht in der IT sondern in den Prozessen der Krankenhäuser. Damit ist klar, dass die IT dies alles nicht allein lösen kann, sie ist hier nur der Lieferant von Werkzeugen. Tatsächlich sind alle Führungskräfte des Krankenhauses, aber auch der Krankenhausgesellschaften, der Eigentümer und auch der Kostenträger gefragt, um diese Veränderung erfolgreich stemmen zu können.

Sonst faxen wir in 20 Jahren immer noch Befunde durch die Gegend.



Lars Forchheim, KH-IT Vorstand – Beisitzer: „Die weitere Finanzierung der Betriebskosten für die über das KHZG beschafften Systeme ist nach wie vor unbefriedigend gelöst.“



5G-Einsatz in Kritischen Infrastrukturen (KRITIS) - Wunsch und Wirklichkeit

Bei der Spezifikation des 5G-Standards hat das Standardisierungsgremium 3GPP die Herausforderungen Kritischer Infrastrukturen (KRITIS) adressiert. 3rd Generation Partnership Project ist eine weltweite Kooperation von Standardisierungsgremien für die Standardisierung im Mobilfunk. Basierten die IT-Systeme, -Komponenten und -Prozesse von KRITIS-Betreibern bisher auf privaten Netzen oder TETRA Mobilfunknetzen, bietet der neue 5G-Standard als erster – und damit anders als die vorherigen Generationen – Mission Critical Services. In der Praxis fehlen 5G-Betreibern offenbar Kenntnisse und Tools zum sicheren Betrieb.

Mission Critical Services

Der Begriff Mission Critical Services (MCX Service) beschreibt einen Kommunikationsdienst, der die Potentiale widerspiegelt, die missionskritische Anwendungen ermöglichen. Dieser wird Endnutzern missionskritischer Organisationen und Anwendungen für andere Unternehmen und Organisationen (z.B. Versorgungsunternehmen oder Eisenbahnen) zur Verfügung gestellt wird.

Der 5G-MCX Service wird

unterteilt in:

- Mission Critical Push To Talk (MCPTT)
- Mission Critical Video (MCVideo)
- Mission Critical Data (MCDData)

Durch MCX Services können Sitzungen mit Priorität aufgerufen, verändert, aufrechterhalten und veröffentlicht werden.

Gleichzeitig ist es möglich, vorrangige Datenpakete auch unter der Bedingung von Netzwerküberlastungen zu übermitteln. Die Prioritätsbehandlung für einen MCX Service umfasst dabei die Handhabung von dringlichen Mitteilungen, einschließlich der Prioritätsbehandlung bei Authentifizierungs-, Sicherheits- und Mobilitätsmanagementverfahren.

5G ist die erste Mobilfunkgeneration, die Höchstdatenübertragung mit niedrigen Latenzen und in Verbindung mit der Vernetzung tausender Geräte ermöglicht – und das alles unter missionskritischen Kommunikationsanforderungen. Damit wird das Internet of Things (IoT) durch den 5G-Standard auch für KRITIS-Betreiber Realität.

<https://www.tuvit.de/de/tuevit/5g/5g-und-kritis/>

5G-Betreibern fehlen Kenntnisse und Tools zum sicheren Betrieb

5G legt erhebliche Herausforderungen bei Kritischer Infrastrukturen (KRITIS) offen. Große Lücken in der Sicherheitskompetenz bei Mobilfunkbetreibern weist eine neue Studie auf. Die Diskrepanz in der Sichtweise der Netzwerkbetreiber auf die Sicherheit ernüchtert. In vielen Fällen konnten diese noch nicht durch Unternehmenspartnerschaften geschlossen werden.

Mit intelligenter Vernetzung und leistungsstarken Mobilfunknetzen entstehen im Krankenhaus neue Möglichkeiten, um gesund zu werden und – noch besser – gesund zu bleiben. Durch den Mobilfunkstandard 5G können Fitnessuhren in Echtzeit den Blutdruck und viele weitere Vitaldaten an den Nutzer oder gleich an den zuständigen Arzt



übermitteln. Gesundheitliche Zwischenfälle können durch ein Echtzeit-Monitoring verhindert werden, bevor sie entstehen.

Laut der Studienerkenntnissen verkaufen 68 Prozent der Netzbetreiber private drahtlose Netzwerke an Unternehmenskunden – der Rest plant, dies bis 2025 zu tun. Fast die Hälfte (45 Prozent) der Betreiber hält es für äußerst wichtig, in Sicherheit zu investieren, um langfristige Umsatzziele zu erreichen. Zu diesem Zweck planen 77 Prozent der Betreiber, Sicherheit als Teil ihrer privaten Netzwerklösungen anzubieten. Fast die Hälfte (45 Prozent) der Betreiber hält es für äußerst wichtig, in Sicherheit zu investieren, um langfristige Umsatzziele zu erreichen.

Die Studie kommt darüber hinaus zu folgenden Ergebnissen:

51 Prozent der Netzbetreiber sehen Edge Computing (Multi-Access Edge Computing, oder MEC) als einen wichtigen Bestandteil ihrer zukünftigen Unternehmensstrategie an. Nur 18 Prozent der Betreiber sichern derzeit ihre Endpunkte oder Edge.

48 Prozent der Betreiber nennen einen Mangel an adäquaten Kenntnissen oder Tools zur Erkennung von Schwachstellen als eine der größten Sicherheitsherausforderungen hinsichtlich 5G.

39 Prozent haben nur einen begrenzten Pool an Sicherheitsexperten.

41 Prozent kämpfen mit Schwachstellen in der Netzwerkvirtualisierung.

Die Rolle, die Netzbetreiber bei der Sicherung des privaten Netzwerk-Ökosystems einnehmen können, ist in der 5G-Ära besonders wichtig. Dass Unternehmen neue Kommunikationstechnologien (5G, Edge-Computing, Cloud-Computing, Private Wireless, IoT) nutzen, um ihr Geschäft bereit für die digitale Transformation zu machen, verändert die Bedrohungsvektoren. Die Netzbetreiber befinden sich jedoch in der idealen Lage, um diese zu adressieren und ihren Kunden dadurch Mehrwerte zu bieten. Um dieser Rolle gerecht zu werden, sollten sie jedoch ihre Kompetenzen erweitern oder Partnerschaften mit Security-, Cloud- oder IT-Anbietern eingehen. Auf diese Weise können sie die Lücken in ihren Sicherheitsportfolios schließen und die fehlende Expertise ausgleichen.

Die Studie basiert auf zwei Marktumfragen von GSMA Intelligence: Die Marktumfrage „GSMA Intelligence Operators in Focus 2021“ befragte 100 Entscheidungsträger von Netzbetreibern weltweit hinsichtlich ihrer Meinung zu den Chancen, die sich im Enterprise-Segment bieten. „The GSMA Intelligence Enterprise in Focus 2020“-Marktumfrage befragte 2.873 Unternehmen in acht Branchen und 18 Ländern.

Sie machen das, was Sie am besten können ...



Ralf Buchholz

... und ich übernehme die Kommunikation zu Ihren Zielgruppen dafür.

- Strategische Beratung
- Pressearbeit
- Corporate Publishing
- Bewegtbild
- Social Media

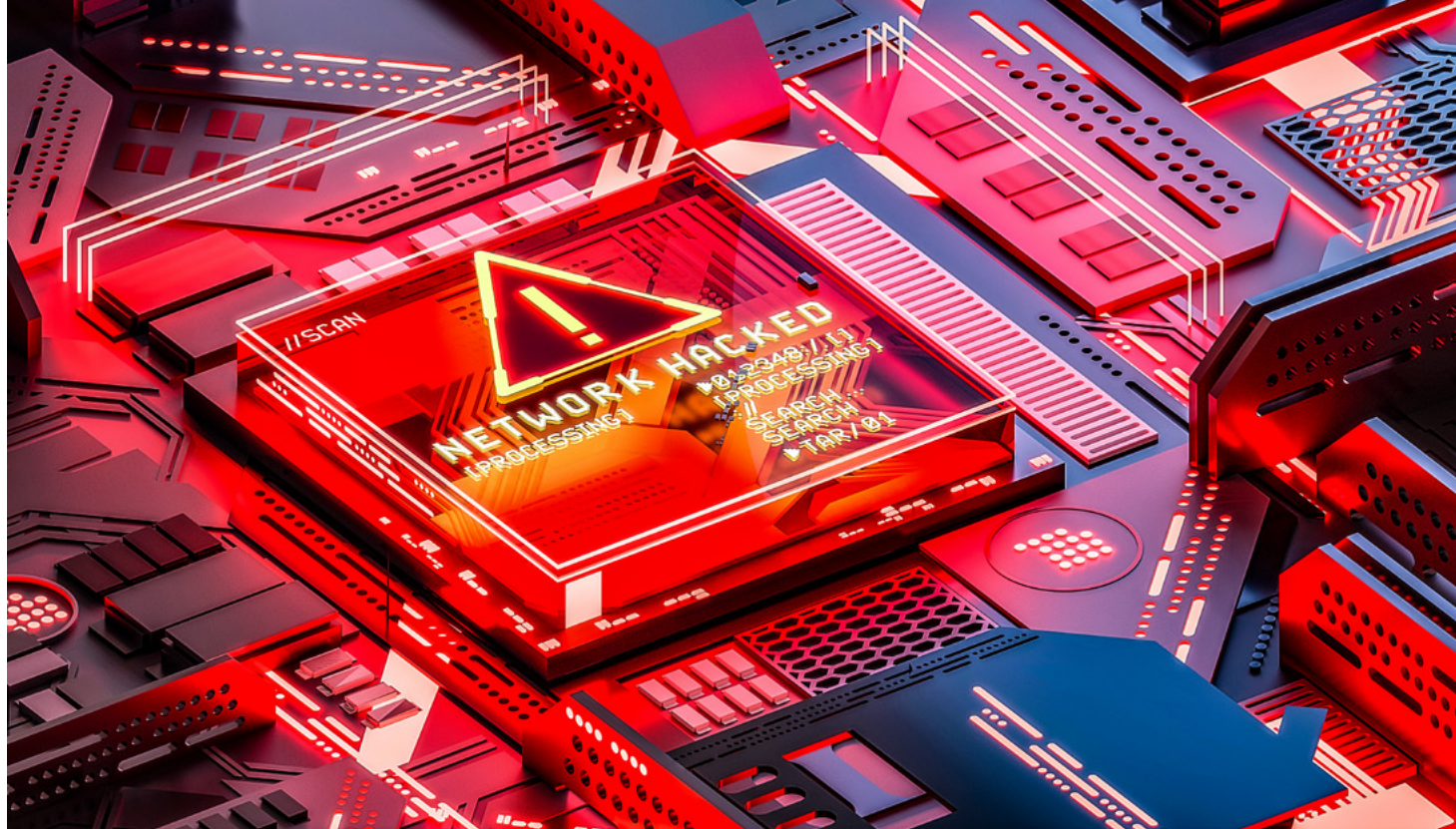
Alles Weitere finden Sie unter www.ralfbuchholz-hc.de



ralf buchholz.
healthcare communications.

Telefon: (0 40) 20 97 68 05

r.buchholz@ralfbuchholz-hc.de



Handlungsfeld IT-Infrastruktur im Krankenhaus

Krankenhäuser erbringen als eine der tragenden Säulen des Gesundheitswesens vielfältige medizinische und pflegerische Dienstleistungen und zählen daher zu den Kritischen Infrastrukturen unserer Gesellschaft. Der effektive Umgang mit IT-Risiken erfordert eine strukturierte Vorgehensweise, in welcher der IT-Risikoanalyse als wichtigem Werkzeug zur Identifikation der relevanten Risiken eine zentrale Rolle zukommt. Die IT-Risikoanalyse unterstützt bestehende Ansätze zum Informationssicherheits- und Risikomanagement – zusammen mit einer organisatorischen Verankerung des Themas „IT-Sicherheit“.

Die Funktionsfähigkeit von Krankenhäusern hängt nicht nur von weiteren externen Kritischen Infrastrukturen, wie beispielsweise der Strom- und Wasserversorgung, abhängig, sondern auch bereits in hohem Maße von der vor Ort eingesetzten Informationstechnologie. Diese findet sich in zahlreichen Formen von Anwendungen zur Behandlungsdokumentation über Inventar- und Bestellsysteme bis hin zu medizintechnischen Geräten wieder. Sie unterstützt bei bisher papiergebundenen Arbeitsabläufen und erleichtert Diagnose- und Behandlungsprozesse oder macht diese sogar erst möglich.

Neben der Möglichkeit zur Optimierung und Effizienzsteigerung von Pro-

zessen birgt die zunehmende IT-Unterstützung aber auch neue Risiken, denen im Rahmen des Risikomanagements entsprechend begegnet werden muss. Bisher standen hier vor allem Risiken im Bereich des Datenschutzes, beispielsweise bei der Einführung elektronischer Patientenakten, im Fokus von Untersuchungen zur Sicherheit der Krankenhaus-IT.

Aus dem Blickwinkel Kritischer Infrastrukturen zur Aufrechterhaltung der Verfügbarkeit der medizinischen Versorgung treten solche Überlegungen in den Hintergrund. Der effektive Umgang mit IT-Risiken erfordert in jedem Fall eine strukturierte Vorgehensweise, in welcher der IT-Risikoanalyse als wichtigem Werkzeug zur Identifikation der

relevanten Risiken eine zentrale Rolle zukommt. Die IT-Risikoanalyse unterstützt damit bestehende Ansätze zum Informationssicherheits- und Risikomanagement und erleichtert sowohl Priorisierung als auch Auswahl der umzusetzenden Maßnahmen. Dabei ersetzt die IT-Risikoanalyse aber in keinem Fall die zwingend notwendige organisatorische Verankerung des Themas „IT-Sicherheit“ oder eine umfassende Sicherheitskonzeption nach gängigen Standards.

Aufgrund seiner wichtigen Aufgaben für die Gesundheitsversorgung der Bevölkerung steht ein Krankenhaus, auch durch gesetzliche Regelungen, in der Pflicht, die Verfügbarkeit seiner Dienstleistungen zu gewährleisten. Angesichts

der zunehmenden Abhängigkeit der Patientenversorgung von einer störungsfrei funktionierenden IT-Infrastruktur muss folglich auch der IT-Sicherheit ein hoher Stellenwert eingeräumt werden. Einige Aspekte benennen für IT-Sicherheitsverantwortliche Handlungsfelder, die für die Gewährleistung angemessener IT-Sicherheit besonders wichtig sind.

Fragepunkte für Handlungsfelder

Sind die Prozesse Ihrer Einrichtung und deren IT-Abhängigkeiten bekannt?

Eine regelmäßig aktualisierte Prozessübersicht (z. B. als „Prozesslandkarte“) erleichtert es nicht nur, Effektivität und Effizienz der Abläufe eines Krankenhauses zu verbessern, sondern auch die kritischen Prozesse und IT-Abhängigkeiten zu erkennen. Sie ist damit eine wichtige Grundlage für die IT-Risikoanalyse. Hierfür sollte die Übersicht angemessen detailliert die Krankenhausprozesse, deren Zusammenwirken und deren IT-Unterstützung beschreiben.

Verfügen die IT-Zuständigen Ihrer Einrichtung über einen umfassenden Überblick über die IT-Infrastruktur und deren Komponenten?

Ein aktuelles und vollständiges Inventar der IT-Infrastruktur hilft bei der Ermittlung derjenigen IT-Komponenten, die für das korrekte Funktionieren der kritischen IT-Anwendungen unverzichtbar sind. Es erleichtert darüber hinaus die Entwicklung von Sicherheitskonzepten zum Schutz dieser Anwendungen. Das

Inventar sollte sämtliche eingesetzten IT-Systeme (Server, Clients usw.) und alle für deren Betrieb wichtigen Angaben enthalten, beispielsweise Einsatzzweck, Softwareausstattung sowie die Art der Netzanbindung.

Sind die für Ihre Einrichtung unverzichtbaren (kritischen) Bestandteile der IT-Infrastruktur bekannt?

Die Kenntnis der unverzichtbaren IT-Anwendungen und IT-Komponenten ist eine Grundvoraussetzung für den Schutz vor IT-Ausfällen, welche die Handlungsfähigkeit Ihrer Einrichtung gefährden, und unterstützt die Auswahl angemessener Sicherheitsmaßnahmen. Die IT-Risikoanalyse ist ein Instrument, um die bestehenden Kenntnisse durch ein strukturiertes Vorgehen systematisch und möglichst vollständig zu erweitern.

Gibt es in Ihrer Einrichtung eine ausgewiesene Zuständigkeit für IT-Sicherheit?

Für die organisatorische Verankerung der IT-Sicherheit in Ihrer Einrichtung ist es hilfreich, wenn in Person eines IT-Sicherheitsbeauftragten eine zentrale Zuständigkeit für die Koordination der zugehörigen Aufgaben festgelegt wird. Ein IT-Sicherheitsbeauftragter ist der Krankenhausleitung berichtspflichtig und sollte eng mit allen Stellen zusammenarbeiten, die mit Sicherheitsfragen der Einrichtung befasst sind. Ihm obliegt es vor allem, die Entwicklung von Sicherheitskonzepten zu steuern und die Umsetzung der darin vorgesehenen Maßnahmen zu kontrollieren.

Sind die Mitarbeiter Ihrer Einrichtung für den sicheren Umgang mit kritischer Informationstechnik geschult?

Zur Vermeidung von IT-Sicherheitsvorfällen ist es erforderlich, dass die Benutzer hinreichend für Risiken bei der Anwendung von IT sensibilisiert und im sicheren Umgang mit dieser Technik geschult sind. Auch Administratoren und andere mit dem IT-Betrieb betraute Mitarbeiter müssen ausreichende Fortbildungsmöglichkeiten erhalten. Die IT-Risikoanalyse kann dazu beitragen, die Sensibilität für IT-Sicherheit in einem Krankenhaus zu erhöhen.

Liegen Notfallkonzepte für die kritischen IT-Anwendungen Ihrer Einrichtung vor?

Die IT-Risikoanalyse zeigt auf, welche IT-Anwendungen für die kritischen Prozesse eines Krankenhauses besonders wichtig sind. Trotz aller Sicherheitsmaßnahmen können IT-Ausfälle niemals völlig ausgeschlossen werden. Daher sind für alle kritischen IT-Anwendungen Notfallkonzepte zu entwickeln, in denen Ersatzmaßnahmen zur Überbrückung eines IT-Ausfalls und Maßnahmen für den Wiederanlauf der IT-Anwendungen beschrieben sind. Diese IT-Notfallkonzepte sind in ein Gesamtnotfallkonzept des Krankenhauses zu integrieren, in dem das Vorgehen bei Ausfällen weiterer kritischer Ressourcen beschrieben ist.

Quelle: Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT, BSI, www.bsi.bund.de

Krisenmanagement in Unternehmen: 9-Punkte-Checkliste

Auch in außergewöhnlichen Situationen, wie der aktuellen pandemischen Ausbreitung des neuen Coronavirus (SARS-CoV-2), müssen grundlegende Aufgaben bei der Versorgung der Bevölkerung wahrgenommen werden. Zu diesen, von Betreibern Kritischer Infrastrukturen und weiteren Unternehmen bereitgestellten Dienstleistungen, werden aktuell seitens der Länder und Kommunen Kriterienkataloge erstellt und fortgeschrieben.

Um arbeitsfähig zu bleiben ist das betriebliche Krisenmanagement gefragt. Dessen Ziele sind: Der schnellstmögliche Wiederanlauf der kritischen Prozesse nach einer Störung.

Viele Unternehmen befinden sich bereits in der Krisenbewältigung und haben ihre Krisenorganisation aktiviert. Die folgende 9-Punkte-Checkliste unterstützt dabei, das betriebliche Krisenmanagement einem Schnell-Check zu unterziehen.

Bereitstellung von Dienstleistungen Kritischer Infrastrukturen

Krisenmanagement: 9-Punkte-Checkliste

1 Alle relevanten Aufgaben und konkrete Entscheidungsbefugnisse sind im Krisenmanagement festgelegt (Lagefeststellung und -beurteilung, Entscheidung und Kontrolle) und konkreten Personen und deren Vertretungen zugewiesen.

2 Regelungen zur internen und externen Krisenkommunikation sind festgelegt (Bestimmung der internen und externen Informationswege, konsistente Information der Beschäftigten, einheitliche Sprachregelung, Auswahl eines Pressesprechers, etc.).

3 Alle Beschäftigten sind hinsichtlich eines verantwortungsvollen Verhaltens und Gefahren während einer Pandemie am Arbeitsplatz und auch im privaten Umfeld informiert (Empfehlungen des RKI: www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/nCoV.html).

4 Alle Beschäftigten sind über die Krisenorganisation und die damit ggf. verbundenen Änderungen in der Ablauforganisation informiert.

5 Das Schlüsselpersonal für Kernprozesse ist identifiziert und Ersatzpersonal steht zur Verfügung (ggf. kann auf Personal aus benachbarten Einrichtungen, Personal im Ruhestand oder Personal in der Ausbildung zurückgegriffen werden).

6 Soweit möglich, ist die Lagerhaltung (Betriebsmittel, Vorprodukte, Ersatzteile etc.) zur Aufrechterhaltung des Betriebes bzw. eines Notbetriebes an Engpässe lagebedingt angepasst.

7 Die Pläne für eine kontrollierte Stilllegung des Betriebes sind für den Fall aktualisiert, dass ein grundlegender Personalmangel eintritt.

8 Alle zur Krisenbewältigung erforderlichen externen Einrichtungen (Zulieferer, Dienstleister, Behörden etc.) sind bekannt und bedarfsgerecht in die Informationsprozesse des Krisenmanagements eingebunden. Dabei wurde auch berücksichtigt, von welchen Dienstleistungen das eigene Unternehmen abhängt und welche Unternehmen von den selbst bereitgestellten Dienstleistungen abhängen.

9 Entscheidungen des Krisenmanagements werden dokumentiert und für die Nachbereitung der Krisenbewältigung vorgehalten.

Eine umfassende Checkliste zum Risiko- und Krisenmanagement bietet Leitfaden „Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement“ des Bundesministeriums des Innern, für Bau und Heimat (www.bmi.bund.de/SharedDocs/).

IoT-Geräte als Einfallstor: Healthcare-IT-Sicherheit gefährdet

Bei Internet of Things IoT genießt in der Konzeption und bei der Herstellung der einzelnen Geräte IT-Sicherheit nicht immer hohe Priorität. Etwa die Hälfte der angeschlossenen Geräte wie Ultraschall- und MRT-Geräte laufen auf veralteten Betriebssystemen ohne Wartung. Damit entsteht eine entsprechend große Angriffsfläche für Hacker, um Daten zu stehlen, zu verschlüsseln sowie für den Alltag kritische Funktionen zu sabotieren.

Sicherheitsrisiken steigen bei der Aktivität von IoT-Geräten in Unternehmensnetzwerken. Dies gilt besonders, während Organisationen auf remote Arbeitsumgebungen umstellen ⁽¹⁾. Im Vergleich zu Untersuchungen vor der Pandemie wurde ein Anstieg von Malware-Angriffen auf IoT-Geräte von 700 Prozent beobachtet. Diese Angriffe zielten auf 553 verschiedene Gerätetypen, wie Drucker, Digital Signage und Smart TVs ab, die mit IT-Netzwerken von Unternehmen verbunden waren, während viele Mitarbeiter wegen der COVID-19-Pandemie aus der Ferne arbeiteten.

Experten identifizierten die anfälligsten IoT-Geräte, die häufigsten Angriffsursprünge und -ziele sowie die Malware-Familien, die für den Großteil des bösartigen Datenverkehrs verantwortlich sind.

Ein Irrtum ist es anzunehmen, dass die Kategorie „Home Entertainment & Automation“ wTop-Gefährder seien. Die größte Vielfalt wiesen Geräte aus den Bereichen „Manufacturing“, „Enterprise“ und „Healthcare“ auf.

Die drei Länder, die am häufigsten in den Fokus von IoT-Angriffen gerieten, waren Irland (48 Prozent), die USA (32 Prozent) und China (14 Prozent). Fast 90 Prozent der kompromittierten IoT-

Geräte sendeten Daten zurück an Server in einem der drei Länder China (56 Prozent), die USA (19 Prozent) oder Indien (14 Prozent).

Konzept zum Schutz der Geräte

Um die unterschiedlichen Angriffswege zu sperren, gilt es besonders auf drei Aspekte zu achten ⁽²⁾:

Schaffen Sie volle Transparenz. Ein umfassendes Konzept zum Schutz der Geräte kann erst dann entstehen, wenn die IT-Fachkräfte über alle Geräte, die auf deren Netzwerk zugreifen, vollständig informiert sind. Viele Unternehmen verlassen sich noch darauf, Geräte manuell zu finden und zu identifizieren. Das mag für traditionelle Server und Workstations als Umgebung funktionieren, kann aber nicht mit der Vielzahl der IoT-Geräte mithalten, da dies eine automatisierte Lösung für eine vollständige Abdeckung erfordert.

Entschärfen Sie Schwachstellen. Patches und Echtzeit-Bedrohungsdaten sind das Herzstück eines jeden Sicherheitsprogramms, weswegen die meisten Unternehmen ein Patching-Programm eingerichtet haben. Doch bezüglich der meisten IoT-Geräte ist es fast unmöglich, auf dem neuesten Stand der Sicherheitsforschung zu bleiben, wenn

Firmen sich nur auf Software-Updates verlassen. So entgehen diesen oft wichtige Schwachstellen in den Geräten selbst. Eine Lösung, die Firmware-Upgrades liefert, bietet darum die besten Erfolgsaussichten.

Implementieren einer Zero-Trust-Sicherheitsarchitektur: Umsetzung strenger Richtlinien für Unternehmensressourcen, so dass Benutzer und Geräte nur auf das zugreifen können, was sie benötigen, wenn sie authentifiziert sind. Beschränken der Kommunikation auf relevante IPs, ASNs und Ports, die für den externen Zugriff benötigt werden. Nicht genehmigte IoT-Geräte, die einen Internetzugang benötigen, sollten eine Traffic Inspection durchlaufen und von allen Unternehmensdaten abgeschirmt werden, idealerweise über einen Proxy. Damit Shadow IoT-Geräte keine Bedrohung für Unternehmensnetzwerke darstellen muss das implizite Vertrauen unterbunden werden und eine strenge Zugriffskontrolle auf sensible Daten erfolgen.

IoT-Geräte können in manchen Fällen über Leben und Tod entscheiden. Entsprechend muss sichergestellt werden, dass sie – und damit auch das Netzwerk an sich – gegen Attacken geschützt sind. Aus diesem Grund sollten Krankenhäuser auf Lösungen setzen, die Transparenz schaffen, um gezielt Sicherheitslücken schließen zu können. Gleichzeitig empfiehlt sich ein Zero-Trust-Ansatz für das gesamte Netzwerk, um im Falle eines Eindringlings den Schaden so gering wie möglich zu halten.

(1) Zscaler.com

(2) checkpoint.com

IT-Sicherheit und IT-Risikoanalyse: Handlungsbedarf erkennen

Aufgrund seiner wichtigen Aufgaben für die Gesundheitsversorgung der Bevölkerung steht ein Krankenhaus, auch durch gesetzliche Regelungen, in der Pflicht, die Verfügbarkeit seiner Dienstleistungen zu gewährleisten. Angesichts der zunehmenden Abhängigkeit der Patientenversorgung von einer störungsfrei funktionierenden IT-Infrastruktur muss folglich auch der IT-Sicherheit ein hoher Stellenwert eingeräumt werden. Zum Schutz Kritischer Infrastrukturen ist die Risikoanalyse der Krankenhaus-IT unablässig. Im Blick stehen Handlungsfelder, die für die Gewährleistung angemessener IT-Sicherheit besonders wichtig sind.

Ein Blick auf ausgewählte relevante Themengebiete soll als Anreiz dienen, den Umsetzungsstand der Einrichtung zu überprüfen, und zugleich aufzeigen, welchen Beitrag die IT-Risikoanalyse zur Absicherung der IT-Infrastruktur eines Krankenhauses leisten kann.

Sind die Prozesse Ihrer Einrichtung und deren IT-Abhängigkeiten bekannt?

Eine regelmäßig aktualisierte Prozessübersicht (z. B. als „Prozesslandkarte“) erleichtert es nicht nur, Effektivität und Effizienz der Abläufe eines Krankenhauses zu verbessern, sondern auch die kritischen Prozesse und IT-Abhängigkeiten zu erkennen. Sie ist damit eine wichtige Grundlage für die IT-Risikoanalyse. Hierfür sollte die Übersicht angemessen detailliert die Krankenhausprozesse, deren Zusammenwirken und deren IT-Unterstützung beschreiben.

Verfügen die IT-Zuständigen Ihrer Einrichtung über einen umfassenden Überblick über die IT-Infrastruktur und deren Komponenten?

Ein aktuelles und vollständiges Inventar der IT-Infrastruktur hilft bei der Ermittlung derjenigen IT-Komponenten, die für das korrekte Funktionieren der kritischen IT-Anwendungen unverzichtbar sind. Es erleichtert darüber hinaus die Entwicklung von Sicherheitskonzepten zum Schutz dieser Anwendungen. Das

Inventar sollte sämtliche eingesetzten IT-Systeme (Server, Clients usw.) und alle für deren Betrieb wichtigen Angaben enthalten, beispielsweise Einsatzzweck, Softwareausstattung sowie die Art der Netzanbindung.

Sind die für Ihre Einrichtung unverzichtbaren (kritischen) Bestandteile der IT-Infrastruktur bekannt? Die Kenntnis der unverzichtbaren IT-Anwendungen und IT-Komponenten ist eine Grundvoraussetzung für den Schutz vor IT-Ausfällen, welche die Handlungsfähigkeit Ihrer Einrichtung gefährden, und unterstützt die Auswahl angemessener Sicherheitsmaßnahmen. Die IT-Risikoanalyse ist ein Instrument, um die bestehenden Kenntnisse durch ein strukturiertes Vorgehen systematisch und möglichst vollständig zu erweitern.

Gibt es in Ihrer Einrichtung eine ausgewiesene Zuständigkeit für IT-Sicherheit?

Für die organisatorische Verankerung der IT-Sicherheit in Ihrer Einrichtung ist es hilfreich, wenn in Person eines IT-Sicherheitsbeauftragten eine zentrale Zuständigkeit für die Koordination der zugehörigen Aufgaben festgelegt wird. Ein IT-Sicherheitsbeauftragter ist der Krankenhausleitung berichtspflichtig und sollte eng mit allen Stellen zusammenarbeiten, die mit Sicherheitsfragen der Einrichtung befasst sind. Ihm obliegt es vor allem, die Entwicklung von Sicherheitskon-

zepten zu steuern und die Umsetzung der darin vorgesehenen Maßnahmen zu kontrollieren.

Werden in Ihrer Einrichtung ausreichende finanzielle und personelle Ressourcen für den IT-Betrieb und dessen Absicherung bereitgestellt?

Informationstechnik trägt auf vielfältige Weise zur Leistungsfähigkeit des Krankenhauses bei. Gerade dadurch ist sie aber auch zu einer kritischen Ressource für die Prozesse eines Krankenhauses geworden, deren Funktionsfähigkeit nur durch ausreichende Ressourcen für den IT-Betrieb und dessen Absicherung zuverlässig gewährleistet werden kann. Die IT-Risikoanalyse kann dazu beitragen, diejenigen Bestandteile der IT-Infrastruktur zu identifizieren, auf denen in dieser Hinsicht ein besonderes Augenmerk liegen sollte.

Sind die IT-Netze Ihrer Einrichtung hinreichend abgesichert?

Selbst der geplant durchgeführte Anschluss von Krankenhausnetzen an öffentliche Netze wie das Internet kann mit hohen Risiken verbunden sein und erfordert eine sorgfältige Absicherung z. B. durch ein zentrales Sicherheitsgateway, an dem der ein- und ausgehende Datenverkehr geprüft und bei Bedarf abgeblockt werden kann. Es ist aber auch sicherzustellen, dass zentrale Schutzmaßnahmen nicht durch unkontrollierte Netzzugänge, z. B. via WLAN oder mobile Datenverbindungen, ausgehebelt

werden können. Auch die ausreichende Absicherung öffentlich zugänglicher Netzanschlüsse, z. B. in Patientenzimmern, ist in einer Einrichtung mit Publikumsverkehr von wichtiger Bedeutung. Die IT-Risikoanalyse kann helfen, solche Segmente des Krankenhausnetzes zu identifizieren, die in besonderer Weise abzusichern sind, und Schwachstellen in den vorhandenen Schutzvorkehrungen zu erkennen.

Unterliegen die IT-Systeme Ihrer IT-Infrastruktur einem systematischen Update- und Patchmanagement?

Die IT-Zuständigen müssen nahezu täglich damit rechnen, dass neue Schwachstellen in der eingesetzten Betriebssystem- und Anwendungssoftware bekannt werden. Um zu verhindern, dass eine Schwachstelle für Angriffe auf das Krankenhausnetz ausgenutzt wird, müssen die für den IT-Betrieb zuständigen Mitarbeiter sich regelmäßig über solche Sicherheitslücken informieren und von den Herstellern bereitgestellte Patches und Updates zeitnah auf die betroffenen IT-Systeme aufspielen. Dies gilt speziell für die als kritisch identifizierten IT-Komponenten. Ein Konzept für diese Aufgabe muss auch geeignete Regelungen für die Behandlung medizinischer Spezialanwendungen vorsehen.

Sind die IT-Systeme und IT-Anwendungen Ihrer Einrichtung hinreichend gegen unberechtigte Zugriffe geschützt?

In Krankenhausnetzen werden hochgradig sensible Daten verarbeitet und kritische IT-Anwendungen betrieben. Dies erfordert starke Mechanismen zum Zugangs- und Zugriffsschutz. Vor allem bei den als kritisch identifizierten IT-Anwendungen und IT-Komponenten müssen unautorisierte Zugriffe verhindert werden. Dabei ist darauf zu achten, dass durch zu restriktive Regelungen zum Zugriffsschutz die Verfügbarkeit von

Daten und Anwendungen, die für die Patientenversorgung unverzichtbar sind, nicht gefährdet wird.

Sind die Mitarbeiter Ihrer Einrichtung für den sicheren Umgang mit kritischer Informationstechnik geschult?

Zur Vermeidung von IT-Sicherheitsvorfällen ist es erforderlich, dass die Benutzer hinreichend für Risiken bei der Anwendung von IT sensibilisiert und im sicheren Umgang mit dieser Technik geschult sind. Auch Administratoren und andere mit dem IT-Betrieb betraute Mitarbeiter müssen ausreichende Fortbildungsmöglichkeiten erhalten. Die IT-Risikoanalyse kann dazu beitragen, die Sensibilität für IT-Sicherheit in einem Krankenhaus zu erhöhen.

Liegen Notfallkonzepte für die kritischen IT-Anwendungen Ihrer Einrichtung vor?

Die IT-Risikoanalyse zeigt auf, welche IT-Anwendungen für die kritischen Prozesse eines Krankenhauses besonders wichtig sind. Trotz aller Sicherheitsmaßnahmen können IT-Ausfälle niemals völlig ausgeschlossen werden. Daher sind für alle kritischen IT-Anwendungen Notfallkonzepte zu entwickeln, in denen Ersatzmaßnahmen zur Überbrückung eines IT-Ausfalls und Maßnahmen für den Wiederanlauf der IT-Anwendungen beschrieben sind. Diese IT-Notfallkonzepte sind in ein Gesamtnotfallkonzept des Krankenhauses zu integrieren, in dem das Vorgehen bei Ausfällen weiterer kritischer Ressourcen beschrieben ist.

Beteiligt sich Ihre Einrichtung an Initiativen oder Kooperationen zur IT-Sicherheit?

Die vielfältigen Bedrohungen für die IT-Infrastruktur machen es nahezu unerlässlich, Erfahrungen im Umgang mit Risiken und zu Themen der IT-Sicherheit einrichtungs- und ggf. sogar branchenübergreifend auszu-

tauschen. Auf diese Weise können alle Teilnehmer des Austausches von dem kollektiven Wissen um Problemfelder und Lösungsansätze profitieren. Neben brancheninternen Kreisen bieten sich hierzu verschiedene staatliche Initiativen an, beispielsweise die Allianz für Cyber-Sicherheit (www.allianz-fuer-cybersicherheit.de). Diese bietet nicht nur die Möglichkeit zum Erfahrungsaustausch, sondern auch dokumentierte Empfehlungen zur Cyber-Sicherheit sowie Informationen zu aktuellen Gefährdungen im Rahmen der Risikokommunikation an.

Quelle: Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT
Herausgeber Bundesamt für Sicherheit in der Informationstechnik – BSI
www.bsi.bund.de

KRITIS-Sektor Gesundheit

Wegen ihrer besonderen Bedeutung für das Funktionieren des Gemeinwesens sind im Sektor Gesundheit kritische Dienstleistungen im Sinne des § 10 Absatz 1 Satz 1 des BSI-Gesetzes:

- Stationäre medizinische Versorgung
- Aufnahme
- Diagnose
- Therapie
- Unterbringung/Pflege
- Entlassung
- Versorgung mit unmittelbar lebenserhaltenden Medizinprodukten, die Verbrauchsgüter sind
- Herstellung
- Abgabe
- Versorgung mit verschreibungspflichtigen Arzneimitteln sowie Blut- und Plasmakonzentraten zur Anwendung im oder am menschlichen Körper
- Herstellung
- Vertrieb
- Abgabe
- Laboratoriumsdiagnostik
- Transport
- Analytik

Cyberfälle: Interne Fehler sind häufig die Auslöser

Eine Analyse von mehr als 1.700 Cyberversicherungs Schäden weltweit offenbart: Externe Ereignisse wie DDoS-Angriffe verursachen 85% der Schadenssummen, aber interne Vorfälle wie menschliches Versagen oder Systemausfälle sind bei weitem der häufigste Auslöser – wenn auch mit geringeren finanziellen Auswirkungen. Anstieg von Lösegeld-Angriffen sowie hohe Kosten infolge großer Datenlecks und Sicherheitslücken durch Arbeiten im Home-Office in der Covid-19-Pandemie stellen zukünftige Cyberrisiken dar. Auch der Healthcare-Sektor ist davon zunehmen betroffen.

Zwar führen externe Angriffe auf Unternehmen zu den teuersten Cyberversicherungsschäden. Fehler von Mitarbeitern und technische Probleme sind hingegen zahlenmäßig die häufigste Ursache für Schadenfälle in der Cyberversicherung. Zu diesem Ergebnis kommt der neue Bericht der Allianz Global Corporate & Specialty (AGCS): „Managing The Impact Of Increasing Interconnectivity – Trends In Cyber Risk“. Die Studie analysiert 1.736 cyberbezogene Versicherungsansprüche im Wert von 660 Millionen Euro (770 Millionen US-Dollar), an denen AGCS und andere Versicherer zwischen 2015 und 2020 beteiligt waren. „Schäden durch Distributed Denial of Service (DDoS) oder Phishing- und Ransomware-Angriffe machen heute einen Großteil des Schadenvolumens in der Cyberversicherung aus“, sagt Catharina Richter, globale Leiterin des Allianz Cyber Kompetenzzentrums. „Aber obwohl Cyberkriminalität die Schlagzeilen beherrscht, sind es vielfach alltägliche Systemausfälle und menschliche Fehler, die Unternehmen große Probleme bereiten, selbst wenn ihre finanziellen Auswirkungen meistens nicht so gravierend sind. Arbeitgeber und Arbeitnehmer müssen deshalb zusammenarbeiten, um das Bewusstsein für diese Gefahren zu

schärfen und die Cyber-Resilienz zu erhöhen.“

Die Zahl der Cyberversicherungsschäden, die AGCS gemeldet wurden, ist in den letzten Jahren stetig gestiegen: von 77 im Jahr 2016 auf 809 im Jahr 2019. Im Jahr 2020 wurden der AGCS in den ersten drei Quartalen bereits 770 Schäden gemeldet. Dieser stetige Anstieg der Schadensfälle ist zum Teil auf das Wachstum des globalen Cyberversicherungsmarktes zurückzuführen, der sich nach Schätzungen von Munich Re derzeit auf 7 Milliarden US-Dollar beläuft. AGCS startete 2013 mit dem Angebot von eigenständigen Cyberversicherungen und erwirtschaftete 2019 weltweit mehr als 100 Millionen EUR an Bruttoprämieeinnahmen in diesem Segment. Zugleich verweist die Studie darauf, dass in den letzten fünf Jahren die durchschnittlichen Folgekosten durch Cyberkriminalität für betroffene Organisationen um rund 70 % auf 13 Millionen US-Dollar gestiegen ist und Sicherheitsverletzungen um rund 60 % zugenommen haben (Quelle Accenture). Cyberschäden, die auf externe Vorfälle wie DDoS-Angriffe oder Phishing-/Malware- oder Ransomware-Kampagnen zurückzuführen sind, machen dem Bericht zufolge den Großteil der

Schadenssummen (85 %) aus, gefolgt von böswilligen internen Aktionen (9 %) – die zwar selten sind, aber kostspielig enden können.

Cyberrisiken nehmen weiter zu

Unbeabsichtigte interne Vorfälle, wie Mitarbeiterfehler bei der Erledigung der täglichen Aufgaben, IT- oder Plattformausschläge, Probleme bei der Migration von Systemen und Software oder Datenverluste verursachen mehr als die Hälfte der analysierten Cyberschadenfälle (54%) gemessen an der Zahl der Schadenmeldungen. Im Vergleich zur Cyberkriminalität – 43 % der registrierten Schadenfälle – sind ihre finanziellen Auswirkungen aber meistens begrenzt. Betriebsunterbrechungen sind der Hauptkostentreiber für Cyberschäden und machen etwa 60 % der Schadenssummen aus, an zweiter Stelle stehen Kosten für die Bewältigung von Datenpannen.

Das Umfeld für Cyberrisiken werde in Zukunft nicht einfacher werden, so die Studie. Unternehmen und Versicherer sehen sich einer Reihe von Herausforderungen gegenüber: Cyber-Betriebsunterbrechungen werden kostspieliger, Ransomware-Angriffe nehmen weiter

zu, Mega-Datenlecks haben schwerwiegende Folgen aufgrund der verschärften Regulierung und mehr Gerichtsprozessen; politische Differenzen werden zunehmend im Cyberspace ausgetragen.

Auch die enorme Zunahme von Arbeiten im Home-Office aufgrund der Coronavirus-Pandemie begünstigt Cyberangriffe und schafft neue Möglichkeiten für Cyberkriminelle, Zugang zu Netzwerken und sensiblen Informationen zu erhalten. Berichte zeigen, dass Malware- und Lösegeldangriffe seit Anfang 2020 um mehr als ein Drittel zugenommen haben – darunter sind auch Covid-19-bezogene Online-Betrügereien und Phishing-Kampagnen. Gleichzeitig könnten auch die potenziellen Auswirkungen von Mitarbeiterfehlern oder technischem Versagen durch die Arbeit im Home-Office verstärkt werden.

Raffinierte Ransomware-Angriffe

Während die Gefährdung zunimmt, kann die Coronavirus-Krise nicht als unmittelbarer Treiber für Cyberversicherungsfälle bestimmt werden. AGCS hat einige erste Cyberschadensfälle beobachtet, die indirekt auf die Pandemie zurückzuführen sind, wie beispielsweise Ransomware-Angriffe im Remote-Working-Umfeld. Allerdings lässt sich noch kein eindeutiger Trend bestätigen.

Ransomware-Schadsoftware ist weiter auf dem Vormarsch und führt zu steigenden Verlusten – die Angriffe gegen Unternehmen werden immer raffinierter, die Erpressungsforderungen für die Freigabe verschlüsselter Daten oder Systeme explodieren. Im vergangenen Jahr wurden weltweit fast eine halbe Million Cybererpressungen gemeldet. Allein die Bezahlung der Lösegeldforderungen soll mindestens 6,3 Milliarden US-Dollar gekostet haben, die Gesamtkosten für die Bewältigung dieser Vorfälle addieren sich auf mehr als 100 Milliarden US-Dollar.

„Durch die zunehmende Kommerzialisierung der Cyberkriminalität sind High-End-Hacking-Tools auf breiterer Basis verfügbar. Kriminelle Softwareentwickler ‚lizensieren‘ die von ihnen entwickelte Malware an andere Angreifer, die dann in geschützte Netzwerke eindringen und die Unternehmen erpressen“, sagen Cyberversicherungsexperten bei AGCS Zentral- und Osteuropa. Erpressungsforderungen seien jedoch nur ein Teil des Schadens. Die ganz oder teilweise Stilllegung des Betriebs verursache ebenfalls hohe Schäden – wobei die Ausfallzeiten immer länger werden – und auch die Kosten für die Wiederherstellung von Systemen und Daten könnten schnell in die Höhe schießen.

Datenschutzverletzungen und staatlich geförderte Angriffe

Die Kosten in Folge großer Datendiebstähle oder -pannen steigen mit der zunehmenden Komplexität von IT-Systemen sowie der Zunahme von Cloud- und Drittanbieterdiensten. Die Datenschutzbestimmungen, die vor kurzem in vielen Ländern verschärft wurden, sind ebenfalls ein Schlüsselfaktor, der die Kosten in die Höhe treibt, ebenso wie die wachsende Haftung gegenüber Dritten und die Aussicht auf Sammelklagen. Sogenannte Mega-Datenpannen (die mehr als eine Million kompromittierte Datensätze betreffen) verursachen aktuell Kosten von durchschnittlich 50 Millionen US-Dollar – eine Steigerung um 20% gegenüber 2019.

Auch die zunehmende Beteiligung von Nationalstaaten an Cyberangriffen gibt Anlass zur Sorge. Große Ereignisse wie landesweit stattfindende Wahlen und die Covid-19-Pandemie bieten gute Möglichkeiten für Angreifer. Laut Google mussten im Jahr 2020 pro Quartal über 11.000 staatlich gesponserte potenzielle Cyberangriffe blockiert werden.

Vorbereiten, üben und verhindern

Die Vorbereitung und regelmäßige Schulung von Mitarbeitern kann die Folgen von Cybervorfällen erheblich verringern, insbesondere bei Phishing und Business E-Mail Compromise. Bei Ransomware-Angriffen können sichere Daten-Backups den Schaden begrenzen. Bei der Sicherheit von Fernarbeit spielen Zugangs- und Authentifizierungsmanagement eine zentrale Rolle; zudem sollten Unternehmen über ausreichend Netzwerkkapazität verfügen, um bei einem Ausfall den Schaden begrenzen zu können.

Der branchenübergreifende Austausch und die Zusammenarbeit zwischen Unternehmen ist ebenfalls von entscheidender Bedeutung, um der in hohem Maße kommerziell organisierten Cyberkriminalität die Stirn zu bieten, gemeinsame Sicherheitsstandards zu entwickeln und die Cyber-Widerstandsfähigkeit zu verbessern.



Catharina Richter, globale Leiterin des Allianz Cyber Kompetenzzentrums: „Vielfach sind es alltägliche Systemausfälle und menschliche Fehler, die Unternehmen große Probleme bereiten, selbst wenn ihre finanziellen Auswirkungen meistens nicht so gravierend sind.“

Digitalisierung und Disruption als Nagelprobe für das IT-Management

Die Digitalisierung in der Gesundheitswirtschaft schreitet unaufhaltsam voran. Nicht zuletzt durch Gesetzesinitiativen, wie insbesondere das Krankenhauszukunftsgesetz (KHZG), steigt der Druck auf die Krankenhäuser und die IT, die digitale Transformation zügig zu vollziehen. Die Kernfrage dabei ist, ob die Krankenhaus-IT dafür richtig aufgestellt ist. Welche Voraussetzungen für und durch das IT-Management gegeben sein müssen, beschreibt Dr. Uwe Günther, Partner Curacon GmbH Wirtschaftsprüfungsgesellschaft und Geschäftsführer Sanovis GmbH, in diesem Beitrag.

Digitalisierung als Treiber nachhaltiger Veränderungen in der Krankenhaus-IT

Die digitale Transformation des Gesundheitswesens, speziell in den Krankenhäusern, nimmt schon seit geraumer Zeit eine vorherrschende Stellung ein. Nicht zuletzt durch das Inkrafttreten des Krankenhauszukunftsgesetzes (KHZG) am 29. Oktober 2020 ist diese Entwicklung noch weiter forciert worden. Im Fokus der Digitalisierungsvorgaben des KHZG stehen alle wesentlichen Bereiche der Krankenhausbabläufe, von der Aufnahme über die Behandlungsprozesse in der Klinik mit entsprechendem Behandlungs- und Dokumentationsmanagement bis hin zu Medikationsmanagement, virtuellen Sprechstunden und Entlassung. Weitere diesbezügliche Gesetzgebungen stehen mit dem Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz (DVPMG) bereits unmittelbar vor der Tür.

Allerdings nicht nur die neuen gesetzlichen Regelungen, sondern vor allem auch die rasant steigenden Anforderungen seitens der Anwender und nicht zuletzt seitens der Geschäftsführungen in den Krankenhäusern erhöhen den Druck auf die IT und vor allem auf das IT-Management, die Digitalisierung zeitnah und schnell umzusetzen.

Dementsprechend verschiebt sich für die Informationstechnologie in der Gesundheitswirtschaft zunehmend der Fokus. Haben sich IT-Abteilungen bisher darauf konzentriert, als verlässlicher „IT-Lieferant“ für ihre Fachbereiche und Anwender aufzutreten, müssen sich diese nun zunehmend von diesem Gedanken lösen und ihre Funktion mehr als „Prozesslieferant“ verstehen. Insbesondere in Zeiten des digitalen Wandels ist eine prozessorientierte und kundenorientierte IT-Ausrichtung zum besseren Verständnis der Anwender, zum Knüpfen einer engeren Bande mit ihnen und zur größeren Zufriedenheit derer essentiell.

Neben den klassischen IT-Aufgaben wie die Planung, die Entwicklung und den Betrieb von medizinischen und administrativen IT-Systemen besteht zunehmend die Notwendigkeit,

proaktiv und frühzeitig mit der Unternehmensleitung und den Fachbereichen zu kooperieren, um disruptive Innovationen gemeinsam zu konzipieren und zu realisieren. Dabei ist die IT mit neuen Technologien, der Notwendigkeit einer verstärkten Geschäftsorientierung, der Forderung nach schnellerer „Time-to-Market“ sowie der kundenorientierten und iterativen Entwicklung von IT-Lösungen konfrontiert.

Dringender Handlungsbedarf im IT-Management

Jedoch fehlt es in der Regel genau an diesem Geschäfts- und Prozesswissen, welches zwischenzeitlich von der IT erwartet wird. Insbesondere aufgrund der primär technologischen Ausrichtung sind viele IT-Organisationen im Hinblick auf vor allem klinische Prozesse nicht optimal aufgestellt.

Verstärkt wird die Situation der deutschen Krankenhaus-IT durch eine oftmals noch zu verbessernde Verantwortungsübernahme und Führungsqualität. Gepaart mit immer wieder auftretenden Kommunikations- und Priorisierungsproblemen, führt dies zu einer mangelnden Akzeptanz der IT-Leitung in der eigenen Organisation sowie durch die Geschäftsführung.

Deshalb ist eine Neuausrichtung vieler IT-Abteilungen Grundvoraussetzung, um sich so den Anwendern und Prozessen nähern zu können. Die IT-Verantwortlichen sind gefordert, sich den Herausforderungen der Digitalisierung zu stellen und dahingehend die IT anforderungs- und zukunftsgerichtet aufzustellen. Nur dadurch kann das IT-Management perspektivisch die eigene Position sichern.

Vor diesem Hintergrund ergeben sich drei wesentliche Ansatzpunkte für die handelnden IT-Akteure, um die erforderlichen Voraussetzungen für die Neuausrichtung der IT zu schaffen:

1. Organisatorische Voraussetzung: Bimodale IT als ideale Organisationsform für die digitalisierte Gesundheitsmarkt-IT.

2. Kommunikative Voraussetzung: „Integrative“ IT-Steuerung zur Einbeziehung der Geschäftsführung und der Anwender in den IT-Prozess.

3. Personelle Voraussetzung: Erweiterte Kompetenz des IT-Managements zur Sicherung der Zukunftsfähigkeit.

Bimodale IT als ideale Organisationsform für die digitalisierte Gesundheitsmarkt-IT

Als mögliche Maßnahme zur Begegnung der Herausforderungen der Weiterentwicklung der IT und als Antwort auf den Ruf nach mehr Agilität und Geschwindigkeit werden agile Organisationsformen derzeit intensiv diskutiert. Gleichzeitig sind die Anforderungen an einen sicheren und stabilen Betrieb von traditionellen IT-Lösungen unverändert. Demzufolge bedarf es einer innovativen Organisationsform für die IT, die traditionelle und agile Ansätze gleichermaßen vereint.

Eine solche Organisationsform ist die bimodale IT. Sie bezeichnet die Zweiteilung einer IT in das Management von sicheren und in ihrem Verhalten vor-

hersagbaren Kernsystemen (vgl. Abbildung 1, graue Darstellung) auf der einen sowie von experimentellen, agilen und Anwendern sowie Partnern zugewandten Applikationen (vgl. Abbildung 1, rote Darstellung) auf der anderen Seite.

Die grundlegende Idee dieses organisatorischen Ansatzes ist, neben der traditionellen IT-Entwicklungs- und -Betriebsorganisation als großer Tanker (Modus 1) eine Art Schnellboot für digitale Transformationsprojekte mit hoher Priorität und hohem Geschwindigkeitsanspruch zu schaffen (Modus 2). Für den Tanker geht es dann vor allem darum, die Kernsysteme (z. B. das Krankenhausinformationssystem) anhand klar definierter Anforderungen und dem Paradigma „Stabilität und Zuverlässigkeit“ folgend weiterzuentwickeln. Das Schnellboot fokussiert sich hingegen auf „disruptive“ IT-Lösungen (z. B. Apps, Portallösungen, Künstliche Intelligenz) und ist entsprechend durch anwender-beziehungsweise geschäftsgetriebene digitale Transformationsprojekte geprägt.

Das IT-Management muss die IT-Organisation dahingehend entwickeln, um beiden Modi gerecht zu werden. Dies beinhaltet neben den strukturellen Veränderungen insbesondere auch den Ausbau und die fachliche Weiterentwicklung – im Sinne eines Wissens- und

Talentaufbaus – des IT-Personals sowie des Leistungsgeschehens im Hinblick auf die benötigte Geschäfts- und Prozessorientierung. Zudem besteht der Konsens, dass moderne IT-Personalführungsansätze für die Mitarbeiterzufriedenheit und den Erfolg der IT-Organisation immer wichtiger werden.

„Integrative“ IT-Steuerung zur Einbeziehung der Geschäftsführung und der Anwender in den IT-Prozess

Die optimale Einbindung der IT in das Krankenhaus ist heute unternehmenskritischer denn je. Dennoch hat man oftmals noch den Eindruck, dass dies bei Weitem noch nicht erfolgt ist. Den einzigen Ausweg aus dieser Misere bietet ein integrativer IT-Managementansatz, bei dem die Kunden der IT, also Geschäftsführung, die Fachabteilungen und die Endanwender, mit in den IT-Prozess einbezogen werden (vgl. Abbildung 2).

Das IT-Management – aber auch die Geschäftsleitung und die Fachabteilungen – müssen sich innovativen und strategisch weiterreichenden Kommunikationsmethoden stellen, um die qualitative und wirtschaftliche Leistungserbringung sowie die prioritätenorientierte Steuerung einer modernen Krankenhaus-IT zu gewährleisten. Aus einem Nebeneinander von IT-Bereich und Kunden (vgl. Abbildung 2, abgekapselte IT im blauen Rahmen) muss ein partnerschaftliches Miteinander werden (vgl. Abbildung 2, integrierte IT im roten Rahmen), welches die möglichst effektive Allokation der IT-Ressourcen gewährleistet. Nur so kann die IT den neuen Herausforderungen gerecht werden und dadurch ein bedarfsgerechtes und modernes Informationsmanagement gewährleisten, welches nachweislich zur Erreichung der strategischen Unternehmensziele im Krankenhaus beiträgt.

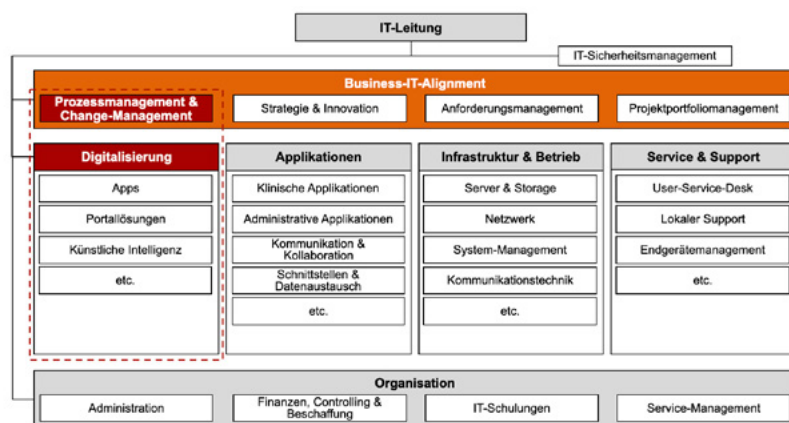


Abbildung 1: Modell einer bimodalen IT für Krankenhäuser (eigene Darstellung)

In der Operationalisierung erfolgt die integrative IT-Steuerung oftmals auf operativer Ebene im Rahmen von IT-Jour Fixes zwischen IT-Leitung und Geschäftsführung sowie auf strategischer Ebene in Gestalt von Gremien, wie z. B. IT-Boards oder IT-Lenkungskreise, bei denen neben der IT-Leitung und der Geschäftsführung auch Vertreter der Anwender (z. B. Ärzte, Pflege und Verwaltung) teilnehmen.

Erweiterte Kompetenz des IT-Managements zur Sicherung der Zukunftsfähigkeit

Weg vom EDV-Leiter, hin zum IT-Manager und strategischen Partner: Das ist die Maxime für die IT-Verantwortlichen, um die Zukunftsfähigkeit der Organisation und auch der eigenen Position zu sichern. Man muss den Anforderungen eines Chief Innovation Officers und des Chief Digital Officers gerecht werden, um nicht eines Tages in der Bedeutungslosigkeit zu verschwinden.

Das bedeutet für das IT-Management, Fähigkeiten in «Digital Leadership» auszubilden. Man muss bereit sein, sich etwas von der Technik zu lösen und sich mehr auf die Geschäftsprozesse zu konzentrieren. Neben technischem Grundverständnis müssen Digital Leader auch über soziale Intelligenz, Kreativität und Innovationskraft sowie Problemlösungskompetenzen verfügen. Nicht nur die praktische Umsetzung der Technologien, sondern auch die Adressierung der mit der digitalen Transformation verbundenen geschäftlichen, organisatorischen, kulturellen und personellen Anforderungen ist hier entscheidend.

Das Ziel der Digital Leadership ist es, in einem sich immer schneller verändernden Marktumfeld mit ungewissen Rahmenbedingungen das eigene Krankenhaus flexibler, schneller und auch innovativer zu machen. Die Digitalisierungslösungen sollen helfen, neue Geschäftsabläufe und -modelle zu schaffen und die damit verbundenen Mehrwerte zu eröffnen. Dabei dürfen IT-Verantwortliche die Technolo-

gietrends sowie das Lieferanten- und Cloud-Management nicht vergessen. Übergreifend müssen die Digitalisierungslösungen in eine ganzheitliche Enterprise-Architektur eingebettet sein, die einen nahtlosen Informationsaustausch und die Zusammenarbeit aller Systeme des Krankenhauses ermöglicht. Schließlich muss auch noch der Wertbeitrag der IT gegenüber der Geschäftsführung nachgewiesen werden, und zwar nicht nur durch Budget- und Kostendisziplin, sondern auch in Form von z. B. Effizienz- oder Umsatzsteigerung für die Organisation. Dies kann z. B. in Form einer projekt- oder lösungsbezogenen Balanced Scorecard (BSC) erfolgen, im Rahmen derer zwischen dem IT-Management und der Geschäftsführung abgestimmte und festgelegte Leistungskennzahlen bzw. Key-Performance-Indicators (KPIs) ermittelt und dargestellt werden. Die klassischerweise vier Dimensionen der BSC, in denen die KPIs thematisch gruppiert werden, können dann die «Investitions- und Betriebskosten», die «Performance und Verfügbarkeit», die «Auslastung und Nutzungsintensität» sowie als eigentliche Wertbeitragsdimension die «Senkung der Prozesskosten oder die durch die Lösung erzielten Zusatz Erlöse» sein.

Fazit und Ausblick

Die allgegenwärtige Digitalisierung in der Gesundheitswirtschaft bietet viele Chancen für die Krankenhäuser und die

verantwortlichen Akteure dort. Eigentlich hätte der Informationstechnologie nichts Besseres passieren können als das rasante Voranschreiten der digitalen Transformation, bringt es doch eine signifikante Verbesserung ihrer Wertigkeit und Rolle mit sich. Um diese auch zu nutzen, ist das IT-Management gehalten, die dafür entscheidenden organisatorischen, kommunikativen und persönlichen Voraussetzungen zu schaffen. Der besondere Fokus liegt dabei auf der Digital Leadership. Nur wenn die IT-Manager diese digitale Kompetenz im Sinne einer erweiterten Verantwortlichkeit anbieten, ist Zukunftsfähigkeit der Krankenhäuser und auch der eigenen Stellung gesichert.

www.curacon.de
www.sanovis.com



Dr. Uwe Günther, Partner Curacon GmbH Wirtschaftsprüfungsgesellschaft sowie Geschäftsführer Sanovis GmbH: „Geeignete organisatorische und kommunikative Strukturen sowie die persönliche Kompetenz des IT-Managements sind entscheidend.“

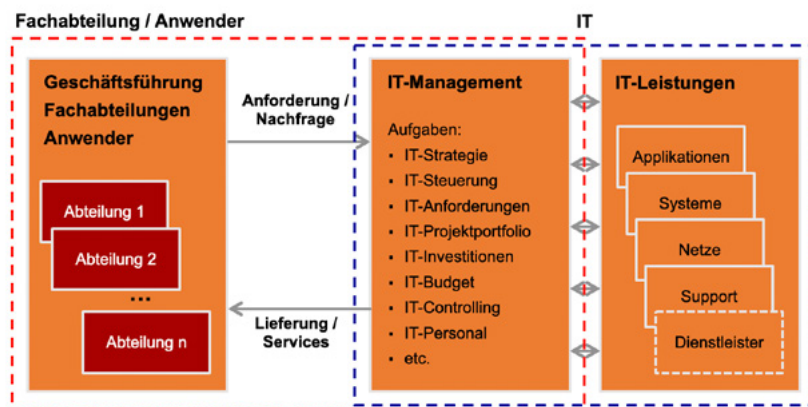


Abbildung 2: „Integrative“ IT-Steuerung (eigene Darstellung)

IT-Kooperation Charité/Vivantes: Digitaler Austausch von Behandlungsdokumenten als Teil der eHealth-Strategie

Patientendokumente und -daten, die ohne zeitraubenden Verwaltungsaufwand rechtssicher, vollständig und strukturiert zur Verfügung stehen, verbessern die Patientenversorgung und steigern zugleich die Effizienz in allen Prozessen. Für die IT-Kooperation von Charité und Vivantes stand daher der lückenlose digitale Austausch von Behandlungsinformationen von Anfang an ganz oben auf der Anforderungsliste. Von Marcus Beck, Gunther Nolte, Martin Peuker, Nina Sodogé



Gunther Nolte, CIO, Ressort IT und Digitalisierung der Vivantes Netzwerk für Gesundheit GmbH,
Kontakt: gunther.nolte@vivantes.de

Zu Beginn des Jahres wurde in einem gemeinsamen Projekt die erste Stufe zur Etablierung der digitalen Plattform erfolgreich umgesetzt. Nachdem der organisationsübergreifende Dokumentenaustausch reibungslos läuft, steht zurzeit die Realisierung der Stufe 2 „Austausch und Mehrfachnutzung strukturierter, granularer Daten“ an.

Eine notwendige Voraussetzung für den organisationsübergreifenden Datenaustausch ist Interoperabilität. Ohne das schnittstellenfreie Zusammenspiel unterschiedlichster IT-Systeme gibt es keine digitale Bereitstellung und weitere Nutzung von Daten. In beiden Klinikkonzernen Charité Universitätsmedizin Berlin und Vivantes Netzwerk für Gesundheit GmbH wurden daher Interoperabilitäts-Plattformen (IOP-Plattformen) in die IT-Architektur der Klinik Anwendungen integriert und an die medizinischen Primärsysteme angebunden. Für den Dokumentenaustausch wurde eine dezentrale Speicherung der Behandlungsinformationen gewählt. Die Patientendaten verbleiben somit in den Primärsystemen der Kliniken und werden nur bei Bedarf und bei Vorliegen einer Einwilligung durch die Patient:innen abgerufen.



Martin Peuker, CIO, Geschäftsbereich IT der Charité – Universitätsmedizin Berlin, Kontakt: martin.peuker@charite.de



**Marcus Beck, Senior Berater
bei eHealth.Business,**
Kontakt: marcus.beck@ehealthbusiness.de

IHE-konformes Einwilligungsmanagement Auf Grundlage von relevanten IHE-Profilen und Kommunikationsstandards (HL7 & HL7-FHIR) erfolgt der Datenaustausch erst nach erteilter Einwilligung der Patient:innen in beiden Kliniken. Die Einwilligungen werden im Krankenhausinformationssystem erfasst und anschließend an das Archivsystem übergeben. Im Archivsystem erfolgt dann die Generierung des Einwilligungsdokumentes (Consent) entsprechend des IHE-Profiles „B/APPC“ (Basic/Advanced Patient Privacy Consents), in dem die individuellen Einwilligungsinformationen der Patient:innen gespeichert werden. Das generierte Einwilligungsdokument wird anschließend dem IHE-Archiv übergeben und ermöglicht unter Nutzung von Security Token Services (STS) so die Steuerung der Zugriffsrechte des digitalen Informationsaustausches. Die in den Primärsystemen der Kliniken abgelegten Dokumente werden standardisiert nach IHE freigegeben, bei Bedarf über die IOP-Plattformen abgerufen und in die Behandlung einbezogen – voll digital, schnell und sicher.

Digitaler Austausch von Behandlungsinformationen Im Mai 2021 wurde die neue Lösung zum digitalen Austausch von Behandlungsdokumenten im Rahmen der IT-Kooperation von Charité und Vivantes, nach nur 18 Monaten, unternehmensweit in Betrieb genommen. In dieser ersten laufenden Phase ist der digitale Austausch des Arztbriefes, des bundeseinheitlichen Medikationsplanes, des Rettungssellenscheines, des Laborbefundes sowie des Mikrobiologiebefundes im PDF-Format über die neuen IOP-Plattformen möglich. In Zusammenarbeit mit den medizinischen Fachbereichen von Charité und Vivantes wird das auszutauschende Dokumentenset sukzessive erweitert.

Ergänzend zu den Dokumenten wird in einem aktuell weiteren laufenden Projekt der digitale Austausch strukturierter Behandlungsdaten über eine FHIR CDR Komponente umgesetzt. Strukturierte Daten werden semantisch angeglichen zwischen den Kliniken ausgetauscht, sodass sie im Anschluss sofort zur Weiterbehandlung des Patienten genutzt werden können. Realisiert wird dies über das Modul FHIR-CDR, ein Clinical Data Repository, in dem strukturierte, granulare Patientendaten gespeichert werden. Die semantische Normierung der Daten erfolgt über den Terminologieserver, die Steuerung der Zugriffsrechte wird über die CDR-Fassade umgesetzt. Strukturierte Daten, wie Laborparameter, Vitalwerte, ICD-10-Diagnosen- sowie OPS-Prozedurencodes, sollen auf diese Weise ab Frühjahr 2022 zwischen den Kliniken getauscht und direkt weiterverwendet werden – ein echter Quantensprung in Richtung mehr Behandlungsqualität.

Zukunftsfähigkeit der Umsetzung

Die IT-Kooperation von Charité und Vivantes hat mit dem „digitalen

Austausch von Behandlungsdokumenten“ einen Grundstein für die digitale Vernetzung zur Optimierung der Versorgung und Forschung der Kliniken in der Gesundheitsstadt Berlin 2030 gelegt. Mit der Umsetzung der IOP-CDR-Suite folgt aktuell die Vernetzung zum Austausch diskreter Daten. Auf Basis dieser Plattformtechnologien und der übergeordneten technischen Sicherheits- und Berechtigungsstruktur wird die medizinische Versorgung in beiden Kliniken deutlich verbessert. Die Liegezeiten der Patienten werden bei steigender medizinischer Qualität kürzer, die Datenlage für Diagnosen und Therapien aller Erkrankungen besser. Durch die Verfügbarkeit diskreter Gesundheitsdaten kommen zukünftig auch künstliche Intelligenz und innovative Technologien wirksam zum Einsatz. Dabei werden die Erkenntnisse der Medizin-Informatik-Initiative und des Forschungsnetzwerkes der Universitätsmedizin zu COVID-19 (NUM) sowie die Anforderungen der Telematik-Infrastruktur berücksichtigt.



**Nina Sodogé, Beraterin bei
eHealth.Business GmbH,**
nina.sodoge@ehealthbusiness.de

ISiK: Standards für Schnittstellen in Krankenhäusern

Die gematik wurde vom Gesetzgeber beauftragt, Standards für Schnittstellen in Krankenhäusern zu definieren und die Umsetzung durch ein Bestätigungsverfahren zu prüfen. Krankenhäuser sind verpflichtet, seit 30.06.2021 mit einer Übergangsfrist von 24 Monaten nur noch von der gematik bestätigte Informationstechnische Systeme im Krankenhaus (ISiK) einzusetzen.

Bisher ist die IT-Systemlandschaft in deutschen Krankenhäusern oftmals so heterogen, dass der schnelle Datenaustausch be- oder sogar verhindert wird – und somit wichtige Informationen für die Behandlung der Patientinnen und Patienten nicht dort landen, wo und in welcher Form sie benötigt werden: Die Systeme können nicht miteinander „reden“. Aktuell werden in Krankenhäusern die unterschiedlichsten IT-Systeme verwendet, oft als Insellösungen, die nicht mit anderen Systemen kompatibel sind. Die Realität ist also noch weit von der notwendigen Interoperabilität entfernt. Das soll sich ändern. Ab dem 30.06.2021 unterstützen Vorgaben der gematik den Interoperabilitätsgedanken. Die gemeinsame digitale Sprache für den Datenaustausch innerhalb und zwischen Krankenhäusern ist ein wichtiger, zentraler Teil der Telematikinfrastruktur.

Die gematik wurde vom Gesetzgeber beauftragt, Standards für Schnittstellen in Krankenhäusern zu definieren und die Umsetzung durch ein Bestätigungsverfahren zu prüfen. Krankenhäuser sind verpflichtet, ab dem 30.06.2021 mit einer Übergangsfrist von 24 Monaten nur noch von der gematik bestätigte Informationstechnische Systeme im Krankenhaus (ISiK) einzusetzen. Das Verfahren zur Bestätigung des interoperablen Datenaustauschs der gematik ist gemäß § 373 SGB V verpflichtend für Softwareprodukte, die als zentrale primäre Informationssysteme im Krankenhaus genutzt werden und die üblicherweise Krankenhausinformationssystem (KIS) oder klinisches Arbeitsplatzsystem (KAS) genannt werden.

Mit den einheitlichen Standards auf Basis von HL7 FHIR wird nicht nur der Datenaustausch innerhalb von Krankenhäusern erleichtert, auch Sektorengrenzen können damit künftig überwunden werden. Im Fokus der Spezifikation stehen Praxis-tauglichkeit und Akzeptanz der Nutzer: Für die erfolgreiche Erarbeitung der Festlegungen des Bestätigungsverfahrens war es zwingend erforderlich, die Probleme und Bedürfnisse der Krankenhäuser zu verstehen und gemeinsam zu erarbeiten, wie ISiK Erleichterungen bewirken können. Daher wurden die Festlegungen gemeinsam mit Stakeholdern der gematik transparent erarbeitet und sind öffentlich einsehbar⁽¹⁾

Interoperabler Datenaustausch

Die gematik wurde vom Gesetzgeber beauftragt, im Benehmen mit der Deutschen Krankenhausgesellschaft (DKG) und den maßgeblichen Bundesverbänden der Industrie im Gesundheitswesen, verbindliche Standards für den Austausch von Gesundheitsdaten mit Informationssystemen im Krankenhaus zu erarbeiten. Dieser FHIR ImplementationGuide (IG) beschreibt die für diesen Zweck entwickelten FHIR Profile und das REST-basierte Application Programming Interface (API). Die REST-API wird im Wesentlichen vom FHIR Standard vorgegeben. Dieser Leitfaden konkretisiert die ISiK-relevanten Funktionen der Standard-REST-API und trifft inhaltliche Festlegungen zu den ISiK-relevanten Ressourcen in Form von Ressourcen-Profilen.

Hersteller bestätigungsrelevanter Systeme sollen durch diesen IG in die Lage versetzt werden, eine konforme Implementierung zu erstellen und das Bestätigungsverfahren der gematik erfolgreich zu absolvieren. Weitere Informationen siehe §373 SGB V.

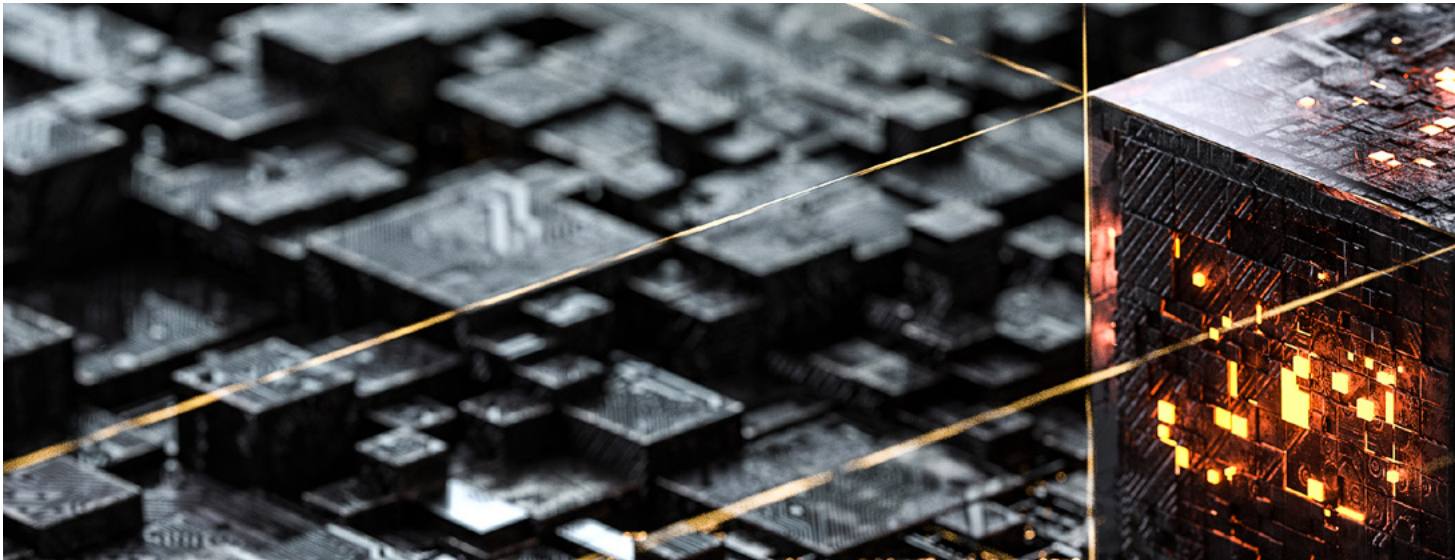
Es sei darauf hingewiesen, dass sowohl für die Implementierung der ISiK-Spezifikation, als auch für den Betrieb eines Produktes das die ISiK-Spezifikation implementiert eine SNOMED-CT-Lizenz notwendig ist. Diese kann durch das beim National Release Center für SNOMED CT in Deutschland beantragt werden.

Showcases mit sieben Krankenhäusern

In sogenannten Showcases mit sieben Krankenhäusern in ganz Deutschland wird aktuell gezeigt wie ISiK im klinischen Arbeitsalltag tatsächlich verwendet werden. Diese Krankenhäuser sind Teil des ISiK Showcase:

- Gemeinschaftskrankenhaus Havelhöhe gGmbH
- Klinikum rechts der Isar der Technischen Universität München (AöR)
- Klinikum der Stadt Ludwigshafen am Rhein gemeinnützige GmbH
- Klinikum Ingolstadt
- Universitätsklinikum Essen (AöR)
- BG Klinikum Unfallkrankenhaus Berlin gGmbH
- Zollernalb Klinikum gGmbH

(1) <https://simplifier.net/guide/ImplementierungsleitfadenISiK-Basismodul/Einfuehrung>



KH-IT: Fels in der Brandung und im Wandel

Genau zwei Jahre ist es nun schon her, dass sich die Community der Krankenhaus-IT-Leiterinnen und -leiter zuletzt im gewohnten Rahmen bei der Herbsttagung in Erlangen getroffen hat. In Heidelberg, in Konstanz, in Berlin wollten wir uns danach treffen, nun veranstalten wir stattdessen bereits die dritte Onlinetagung. Schöne neue Welt? Sicher, man spart sich eine Menge an Reisezeit und Reisekosten, man kann sich sogar während der Tagung noch für andere, vermeintlich wichtigere Dinge mitunter kurz ausklinken, Multitasking sozusagen.

So ist es inzwischen auch im Alltag des IT-Managers geworden: Man schaltet sich von einer Videokonferenz zur nächsten, manchmal beginnt man gar parallel zwischen zweien hin und her zu springen, weil die Terminkoordination nicht so ganz gepasst hat, weil jemand schnell man eine Konferenz angesetzt und die passenden Menschen dazu eingeladen hat und ein anderer dasselbe für denselben Zeitraum auch getan hat. So läuft gefühlt immer mehr in derselben Zeit, die Digitalisierung schreitet auch hier mit Riesenschritten voran.

Durch das Krankenhauszukunftsgesetz (KHZG) ist nun endlich viel mehr Geld für die Krankenhaus-IT im Spiel, zumindest in einem ersten Wurf, das was wir doch immer wollten und wonach wir IT-Verantwortliche geschrien haben.

Endlich wird die IT-Welt auch per Gesetz immer sicherer, die Sicherheitsgesetze für Kritische Infrastrukturen werden ständig erweitert und verfeinert, auch das eigentlich ein Kernanliegen unter anderem der Krankenhaus-IT schon seit langer Zeit. Schließlich scheint es, dass die Telematikinfrastruktur endlich zu einem Ziel kommt, Formen annimmt, nachdem doch sage und schreibe bereits im Jahre 2005 die erste Tagung des KH-IT zu diesem Thema stattgefunden hatte.

Das sind eigentlich alles gute Nachrichten. Vieles, was wir jahrelang höchstens ansatzweise zu träumen wagten, wird nun vielleicht nach und nach Realität.

Nur woher kommt dann das Störgefühl dabei? Ist es wirklich immer nur die Politik, die zwar an den Themen herumdoktert, es aber nie recht machen kann? Muss die Hoffnung auf Bundestagswahlen und einer neuen Regierung liegen, mit der dann alles wirklich (noch) besser wird? Oder ist es vielleicht gerade während oder am Ende, oder wer weiß es schon, dieser Pandemie nicht ein guter Zeitpunkt, einmal innezuhalten und zu reflektieren, warum es uns mit dem Aktionismus anders aber trotzdem nicht besser geht?

Versuchen wir es und fangen wieder ganz oben damit an.

Der KH-IT hat es geschafft, sich auf die neuen Rahmenbedingungen einzustellen. Onlinetagungen und Webinare statt Reisen durch Deutschland und Seminare heißt das Gebot der Stunde. Das war für uns nicht einfach, das hat eine Menge an Aufwand, Hirnschmalz, Zeit und Geld gekostet, sich aber sicher gelohnt. Schon zum dritten Mal in Folge können wir



im September eine hochwertige Tagung mit hervorragenden Fachvorträgen und der Möglichkeit zum Austausch über Chat, Breakout-Rooms, virtuellen Ausstellerständen und –foren anbieten. Das kann sich sehen lassen. Trotzdem wirft es Fragen auf. Ist es wirklich dasselbe wie die Tagungen bis 2019, bei denen wir uns physisch getroffen haben und nicht eine im Hintergrund laufende minutiöse Regie den Veranstaltungsablauf bestimmte, man sich zwangslos zwischen den Sessions und bei der Abendveranstaltung unterhalten konnte? Dabei ist unsere Tagung immerhin wirklich live und nicht aus der Konserve. Aber dasselbe ist es eben trotzdem nicht. Wir sind schließlich Menschen und jeder Besucher eines Kommunikationsseminars weiß, dass über 80 Prozent der zwischenmenschlichen Kommunikation nonverbal abläuft.

Wie wird es in Zukunft werden? Kehren wir ganz zurück zum Format der Jahre 1996-2019 oder wird es eine hybride Angelegenheit werden, welche die Vorteile der Onlinetagung versucht aufzunehmen, ohne die Nachteile mitzunehmen? Noch kann es niemand genau sagen.

Und die anderen angesprochenen Themen? Sicher alles schöne Entwicklungen, welche die IT und damit die Digitalisierung im Krankenhaus voranbringen. Nur muss auch der Faktor Mensch mitspielen. Alle diese Segnungen für die Anwender müssen letztlich erst einmal umgesetzt werden. Das ist viel Arbeit, das geht nicht von heute auf morgen und auch nicht auf übermorgen, und die Mitarbeitenden dafür müssen erst einmal da sein. Diese müssen nicht nur da sein, sondern auch orchestriert werden, jemand muss immer noch den Überblick bewahren, was im Zuge all dieser Maßnahmen immer schwieriger wird. Vor allem sollte hier ein Satz aufhören lassen, der nach den Vorträgen der letzten KH-IT-Tagung abends in einem Breakout-Room zu hören war: „Vor lauter Videokonferenzen komme ich ja nicht einmal mehr dazu, die notwendigsten Bedürfnisse wie Essen und was sonst noch dazu gehört zu berücksichtigen, 10 Stunden Arbeitstag und 12 Videokonferenzen“.

Die Menschheit kommt durch Krisen und Innovationen unbestritten langfristig voran. Aber der Mensch muss den Ent-

wicklungen auch folgen können, was in moderner Zeit immer schwieriger wird, weil die Verdichtung an Kommunikation, Projekten, und Aufgaben mit der Digitalisierung exponentiell zunimmt.

Eine große Herausforderung für die Krankenhaus-IT und speziell auch für unseren Verband wird in den nächsten Monaten und Jahren sein, bei allen inhaltlichen Themen, darauf zu achten, dass die Kolleginnen und Kollegen nicht auf der Strecke bleiben. Errungenschaften der Verbandsarbeit wie eine automatisch in der Mitgliedschaft eingeschlossene berufliche Rechtsschutzversicherung oder ein einmal im Monat am Mittwochabend stattfindender Austausch im sogenannten Clubabend sind Bausteine für eine solche Strategie. Auch letztere sind virtuell, sicher, aber der Fels in der Brandung muss ein wenig auch mit der Strömung des Wassers gehen, sich anpassen aber dabei standhaft bleiben.

In diesem Sinne wünsche ich Ihnen und uns alles Gute, bleiben Sie gesund, und hoffe auf ein baldiges Wiedersehen „in echt“, einmal wieder wie früher auf einer Tagung irgendwo in Deutschland, uns mit einem herzlichen Handschlag begrüßend.



Horst-Dieter Beha, Vorsitzender Bundesverband der Krankenhaus IT-Leiterinnen/Leiter KH-IT

KH-IT-Herbsttagung 2021:

Abschied von Compliance as-we-know-it

Wohin geht die Compliance-Reise hin bei IT, KHZG und TI 2.0 im Krankenhaus? Antworten und Lösungen vermittelten Experten den 233 Teilnehmern auf der virtuellen KH-IT-Herbsttagung am 22. und 23.9.2021. Auf der Agenda standen praktische Impulse aus der Praxis und Perspektiven zur Umsetzung bei intersektoralen Versorgungsketten, Messenger-Standard oder auch dem Investitionsprogramm KHZG und rechtskonformen Vergabe. Das gemeinsame Signal für IT-Verantwortliche lautet: Abschied von Compliance as-we-know-it.

Krankenhäuser haben mannigfaltige Anforderungen aus regulatorischen und rechtlichen Vorgaben zu befolgen. Einfach ist das kaum. Daher intonierten die beiden Programmgestalter der KH-IT-Herbsttagung Prof. Martin Staemmler und Thorsten Schütz zum Tagungsaufakt: „Compliance ist vielfältig und bedarf einer sorgfältigen Zuordnung von Verantwortlichkeiten, die nicht ausschließlich bei der IT liegen muss. Sie ist jedoch häufig von der IT zu unterstützen, sei es in der Bereitstellung von Tools, Anwendungen und Verfahren oder in der konkreten Umsetzung von Interaktion, Vernetzung und Datenaustausch.“ Regelkonformes Verhalten der Mitarbeiter ist ebenso unerlässlich wie Gesetze und Regeln grundsätzlich einzuhalten. Die Implementierung eines Compliance-Systems kann Haftungsrisiken oder Reputationsverlust verhindern. Präventive Maßnahmen dienen dazu, mögliches Fehlverhalten zu vermeiden und gegebenenfalls zu sanktionieren.

Kooperation Vivantes und Charité

Die Klinikbetreiber Vivantes und Charité sehen große Chancen in der engeren Zusammenarbeit. Sie wollen einen wesentlichen Beitrag zur Verbesserung der Versorgungsqualität leisten und Berlin als „Gesundheitsstadt 2030“ weiterentwickeln. Gemeinsam wollen beide Partner unter anderem die Umsetzung medizinischer Forschungsergebnisse in

die breite Versorgung (Translation) entscheidend voranbringen.

Die Vivantes E-Health Strategie verfolgt einen nachhaltigen, langfristig orientierten und weitreichenden Ansatz, um die Qualität der Versorgungsleistungen weiter zu steigern und dadurch die wirtschaftliche Leistungsfähigkeit des Unternehmens zu erhalten. Im Zentrum der digitalen Transformation bei Vivantes steht die qualitative und ökonomische Verbesserung von Behandlungsprozessen für die Patientinnen und Patienten.

„Digital unterstützte intersektorale Versorgungsketten – innovativ, funktional, sicher, vertrauenswürdig und compliant“, so sieht es Martin Peuker, Leitung Geschäftsbereich IT, Charité – Universitätsmedizin Berlin. „Wenn es in Berlin klappt, dann auch in anderen Regionen“, kommentierte der CIO. Das Einwilligungsmanagement-Projekt „TOR“ ist ein solcher „Treffer“. „TOR – Technisch – Organisatorisch – Rechtlich“ lautet die Formel in der IT-Kooperation von Charité und Vivantes. Beim Umgang mit personenbezogenen Gesundheitsdaten ist es notwendig, die rechtlichen Anforderungen an eine Einwilligung der betroffenen Personen auch technisch passgenau umzusetzen. Die Einwilligungsquote der Patienten zur Zusammenarbeit liegt bei 95%. Zertifizierungen unterstützen die Compliance.

Zu den Erfolgsfaktoren der IT-Kooperation von Charité und Vivantes zählte Martin Peuker auf:

Gemeinsame Zieldefinition, klare Projektstrukturen anhand der TOR-Methodik (Technik, Organisation, Recht) und der Einbezug aller relevanten klinikinternen Akteure aus Medizin, IT, Verwaltung und Datenschutz ebenso wie ein frühzeitiger Einbezug des Landesdatenschutz. Hinzu kommen eine regelmäßige Abstimmung zwischen den Kliniken und Industriepartnern mit Unterstützung externer Berater, Berücksichtigung bereits bestehender Prozesse bei der organisatorischen Umsetzung in den Kliniken sowie die Bereitstellung von Schulungs- und Informationsmaterial für die Mitarbeiter aus Medizin, Verwaltung und IT.

Anforderungen an Messenger-Dienste

Im Gesundheitswesen spielt das Konzept der schriftlichen „Sofort“-Kommunikation eine immer wichtigere Rolle. Voraussetzungen und Anforderungen waren Schwerpunkte der Herbsttagung. Aufgrund der im privaten Bereich weitverbreiteten und etablierten Nutzung wird auf diese Messenger-Dienste zunehmend auch im Gesundheitsbereich zurückgegriffen, häufig verbunden mit der Nutzung eines privaten Endgeräts.

Helmut Eiermann, stellv. Landesbeauftragter für den Datenschutz, Rheinland-Pfalz, betonte, Datenschützer

argumentieren heftig gegen Facebook-Sprössling und Marktführer Whatsapp. Sie führen Sicherheitsbedenken besonders bei der Vertraulichkeit der Information im beruflichen Bereich ins Feld. Metadaten und Verbindungsdaten (u.a. Telefonnummern) sind offen, Cloud-Backups unverschlüsselt. Im „Positionspapier der Datenschutzkonferenz“ lassen sich technische Anforderungen an Messenger-Dienste im Krankenhausbereich ablesen. Dazu gehören: Für die bei dem Dienstleister im Rahmen der Messenger-Lösung gespeicherten Daten ist eine regelmäßige Löschung sicherzustellen. Personenbezogene Patientendaten müssen auf den Servern des Krankenhauses oder dessen Auftragsverarbeitern verarbeitet werden.

Ein reiner Messenger ist zu wenig

Kommunikation nutzt bislang den konventionellen Datenaustausch sondern setzt künftig auf Messenger Dienste. Julia Opstals und Till Berger, beide bei Allm EMEA, fokussieren auf den Mehrwert von Messenger-Anforderungen und -Voraussetzungen. „Ein Messenger für das Gesundheitswesen muss mehr bieten als Chatten“. Die meisten klinischen Messenger am Markt beschränken sich auf herkömmliche, gängige Funktionen: Chatten und die Möglichkeit, Bilder oder Videos zu teilen, evtl. Sprach- und Videotelefonie. Unterschiedliche Fachrichtungen in einer Klinik benötigen jedoch unterschiedliche, umfangreiche Funktionen.

Die bestmögliche Patientenversorgung kann nur umgesetzt werden, wenn medizinische Fachkräfte immer die qualitativ hochwertige Informationen und Bilder zur Hand haben, die sie für Entscheidungen und Behandlungen brauchen. Ein Messenger ist eine Kommunikationslösung, die in die Krankenhaus-IT integriert werden kann (PACS, KIS, LIS etc.) und neben der gesamten Bandbreite kommunikativer Möglichkeiten – Chatten, File-Sharing, Sprach- und Videotelefonie – auch dediziert medizinische Funktionen bietet: DICOM-Viewer,

TimeStamps, Fall-Listen und die mobile, strukturierte Erfassung Daten. Behandlungszeiten lassen sich erheblich kürzen.

Interoperables Instant-Messaging

Die Messenger-Definition der gematik mit offenen Standards will es allen Recht machen: „TI-Messenger - der neue Standard für sicheres, interoperables Instant-Messaging im Gesundheitswesen

Eric Grey, Produktmanager gematik GmbH Berlin, proklamierte „TI-Messenger - der neue Standard für sicheres, interoperables Instant-Messaging im Gesundheitswesen“. Dabei gibt es besonders zwei Hürden: Sicherheit und Interoperabilität der bisherigen Angebote. Die gematik will einen neuen Standard mit dem „sicheren, interoperablen und leistungsfähigen Tool“ TI-Messenger zusammen mit Nutzern und Industriepartnern anstoßen. Anbieter sollen miteinander verknüpft werden können. Der Telematikinfrastruktur-Messenger soll den Informationsaustausch zwischen Praxen, Kliniken und Apotheken ermöglichen. Zu diesem Zweck sind diese Punkte spezifiziert: Zugang zum TI-Messenger für alle Mitarbeitenden einer Organisation im Gesundheitswesen mit SMC-B-Karte, Austausch von Textnachrichten, Bild- und Tonübertragung in Zweier- und Gruppenchats sowie zentraler Verzeichnisdienst mit der Möglichkeit zur anbieter- und sektorenübergreifenden Suche von Institutionen und Personen.

Der Anwender hat die freie Wahl bei Anbietern bei der nicht mehr Konnektor gebunden, sondern flexiblen Welt TI 2.0, angekündigt für das zweite Quartal 2022. Kritik dazu: Die Realität holt die Entwicklung ein, da Regelungen zu lange dauern.

Zwei Jahres-Schritt für Stand der Technik

Rüdiger Gruetz, ISB Klinikum Wolfsburg, Stellvertretender Leiter BAK, erörterte Entwicklungen B3S und SGB 75c. Im September 2020 wurde der neue § 75c in das Sozialgesetzbuch 5 (SGB V)

aufgenommen. Damit sind auch Krankenhäuser, die bisher nicht die Regelungen zum Schutz kritischer Infrastrukturen (KRITIS) nach § 8a BSI-Gesetz anwenden müssen, ab dem 1. Januar 2022 gemäß § 75c Abs. 1 SGB V verpflichtet, „nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind“. Die IT-Systeme sind gemäß dieser Regelung spätestens alle zwei Jahre dem aktuellen Stand der Technik anzupassen.

Diese neue Verpflichtung können die Krankenhäuser gemäß § 75c Abs. 2 SGB V insbesondere dadurch umsetzen, dass sie einen branchenspezifischen Sicherheitsstandard (B3S) für die informationstechnische Sicherheit der Gesundheitsversorgung im Krankenhaus in der jeweils gültigen Fassung anwenden. Hierbei ist nach aktuellem Stand der B3S für die Krankenhäuser die Mindestanforderung. Alternativ können gleichwertige Managementsysteme für Informationssicherheit (ISMS) zur Erfüllung der Nachweispflicht verwendet werden.

Reifegradradar – Digitalisierungsgrad im Fokus

Das Thema Krankenhauszukunftsgesetz KHZG weist vielfältige "Compliance"-Vorgaben auf. Im Beitrag „Reifegradradar - Herausforderungen und Möglichkeiten“ zeigte Prof. Dr. Sylvia Thun, Direktorin für eHealth und Interoperabilität, Berlin Institute of Health at Charité (BIH) auf, wie für das KHZG die Reifegradmessung aufgebaut ist und welche Rolle die "Muss"-Vorgaben der einzelnen Fördertatbestände spielen. Input zum „Radar“ kommt aus Literatur, von Experten, KHZG, KITCON & EMRAM. Das Ziel des Digitalradars ist die Evaluierung des Reifegrades der

Krankenhäuser hinsichtlich der Digitalisierung nach § 14b KHG. Das Reifegradmodell ermöglicht eine standardisierte und umfassende Bewertung des Digitalisierungsgrads von Krankenhäusern mittels Durchführung und Auswertung von Erhebungen bzw. Selbsteinschätzung der Krankenhäuser. Da die datenschutzrechtliche Compliance im KHZG für digitale Projekte ausdrücklich als Förderungsbedingung vorgesehen ist, muss auch der Förderungsantrag der Krankenhäuser eine entsprechende Erklärung enthalten. Effekte der Förderung in Bezug auf den Digitalisierungsgrad und der Verbesserung der Versorgung von Patienten bzw. regionaler Versorgungsstrukturen sind zu untersuchen und zu bewerten.

TI 2.0: Architektur im Plattformprinzip

Das KHZG-Investitionsprogramm setzt auf eine veränderte Infrastruktur für digitalen Austausch im Gesundheitswesen. „TI 2.0 – Möglichkeiten für Krankenhäuser“ erörterte Claus-Georg Becker, IT-Architekt, gematik GmbH, Berlin. Mit TI 2.0 signalisiert die gematik auch durch eine moderne Sicherheitsarchitektur einen grundlegenden Wandel für die nächsten Jahre. In der „gemeinsamen Arena für alle Akteure“ stellt die gematik komplexe, klare Grundbedingungen im zeitlichen Horizont bis 2025 auf. Die neue TI-Architektur mit Plattformprinzip steht auf Säulen wie:

Einem föderierten Identitätsmanagement, weil mit dieser „Brücke“ mehr Flexibilität und Nutzerfreundlichkeit durch die einfache Nutzung von Identitätsbestätigungen der TI für eigene digitale Angebote der Nutzergruppen möglich ist.

Der universellen Erreichbarkeit der Dienste durch Zugangsschnittstellen im Internet, weil der Wegfall proprietärer IT-Lösungen (z. B. Konnektor) Kosten senkt, den Betrieb stabilisiert und die Integration weiterer medizinischer Berufsgruppen erleichtert.

Interoperabilität und strukturierten Daten, weil die anwendungsfallbezogene Versorgung und Forschung eine Verbesserung der Datenqualität erfordert. Standardbasierte strukturierte Daten und Schnittstellen erhöhen die Verfügbarkeit bei Produkten und Services.

KHZG: rechtskonforme Vergabe im Klartext

Krankenhäuser, die Fördermittel aus der KHZG-Finanzierung einsetzen, müssen das Vergaberecht beachten. Übergeordnet steht die rechtskonforme Ausschreibung und Vergabe von Aufträgen zum KHZG an. Werner Bachmann, Rechtsanwalt, Friedrich Graf von Westphalen & Partner mbH, gab zu „KHZG: rechtskonforme Vergabe“ praktische Hinweise zum geeigneten Vorgehen und wies auf mögliche Fehler hin. Kernpunkte markieren eine korrekte Umsetzung und die Vermeidung von nachträglichen Einsprüchen der Marktteilnehmer oder Fördermittelgeber.

Länderverfahren sind nicht einheitlich, obwohl das Haushaltsrecht gilt, KHZG-MUSS Kriterien sind maßgeblich, auch beim Patienten-Portal, die Malus-Regelung in 2024 ist unklar. Vorabkennzeichnung gelten nur für Fristen, nicht für die Auswahl von Produkten. Vorabkennzeichnung bei Ausschreibungen sind sinnvoll auszugestalten, sie gelten nur für Fristen, nicht für Auswahl. Bei der Vergabe von Aufträgen sind die Vorgaben des nationalen und europäischen Vergaberechts durchgehend zu berücksichtigen. Es gelten hierbei die sonst üblichen sowie landesspezifischen Regelungen. Verstößt ein Krankenhaus gegen das Vergaberecht, so liegt ein Auflagenverstoß vor, der den Fördermittelgeber gemäß § 49 Abs. 3 S. 1 Nr. 2 VwVgG zum Widerruf der Bewilligung und gemäß § 49a Abs. 3, 4 VwVgG zur Rückforderung von Fördermittel verpflichtet. Die zurückgeforderte Summe muss darüber hinaus mit 5 Prozentpunkten über dem Basiszinssatz verzinst werden (§ 49a Abs. 3 VwVgG).

Die Entscheidung, ob ein sogenannter schwerwiegender Verstoß gegen das Vergaberecht vorliegt, steht im Ermessen des Fördermittelgebers. Dies gilt für alle Fördermittelnehmer, auch kommunale Krankenhäuser.

Konvergenz, Compliance und Synergien

Keine Konvergenz ohne Compliance. Das lassen Ergebnisse der jüngsten KH-IT Umfrage zur Verschmelzung von Medizintechnik und IT-Abteilungen erkennen. Das Zusammenwachsen von Funktionen und Institutionen in Krankenhäusern, insbesondere die Konvergenz von IT mit anderen, IT-bestimmten Abteilungen, ist eine anhaltende Entwicklung. Ihr Spannungsbogen reicht von Synergien bis zur Abgrenzung von Aufgaben mit der einhergehenden klaren Trennung von Funktionen und Institutionen. Einblicke gibt die Umfrage „IT konvergiert - Umfrageergebnisse zur Verschmelzung IT-lastiger Krankenhausabteilungen“. Kernpunkte stellte Dipl.-Ing. Ulrich Wieland, Medizinprodukte-Sicherheits- und Strahlenschutzbeauftragter, DRK-Klinikservicegesellschaft Sachsen mbH, und Mitglied des KH-IT-Vorstandes, vor. „Interessant ist, dass der Veränderungswunsch nie von anderen Abteilungen ausgeht und die IT-Abteilungen in der Regel die führenden Bereiche bei gemeinsamen Strukturen sind.“ Zunehmend stärkere Digitalisierung der techniklastigen Bereiche im Krankenhaus erfordert bessere Kooperation mit der IT. Daher sollten IT-Abteilungen die Zusammenarbeit – ob strukturell oder informell – fördern und unterstützen, und dabei auch nach Möglichkeiten suchen, wie diese institutionalisiert werden kann. Ulrich Wieland: "Wenn sich die IT an die Spitze der Bewegung stellt, können Synergieeffekte genutzt und Reibungsverluste minimiert werden."

Viel Arbeit – heute und morgen

Krankenhäuser und Kliniken befinden sich mit Blick auf Betriebs- und Geschäftsrisiken in einer herausfordernden Situation. Die Fragen, auf die Compliance-Verantwortliche Antworten finden müssen, sind vielfältig, die möglichen Schadensszenarien teilweise bedrohlich. Eine allgemeingültige Interpretation von Integritäts- und Compliance-Management existiert im Klinikbereich nicht. Das Verhältnis zu Industrie bleibt ein Spannungsfeld. Das Krankenhaus versteht sich als Anbieter für innovative Spitzenmedizin. Dies erfordert eine enge Zusammenarbeit mit der Industrie, um den Patienten den neuesten und besten Standard zu gewährleisten. Einerseits ist die Industrie bei der Entwicklung neuer Produkte auf das Wissen der Klinik-Experten angewiesen. Auf der anderen Seite darf die Zusammenarbeit mit der Industrie keinen Einfluss auf die Entscheidungen der Häuser haben. Wegen dieser Besonderheit von Compliance im Krankenhaus ist die Zusammenarbeit stark reglementiert.

Die Themen bei dieser zweitägigen Veranstaltung im Herbst 2021 zeigten Entwicklungen, um die IT und damit die Digitalisierung im Krankenhaus voranzubringen. Im Spannungsfeld der Krankenhauspraxis zeichnet sich ein Abschied von Compliance as-we-know-it ab. Horst-Dieter Beha, Vorsitzender Bundesverband der Krankenhaus IT-Leiterinnen/Leiter KH-IT, gab zu bedenken: „Das ist viel Arbeit, das geht nicht von heute auf morgen und auch nicht auf übermorgen, und die Mitarbeitenden dafür müssen erst einmal da sein. Diese müssen zudem auch orchestriert werden, jemand muss immer noch den Überblick bewahren, was im Zuge all dieser Maßnahmen immer schwieriger wird.“

KH-IT-Frühjahrstagung 2022

Die Frühjahrstagung des KH-IT Bundesverbandes der Krankenhaus IT-Leiterinnen/Leiter KH-IT findet am 30. und 31.3.2022 vor Ort in Heidelberg statt. Das Thema lautet „Prozess unterstützen – Medizingeräte, neue Geräte, Holodeck“. Gastgeber ist das Deutsche Krebsforschungszentrum Heidelberg. Agendaverantwortliche aus dem KH-IT sind Andreas Lockau, Dietmar Zelinski, Bastian Stockhausen und Ulrich Wieland (lockau@kh-it.de, tagung@kh-it.de). Die Organisation betreut Günter Gartner, KH-IT e.V. (gartner@kh-it.de).

Themen und Referenten

Compliance aus Sicht der IT-Sicherheit



Eröffnung und Begrüßung

Horst-Dieter Beha, Vorsitzender KH-IT e.V.

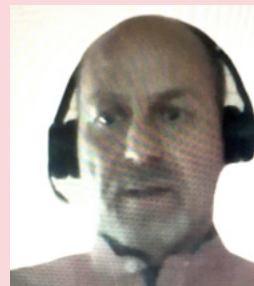
Einführung in das Tagungsthema



Digital unterstützte intersektorale Versorgungsketten – innovativ, funktional, sicher, vertrauenswürdig und compliant

Martin Peuker, Leitung Geschäftsbereich IT

Charité – Universitätsmedizin Berlin



Aktuelle Entwicklungen B3S und SGB 75c

Rüdiger Gruetz, ISB Klinikum Wolfsburg,

Stellvertretender Leiter BAK



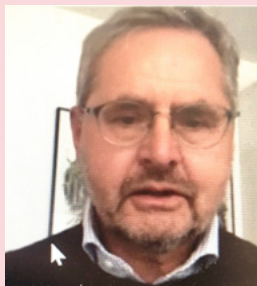
KRITIS, §8a BSIG ISO 27001 und BCM -

Bringen Sie sich in Sicherheit

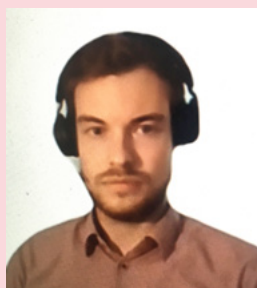
Britta Weber, IS-Beauftragte / QM Managerin, Dipl.-Inf. (FH),

Michael Heitmann, IT Leiter Agaplesion Diakonieklinikum

Rotenburg gGmbH



Anforderungen an Messenger-Dienste
Helmut Eiermann, stellv. Landesbeauftragter für den Datenschutz,
Rheinland-Pfalz



TI-Messenger - der neue Standard für sicheres, interoperables Instant-Messaging im Gesundheitswesen
Eric Grey, Produktmanager gematik GmbH Berlin



Ein Messenger für das Gesundheitswesen muss mehr bieten als Chatten
Julia Opstals, Till Berger, Head of Marketing & Communications, Allm EMEA GmbH, Erlangen

KH-IT News

IT konvergiert - Umfrageergebnisse zur Verschmelzung IT-lastiger Krankenhausabteilungen
Dipl.-Ing. Ulrich Wieland, Medizinprodukte-Sicherheits- und Strahlenschutzbeauftragter, DRK-Klinikservicegesellschaft Sachsen mbH

Dialog mit der Industrie

Begleitet wurde die Herbsttagung von Industriepartnern, die ihre Lösungen in Kurzbeiträgen und in virtuellen Ausstellungsräumen präsentierten und die Teilnehmer zur Diskussion einluden.

www.kh-it.de

Compliance zum KHZG und zur TI 2.0



Das Reifegradradar - Herausforderungen und Möglichkeiten
Prof. Dr. med. Sylvia Thun, Berlin Institute of Health an der Charité



KHZG: rechtskonforme Vergabe
Werner Bachmann, Rechtsanwalt,
Friedrich Graf von Westfalen & Partner mbH



TI 2.0 – Möglichkeiten für Krankenhäuser
Claus-Georg Becker, IT-Architekt, gematik GmbH, Berlin

KBV-Richtlinie SGB 5 §75b
Udo Karlins, KV Schleswig-Holstein, Bad Segeberg

KH-IT-Vorstandswahl 2021

Am Rande der virtuellen KH-IT-Herbsttagung vom 22. und 23. September 2021 wurde erstmals eine virtuelle Mitgliederversammlung durchgeführt. Als Haupt-Agendapunkt stand die Wahl des Vorstands auf der Tagesordnung. Da die Legislaturperiode des amtierenden Vorstands auch unter Corona-Bedingungen nun abgelaufen war und zwei Mitglieder des Vorstands aus persönlichen Gründen nicht mehr zur Verfügung standen, musste die Neuwahl durchgeführt werden.

Im Ergebnis wurden die Positionen wie folgt besetzt:

Vorsitzender: **Horst-Dieter Beha**

Stellvertreter: **Thorsten Schütz, Lars Forchheim**

Schatzmeister: **Andreas Lockau**

Schriftführer: **Klemens Behl**

Beisitzer für Presse- und Öffentlichkeitsarbeit, Soziale Medien: **Jürgen Flemming, Jens Schulze**

Neu wurden **Alexandra Heibel** und **Stephan Herz** als Beisitzer in den Vorstand gewählt.

Die Kassenprüfer wurden mit **Axel Maier, Maria Schedy** und **Dietmar Zelinski** wieder gewählt.

Stefan Smers und **Reimar Engelhardt** schieden aus dem Vorstand aus.

Die Profile der Vorstände finden Sie unter: www.kh-it.de/vorstand.html

Der Verband vertritt die Interessen der Krankenhaus-IT-Leiterinnen und Leiter. Er macht es sich zur Aufgabe, die Stellung der IT in der Klinik zu stärken im Sinne einer bestmöglichen und wirtschaftlichen Unterstützung der Patientenversorgung. IT-Verantwortliche können diesen wichtigen Beitrag nur gemeinsam gestalten. Der Bundesverband der Krankenhaus-IT-Leiterinnen/Leiter KH-IT wurde 2003 als eingetragener Verein gegründet.

www.kh-it.de

Leitung Bereich IT u. Digitalisierung (m/w/d)

Führungs- und Gestaltungsaufgabe im engsten Kreis der kfm. Leitung im Rhein-Neckar Gebiet

Unser Kunde ist ein städtisches Klinikum mit über 300 Betten in Südwest-Deutschland. Große Fachabteilungen decken das gesamte Spektrum der Versorgung bis in die Schwerpunktmedizin ab: Innere Medizin, Chirurgie, Gynäkologie/Geburtshilfe, Psychiatrie und Psychotherapie, Neurologie, Anästhesie und eine große Intensivstation sowie Belegabteilungen. Im Zuge einer geplanten Modernisierung sind über 40 Mio. € Investitionen allein für einen Neubauflügel vorgesehen.

Die gut strukturierte und langfristig orientierte Einrichtung befindet sich (abgesehen von den alle Kliniken betreffenden Einschränkungen der Pandemie) auf einem wirtschaftlichen Erfolgskurs und plant diesen durch neue dynamische Maßnahmen fortzusetzen. Hierzu gehört selbstverständlich die Umsetzung einer ehrgeizigen und auch investitionsintensiven IT und Digitalisierungsstrategie. Geboten wird eine umfang-

reiche und eigenverantwortliche Gestaltungsaufgabe. Die Dotierung ist attraktiv. Ausführliche Hintergrundinformationen können telefonisch erörtert werden. Wir sichern Ihnen unsere absolute Diskretion zu und freuen uns auf Ihre Fragen. Wenn Sie Interesse haben und mit uns unverbindlichen Kontakt suchen, würden wir gerne mit Ihnen über diese interessante Herausforderung oder andere Themen zu Ihrer beruflichen Entwicklung ins Gespräch kommen.

Herr Steffen Deutschenbauer steht Ihnen mit seinem Team für weitere Fragen telefonisch oder in einem ausführlichen Gespräch zur Verfügung. Health Care Leaders ist eine auf leitende Positionen im Gesundheitswesen spezialisierte Personalberatung. Gerne sprechen wir mit Ihnen über Ihre Karriere, interessante Weiterentwicklungsoptionen und das Thema „Führen im Gesundheitswesen“.

HCL Ref. Nr. 12510

HCL
HEALTH CARE LEADERS



**Steffen
Deutschenbauer**

HCL Health Care Leaders
Steffen Deutschenbauer
Hintere Schöne 14
87669 Rieden am Forggensee
www.healthcareleaders.de

Wir beantworten Ihre fachlichen Fragen per Email: deutschenbauer@healthcareleaders.de oder Tel.: +49 8362 925980

Patientenzentriertes Ökosystem – die Zukunft der Gesundheitsversorgung

Krankenhauszukunftsgesetz, COVID-19 und innovative Kollaborationen fördern den digitalen Durchbruch im Gesundheitssystem. Dabei steigt der Anpassungsdruck bei ambulanten und stationären Gesundheitsanbietern. Einen Paradigmenwechsel in der Versorgung bringt auch das veränderte Patientenverhalten. In der Studie „LSHC Predictions 2025“ prognostiziert Deloitte den jährlichen Rückgang stationärer Patientenzahlen: rund 1 Million weniger stationäre Fallzahlen bis 2025.

Homecare, selbstbestimmende Patienten, optimale Vernetzung der Versorgungskette und innovative Präventionsmöglichkeiten – was die Future of Health-Initiative von Deloitte noch für die Zeitspanne bis 2040 prognostizierte, lassen die COVID-19-Pandemie, neue Regulierungen und innovative Kooperationen schon heute zur Realität werden. Deloitte hat in der Studie „Life Sciences & Health Care Predictions 2025“ untersucht, inwiefern bereits jetzt Disruptionen im Gesundheitssystem zu verzeichnen sind und welche Chancen bzw. Risiken sich für die einzelnen Player ergeben.

Pandemie als Katalysator

Im Gesundheitswesen werden bis 2025 einschneidende Veränderungen zu beobachten sein: Bereits jetzt erweist sich die COVID-19-Pandemie als Treiber und Verstärker von Innovation und Digitalisierung. Traditionelle Grenzen werden durchlässiger und öffnen die Türen für neue Verhaltensweisen sowie Geschäfts- und Finanzierungsmodelle. Es lässt sich auch eine Reihe von Partnerschaften zwischen Regierungen, Aufsichtsbehörden, Gesundheitsdienstleistern, der Life-Science-Industrie, Technologie- und Gesundheitsunternehmen beobachten. Diese Kooperationen führen bereits heute zu einem Wissenstransfer über die gesamte Wertschöpfungskette hinweg und definieren Betriebsmodelle für ein effektiveres Gesundheitsökosystem neu.

„Die Corona-Pandemie hat die wachsende Lücke zwischen der Nachfrage nach Gesundheitsdienstleistungen auf der einen und dem Mangel an Fachpersonal und Ressourcen auf der anderen Seite noch einmal offengelegt“, beschreibt Ibo Teuber, Partner im Bereich Health Care bei Deloitte. „Ein wesentlicher Schlüssel, um diese Lücke zu schließen, ist eine breite Anwendung digitaler Technologien.“

Paradigmenwechsel in der Versorgung

Patienten sind die führende Innovationskraft im Gesundheitssystem. Ihre Bedürfnisse und Vorstellungen treiben Innovationen im Bereich von Leistungsangeboten, Produkten und Digitallösungen voran. Die COVID-19 Pandemie hat ihr Verständnis von „Well-being“ auf die Probe gestellt und den Wunsch bestärkt, die eigene Gesundheit aktiv zu gestalten. Prävention, Lifestyle und Früherkennung werden einen deutlich größeren Schwerpunkt einnehmen und zu einer entsprechenden Reallokation von Ressourcen und Verschiebung von Leistungsangeboten führen.

In der künftigen Versorgungswelt rückt der Patient in den Mittelpunkt: Diagnosen und Behandlungsentscheidungen werden von Kliniken und Behandlern auf einer prädiktiven, präventiven, personalisierten und partizipativen Medizin basieren. Dieser patientenzentrierte Ansatz verspricht



Ibo Teuber, Partner im Bereich Health Care bei Deloitte: „Ein wesentlicher Schlüssel, um diese Lücke zu schließen, ist eine breite Anwendung digitaler Technologien.“

viele Chancen: von Produktivitäts- und Kostensteigerungen bis hin zu einer effizienteren Bedarfsprognose, Bestandsverwaltung, Logistikoptimierung und Personalplanung. Ein zentraler Baustein in dieser Transformation wird die im Juli 2021 verpflichtend einzuführende elektronische Patientenakte sein.

„Ab diesem Jahr können Patienten mit der elektronischen Patientenakte ihre Daten mit ihrem Behandler selbstbestimmt teilen und eine digitale Informationsbasis schaffen“, ergänzt Ibo Teuber. „Eine weitere wichtige Entwicklung wird das Verschreiben von digitalen Gesundheitsapplikationen sein. Angebote für einen gesünderen Lebensstil, primäre und sekundäre Prävention sowie Früherkennung können direkt vom Behandelnden verschrieben und von den Krankenversicherungen vergütet werden. Vor allem die sektoren-, technologie- und fachbereichsübergreifende Interoperabilität aller Daten wird in Zukunft komplett neue medizinische Standards setzen.“ Für die Ausbreitung einer integrierten und vernetzten Versorgung werden das Internet of Medical Things (IoMT) sowie Technologien im KI-, Nano- und Quantencomputing-Bereich in Kombination mit 5G eine zentrale Rolle spielen.

Vom traditionellen Versorger zum innovativen Marktführer

Ein weiteres Zukunftsbild der Studie: Bis 2025 werden sich internationale Tech-Giganten im Gesundheitsmarkt weiter etablieren und mit ihrem digitalen Know-how einen direkten Zugang zu Patienten verschaffen. Ihr Ziel ist es, ein „nahtloses“ Patientenerlebnis mit radikal interoperablen Daten und offenen, aber sicheren Plattformen zu schaffen.

„Neue Player im Ökosystem werden die Grenzen im Gesundheitssektor zunehmend verschwimmen lassen. Vor allem Krankenhäuser müssen sich jetzt entscheiden, wo sie zukünftig stehen wollen“, betont Alexander Morton, Partner bei Deloitte. „Bereits 2019 hatten fast 29 Prozent der Kliniken in Deutschland einen Jahresverlust zu verzeichnen. Seit dem Ausbruch von COVID-19 sind

die Auslastungen in vielen Krankenhäusern deutlich zurückgegangen. Zwar hat der im Zuge der Pandemie aufgespannte Rettungsschirm den Strukturwandel zunächst aufgehalten, allerdings werden viele Krankenhäuser 2021 nicht das Erlösniveau von 2019 erreichen. Sie müssen sich und ihre Geschäftsmodelle neu erfinden, um weiterhin erfolgreich zu bestehen.“

Krankenhäuser in Zugzwang

Die Entstehung neuer Versorgungsmodelle sowie der Rückgang der klassischen stationären Versorgung setzt ambulante und stationäre Gesundheitsanbieter unter Druck: „Auf Basis unseres Future of Health-Prognosemodells gehen wir davon aus, dass in den kommenden Jahren von einem durchschnittlichen jährlichen Verlust von ca. einem Prozent der stationären Patientenzahlen ausgegangen werden muss. 2025 wäre so mit rund 19 Millionen stationären Fällen zu rechnen, das heißt einem Rückgang um fünf Prozent bzw. ca. 920.000 Fällen im Vergleich zu 2019“, resümiert Alexander Morton. „Der Rückgang des konventionellen stationären Leistungsgeschehens und der Investitionsdruck in neue Technologien, Strukturvorgaben und Fachkräfte stellen Krankenhäuser vor große Herausforderungen.“

Neue Finanzierungs- und Vergütungsmodelle pushen Transformation

Um fehlende Investitionsmöglichkeiten und Personalmangel im Gesundheitssektor zu kompensieren, werden viele Versorger in der Transformation auch von staatlichen finanziellen Mitteln abhängig sein. So schafft das Anfang des Jahres in Kraft getretene Krankenhauszukunftsgesetz neue Voraussetzungen im Gesundheitssektor: Die finanziellen Mittel von

Bund und Ländern ermöglichen Investitionen für moderne Notfallkapazitäten sowie Maßnahmen zur Digitalisierung und zur Verbesserung der IT-Sicherheit. Auch neue Vergütungssysteme werden laut Deloitte-Prognose im Jahr 2025 zur Verfügung stehen müssen, um digitale Gesundheitsangebote erfolgsabhängig abrechnen zu können. Vor allem daten-gesteuerte Finanzierungsmodelle treiben die Innovation im gesamten Gesundheitsökosystem voran. Diese werden flexibel und ergebnisorientiert gestaltet sein, um auch Telemedizin und digitale Therapiemöglichkeiten pro Patientennutzung vergüten zu können – eine wichtige Entwicklung für die Wertschöpfungskette im gesamten Ökosystem.



Alexander Morton, Partner bei Deloitte:
„Sie müssen sich und ihre Geschäftsmodelle neu erfinden, um weiterhin erfolgreich zu bestehen.“

Tech-Unternehmen und die digitale Zukunft der Medizin

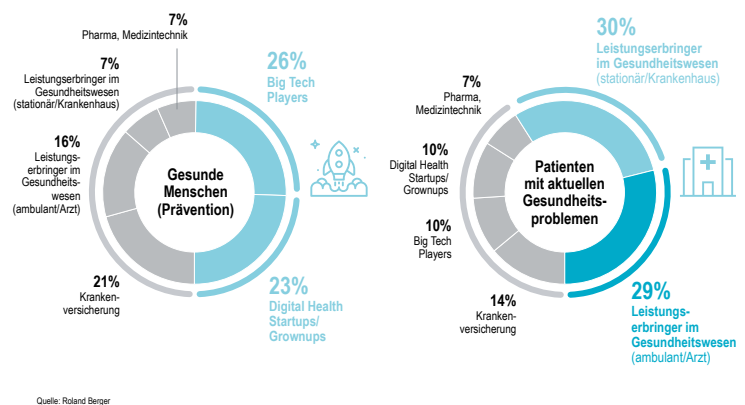
Das Potenzial im Gesundheitswesen haben die amerikanischen Big-Techs erkannt und drängen seit einigen Jahren verstärkt in den Markt. Mit dem Einsatz digitaler Technologien wie Künstliche Intelligenz (KI) verändern die Tech-Giganten zunehmend die Art von und den Umgang mit Therapien und Diagnostik. Die deutsche Gesundheitswirtschaft hinkt hier noch stark hinterher, denn ihr fehlen bislang digitalisierte, ganzheitliche Lösungen. Von Oliver Rong und Dr. Peter Magunia, beide Senior Partner bei Roland Berger. Im Fokus beider Berater stehen Leistungserbringer und MedTech-Unternehmen sowie die Themen Digitalisierung, Strategieentwicklung, Performance und Restrukturierung.

Die Gesundheitswirtschaft ist einer der größten deutschen Wirtschaftssektoren. Mit einem Wachstum von jährlich durchschnittlich 4,1 Prozent wuchs der Sektor in den vergangenen Jahren stärker als das Bruttoinlandsprodukt (BIP) und macht heute bereits mehr als 12 Prozent des BIP aus – Tendenz steigend. Neben einer qualitativ hochwertigen und umfassenden Gesundheitsversorgung zeichnet sich der deutsche Gesundheitsmarkt vor allem durch die Entwicklung innovativer High-tech-Produkte in der Medizintechnik und Arzneimittel sowie neuer Behandlungs- und Untersuchungsmethoden aus. Damit spielt der deutsche Gesundheitsmarkt auch als "Schaufenster" für die Gesundheitsindustrie – die ihre Produkte global anbietet – eine wichtige Rolle.

Das Potenzial im Gesundheitswesen haben auch die amerikanischen Big-Techs erkannt und drängen seit einigen Jahren verstärkt in den Markt. Bis 2025 wird das Marktvolumen in Europa für digitale Produkte und Dienstleistungen im Gesundheitswesen voraussichtlich bei ca. 155 Milliarden Euro liegen, davon rund 38 Milliarden Euro allein in Deutschland. (Quelle: Roland Berger Focus – Future of health, Oktober 2019).

Und die Tech-Unternehmen sind durch ihre traditionell stark datengetriebenen Geschäftsmodelle bestens für die Ansprache gesunder Menschen positioniert. Mit ihren Quasi-Monopolen bei Suchmaschinen, e-Commerce und Social Media haben sie die idealen Voraussetzungen geschaffen, um (fast unbemerkt) auch eine Vielzahl von Gesundheitsdaten zu sammeln und zu analysieren. Dementsprechend richtet sich ihr Angebot aktuell und im Sinne eines Einstiegs in den Gesundheitsmarkt vornehmlich auf die Krankheitsvermeidung (Prävention / Gesundheitserhaltung), im Gegensatz zu den etablierten Akteuren wie Krankenhäuser und Ärzte, die sich stark auf die Behandlung erkrankter Menschen fokussieren (s. Abbildung 1).

Wer ist der bevorzugte Partner für gesunde Menschen und Patienten?

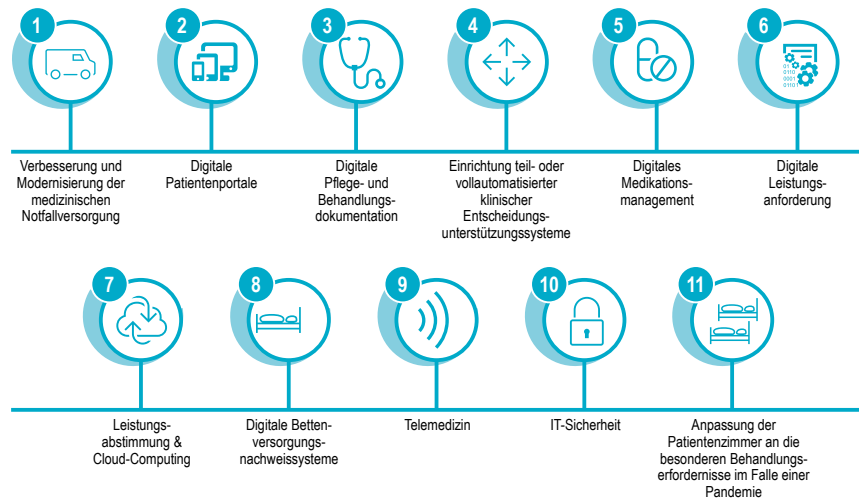


Aber, mit dem Einsatz digitaler Technologien wie Künstliche Intelligenz (KI) verändern die Tech-Giganten auch zunehmend die Art von und den Umgang mit Therapien und Diagnostik. Sie tragen so dazu bei, dass Krankheiten früher erkannt, bessere Therapien und passgenau Medikamente verordnet werden können, deren Einnahme zudem präzise nachverfolgt wird und damit der therapeutische Erfolg überhaupt erst erreicht werden kann. Mit ihren Technologien, Plattformen und Kooperationen bieten sie neue, innovative Produkte und Dienstleistungen an, die zu teilweise radikalen Veränderungen im Gesundheitswesen führen werden. Für die Kunden bzw. Patienten ist das grundsätzlich eine gute Nachricht, denn sie können mit vielen neuen Anwendungen rechnen, die ihr Leben erleichtern oder ihre Gesundheit verbessern. Die deutsche Gesundheitswirtschaft hinkt hier noch stark hinterher, denn ihr fehlen bislang digitalisierte, ganzheitliche Lösungen. Mehr zu den Entwicklungen und Auswirkungen des digitalen Wandels auf das deutsche Gesundheitswesen behandeln wir in unserer Studien-Serie „Future of health“, die seit 2019 jährlich erscheint.

Krankenhauszukunftsgesetz (KHZG) soll Digitalisierung in Krankenhäusern beschleunigen

Dabei wird eines deutlich: die digitale Transformation des Gesundheitsmarkts hat das Potenzial, für ein kostengünstigeres und effizienteres Gesundheitssystem zu sorgen. Denn mehr Wettbewerb durch neue Akteure führt auch zu einer höheren Kundenorientierung. Aber nicht nur das. Auch für eng mit der medizinischen Versorgung vernetzte Bereiche, wie den Einkauf, bietet die Nutzung digitaler Werkzeuge viele Vorteile. Sei es, um die Transparenz über das Verbrauchsverhalten und damit die Lieferantensteuerung abteilungsübergreifend zu ermöglichen oder, um Abläufe und Prozesse transparent zu machen und Schnittstellen zu optimieren. Allerdings kämpfen vor allem deutsche Krankenhäuser und Gesundheitseinrichtungen weiterhin mit einem stark regulierten Markt, strengen Datenschutzregelungen, veralteten, ineffizienten IT-Infrastrukturen und Ressourcenproblemen. Mit dem am 29. Oktober 2020 in Kraft getretenen Krankenhauszukunftsgesetz (KHZG) haben Krankenhäuser nun die Chance, bei der Digitalisierung einen großen Schritt nach vorne zu machen (s. Abbildung 2). Kernelemente des KHZG sind neben der IT-Sicherheit auch Patientenportale und eine durchgängige digitale Begleitung des Patienten im gesamten Behandlungsprozess zur Verbesserung der Patientenbindung. Ziel ist es, die Qualität der Versorgungsleistungen zu erhöhen, die Effizienz zu steigern sowie bessere Arbeitsbedingungen und eine höhere Akzeptanz bei den Mitarbeitern für digitale Lösungen zu schaffen. Insgesamt stehen bis zu 4,3 Milliarden Euro Fördervolumen vom Bund und den Ländern zur Verfügung. Und: Krankenhäusern, die bis Anfang 2025 keine digitalen Dienste anbieten können, drohen Erlöseinbußen. Die Abschläge können bis zu zwei Prozent der Patientenrechnungen ausmachen und beeinflussen damit erheblich die künftige wirtschaftliche Entwicklung der Krankenhäuser.

Übersicht über Fördertatbestände



Quelle: Bundesministerium für Gesundheit; Roland Berger

Die Regierung setzt damit neue Standards und will mit dem Gesetz, auf Basis einheitlicher Vorgaben, alle deutschen Krankenhäuser auf ein höheres Digitalisierungslevel heben.

Voraussetzungen für eine erfolgreiche Digitalwende: Prozessumbau, agile Arbeitsmethoden und die Einbindung der Mitarbeiter

Aber: die digitale Transformation ist vor allem in Krankenhäusern mit einer hohen Komplexität verbunden. Gewachsene Strukturen und Prozesse, starre Hierarchien, vielfältige IT-Insellösungen sowie die Ablehnung der Mitarbeiter führten bisher in vielen Fällen zu einem Scheitern von Digitalisierungsprojekten. Es gilt nun, all dies grundlegend zu hinterfragen und im Rahmen einer Gesamtstrategie neu auszurichten. Dabei sollten auch agile Arbeitsweisen oder neue Formen der Zusammenarbeit mit Partnern nicht außer Acht gelassen werden. Entscheidend für die erfolgreiche Umsetzung der digitalen Transformation wird allerdings die Gewinnung der Mitarbeiter und Führungskräfte sein. Alle Maßnahmen müssen einen direkten Mehrwert mit sich bringen und nachvollziehbar sein, um eine höhere Akzeptanz bei der Belegschaft zu erzielen. Durch ein frühzeitiges Einbinden und transparente Kommunikation können Ängste vor Veränderungen abgebaut und der dringend notwendige kulturelle Wandel nachhaltig vorangetrieben werden.



Oliver Rong ist Senior Partner bei Roland Berger in Hamburg. Seit rund 25 Jahren berät er Kunden im Gesundheitswesen.



Dr. Peter Magunia ist Senior Partner bei Roland Berger am Standort in Stuttgart. Mit seinem medizinischen Hintergrund begleitet er seit 15 Jahren Kunden aus der Gesundheitsbranche.

Fotos Credits: Roland Berger GmbH

Gesundheitswirtschaft ist zentrale Branche für Wirtschaftsstandort Deutschland

Die aktuellen Daten der Gesundheitswirtschaftlichen Gesamtrechnung (GGR) für das Jahr 2020 zeigen, dass die Gesundheitswirtschaft weiterhin zu einer der zentralen Branchen des Wirtschaftsstandort Deutschlands zählt. Die größte Gruppe bildeten die 7,4 Millionen Erwerbstätigen im Sektor Gesundheit.

Die Gesundheitswirtschaft ist und bleibt eine der wichtigsten Branchen für die deutsche Volkswirtschaft. Im Jahr 2020 erwirtschaftete sie 364 Milliarden Euro und damit zwölf Prozent der deutschen Bruttowertschöpfung. Gerechnet auf einen Tag hat die Gesundheitswirtschaft im Jahr 2020 rund 1 Milliarde Euro Bruttowertschöpfung geschaffen. Jeder sechste Erwerbstätige arbeitet in der Gesundheitswirtschaft, insgesamt sind das 7,4 Millionen Menschen.

Im Pandemie-Jahr 2020 hat auch die Gesundheitswirtschaft einen Rückgang von minus 3,7 Prozent Bruttowertschöpfung verzeichnet. Während die industrielle Gesundheitswirtschaft mit minus 9 Prozent einen deutlichen Einbruch erlitten hat, war der Rückgang im Bereich der medizinischen Versorgung mit minus 1,4 Prozent vergleichsweise gering.

Die Daten zeigen, dass die Gesundheitswirtschaft ein wichtiger Wachstumsfaktor für die Gesamtwirtschaft ist: Im Durchschnitt der letzten zehn Jahre ist die Gesundheitswirtschaft stetig gewachsen, mit durchschnittlich 3,3 Prozent pro Jahr sogar deutlich stärker als die Gesamtwirtschaft. Zum Vergleich: Die deutsche Volkswirtschaft wuchs durchschnittlich um 2,5 Prozent pro Jahr.

Wie das Statistische Bundesamt (Destatis) anhand erster Ergebnisse des Mikrozensus 2020 mitteilt, arbeiteten im Jahr 2020 rund 17,9 Millionen

Menschen oder 43 % der erwerbstätigen Personen ab 15 Jahren in Branchen, in denen kritische Infrastrukturen beheimatet sind. Die größte Gruppe bildeten die 7,4 Millionen Erwerbstätigen im Sektor Gesundheit, gefolgt von 3,4 Millionen Erwerbstätigen im Sektor Staat und Verwaltung sowie 2,9 Millionen im Sektor Ernährung.

Gesundheitswirtschaft im Überblick

Die Gesundheitswirtschaft setzt sich aus vielen Akteuren zusammen. Der Kernbereich, auch erster Gesundheitsmarkt genannt, umfasst den Bereich der "klassischen" Gesundheitsversorgung, die größtenteils durch die gesetzliche Krankenversicherung (GKV) und die private Krankenversicherung (PKV) einschließlich Pflegeversicherung finanziert werden.

Als zweiter Gesundheitsmarkt werden alle privat finanzierten Produkte und Dienstleistungen rund um die Gesundheit bezeichnet. Dabei ist die Zuordnung, welche Waren und Dienstleistungen einen Bezug zur Gesundheit aufweisen, nicht klar definiert und teilweise umstritten. Der zweite Gesundheitsmarkt umfasst nach allgemeinem Verständnis freiverkäufliche Arzneimittel und individuelle Gesundheitsleistungen, Fitness und Wellness, Gesundheitstourismus sowie – zum Teil – die Bereiche Sport/Freizeit, Ernährung und Wohnen.

Die demografische Entwicklung in Deutschland, der medizinisch-technische Fortschritt und das wachsende Gesundheitsbewusstsein in der Bevölkerung führen zu einer zusätzlichen Nachfrage an herkömmlichen professionellen Dienstleistungen in den Bereichen Gesundheit, Pflege und Betreuung, aber auch an Produkten und Dienstleistungen des zweiten Gesundheitsmarktes. Die Gesundheitswirtschaft bietet somit jetzt und für die Zukunft vielfältige Chancen für Wachstum und Beschäftigung sowie für Innovationen. Die Sonderauswertungen des DIHK zur wirtschaftlichen Lage und zu den Perspektiven der Unternehmen der Gesundheitswirtschaft ergeben daher in den letzten Jahren regelmäßig ein positives Bild, auch wenn die Erwartungen der Unternehmen derzeit gegenüber den Vorjahren gesunken sind. Die demografische Entwicklung wirkt aber nicht nur auf der Nachfrageseite, sondern stellt auch ein Risiko für die Gesundheitswirtschaft in Form des drohenden Fachkräftemangels dar. Dem steigenden Bedarf steht damit ein immer geringeres Angebot an jungen Arbeitskräften gegenüber. Wie in allen Wirtschaftsbereichen werden die Belegschaften älter und der Nachwuchs wird knapp.

Fusionen verändern die Gesundheitsversorgung

In Deutschland nimmt die Anzahl der Krankenhäuser ab. Waren es zur Jahrtausendwende noch 2424, zählte das Statistische Bundesamt im Jahr 2019 noch 1914 Krankenhäuser. Ein Grund für die Abnahme: Klinikfusionen. Konträre Diskussionen sezieren deren Vor- und Nachteile. Fusionsrechtliche Bedenken und verändertes Behandlungsangebot fusionierender Krankenhäuser sollten für die Gesundheitsversorgung ausbalanciert im Blick bleiben.

Fusionierende Krankenhäuser und Behandlungsangebot

Potenzial für eine Verringerung der Klinikanzahl ist vorhanden. Der Anteil der von Insolvenz bedrohten Kliniken wird in den kommenden Jahren voraussichtlich weiter steigen. Besonders Fusionen verändern die Gesundheitsversorgung, signalisiert das Deutsche Institut für Wirtschaftsforschung DIW. Einerseits können Fusionen die Qualität der Behandlung reduzieren, weil sie den Wettbewerb verringern, andererseits können sich Krankenhäuser durch Fusionen stärker spezialisieren und durch mehr Routine die Qualität verbessern.



synedra

|
information technologies

synedra AIM – Health Content Management

Jede Gesundheitseinrichtung ist einzigartig und stellt **individuelle Anforderungen**. Für Ihre Bedürfnisse bieten wir **synedra AIM** als maßgeschneiderte Lösung an.



Was können wir für Sie tun?
sales@synedra.com | www.synedra.com

Fusionen in Frankreich beispielsweise zeigen Auswirkungen. Betrachtet man die Akutkrankenhäuser, ist der regulatorische Kontext in Deutschland mit dem französischen vergleichbar. In beiden Ländern werden die Preise für die Gesundheitsversorgung gesetzlich festgelegt, Patienten können das behandelnde Krankenhaus relativ frei wählen und es gibt einen hohen Anteil privater Versorgung. Daher konkurrieren die Krankenhäuser eher in der Qualität als im Preis. Auch in Deutschland hat es viele Krankenhausfusionen gegeben. Laut dem Bundeskartellamt wurden zwischen 2003 und 2020 mehr als 300 Fusionen genehmigt. Das Bundeskartellamt sollte bei seinen Entscheidungen in Betracht ziehen, dass fusionierende Krankenhäuser eventuell ihr Behandlungsangebot verändern.

Bundeskartellamt und die Fusionskontrolle

Krankenhäuser sind unabhängig von ihrer Trägerschaft (Kommunen, Kirchen, privat) unternehmerisch tätig und stehen untereinander im Wettbewerb. Aufgrund der engen gesetzlichen Vorgaben existiert in diesem Bereich kaum Preiswettbewerb; Ziel der Fusionskontrolle ist es darum in erster Linie, den Wettbewerb um die Qualität der Versorgung der Patienten zu erhalten. Entscheidend dabei ist, dass den Patienten vor Ort hinreichende Auswahlalternativen zur Verfügung stehen.

Bei einer geplanten Fusion wird zunächst geprüft, ob die Leistungen der Krankenhäuser aus Sicht der Patienten vergleichbar sind. Beispielsweise wird der Markt der Akutkrankenhäuser vom Markt für Rehabilitationseinrichtungen oder Alten- und Pflegeheimen abgegrenzt. In räumlicher Hinsicht werden nur Krankenhäuser in eine Prüfung einbezogen, die von Patienten auch tatsächlich als Alternative aufgesucht werden.

Gerade bei Zusammenschlussprojekten öffentlich-rechtlicher Träger ist die Beschlussabteilung regelmäßig auch mit informellen Vorprüfungen der Pläne befasst. Auf diesem Wege können frühzeitig mögliche fusionsrechtliche Bedenken in die politischen Entscheidungsprozesse in den einzelnen Gremien der Gebietskörperschaften einfließen und nötigenfalls rechtzeitig alternative Lösungen angestrebt werden.

In den vergangenen Jahren mussten trotz des fortschreitenden Konzentrationsprozesses im Krankenhausbereich nur sehr wenige Vorhaben vom Bundeskartellamt untersagt werden. Zwischen 2003 und Juli 2020 wurden von insgesamt 325 angemeldeten Transaktionen lediglich sieben untersagt. Acht Projekte wurden nach kritischer Bewertung im Rahmen einer informellen Voranfrage letztlich nicht angemeldet (August 2020).

Klinikschließungen als Schock

Eine Bertelsmann-Studie 2019 schreckte auf: In Deutschland gibt es zu viele Krankenhäuser. Eine starke Verringerung der Klinikanzahl von aktuell knapp 1.400 auf deutlich unter 600 Häuser, würde die Qualität der Versorgung für Patienten verbessern und bestehende Engpässe bei Ärzten und Pflegepersonal mildern.

Eine Reduzierung der Klinikanzahl würde zu einer besseren medizinischen Versorgung der Patienten in Deutschland führen. In der Bertelsmann-Studie weisen führende Krankenhausexperten darauf hin, dass viele Krankenhäuser in der Bundesrepublik Deutschland zu klein sind und oftmals nicht über die nötige Ausstattung und Erfahrung verfügen, um lebensbedrohliche Notfälle wie einen Herzinfarkt oder Schlaganfall angemessen zu behandeln. Viele Komplikationen und Todesfälle ließen sich durch eine Konzentration auf deutlich unter 600 statt heute knapp 1.400 Kliniken vermei-

den. Ebenso gingen damit eine bessere Ausstattung, eine höhere Spezialisierung sowie eine bessere Betreuung durch Fachärzte und Pflegekräfte einher.

Analyse zu Versorgungs- und Qualitätsproblemen

Behauptungen über vermeintliche Versorgungs- und Qualitätsprobleme in der deutschen Krankenhauslandschaft im Ländervergleich sind oftmals falsch oder müssen deutlich relativiert werden. Internationale Vergleiche der Krankenhausversorgung sind vielfach undifferenziert und unkritisch. Zu diesem Ergebnis kommt eine Analyse des Deutschen Krankenhausinstituts (DKI), in der ausgewählte Gesundheits- und Versorgungsindikatoren der OECD-Datenbank darauf untersucht wurden, ob diese für Vergleiche geeignet sind. Dabei haben die Ersteller der Studie hinterfragt, ob den Daten einheitliche Datengrundlagen oder Definitionen zugrunde liegen und wie valide diese Daten sind. In einem zweiten Schritt wurden Besonderheiten der jeweiligen Gesundheitssysteme und bevölkerungsspezifischen Merkmale in die Analyse einbezogen, um Unterschiede zu erklären und die Aussagefähigkeit der Statistiken einzuordnen. Als Vergleichsländer wurden neben Deutschland, Österreich, Frankreich, Dänemark und die Niederlande herangezogen.

Krankenhaus- und Betten-dichte, stationäre Fallzahlen und Verweildauern

■ Im internationalen Vergleich weist Deutschland eine hohe Krankenhaus- und Bettendichte bzw. überdurchschnittliche Fallzahlen und Verweildauern im Krankenhaus auf. Dies belegt ein hohes Versorgungsniveau in Deutschland, das zudem einen spezifischen Bedarf bzw. Besonderheiten des deutschen Gesundheitssystems widerspiegelt.

■ Aufgrund einer im internationalen Vergleich überdurchschnittlichen Alters- und Morbiditätslast sowie einer größeren sozialen Ungleichheit, besteht in Deutschland ein höherer Bedarf an akutstationären Versorgungskapazitäten. Besonderheiten der prä- und poststationären Versorgung hierzulande, vor allem die mangelnde sektorenübergreifende Integration und Kooperation von Leistungsangeboten und unzureichende Nachsorgeangebote führen dazu, dass der Krankenhausbereich Versorgungsdefizite in anderen Leistungssektoren kompensieren muss. Eine isolierte Betrachtung der stationären Kapazitäten und Fallzahlen erscheint daher aufgrund der zentralen Rolle der Krankenhäuser in der Versorgungslandschaft nicht angemessen.

■ Auch die im internationalen Vergleich längeren Krankenhausverweildauern in Deutschland lassen sich maßgeblich durch den höheren Anteil der älteren Bevölkerung und der damit einhergehenden größeren Krankheitsschwere sowie durch bessere Nachsorgeangebote im Ausland erklären. So werden in Dänemark Kommunen finanziell sanktioniert, wenn sie unzureichende Nachsorgeangebote anbieten.

■ Es gibt viele länderspezifische Besonderheiten in der Datenverfügbarkeit, beim Datenumfang und der Datenauswertung. So werden bei Krankenhausverweildauern in Dänemark nur Fälle in somatischen Krankenhäusern mit einer Verweildauer unter 18 Tagen berücksichtigt. Auch der Datenumfang bei der Kennzahl zu Krankenhausbetten ist höchst unterschiedlich. In einigen Ländern werden psychiatrische Betten in der Kennzahl berücksichtigt, in anderen nicht.

Ausland zeigt Potenzial für Verringerung

Der Blick ins Ausland zeigt, so die Bertelsmann-Studie, dass es Potenzial für eine Verringerung der Klinikanzahl gibt. Deutschland weist im internationalen Vergleich im Durchschnitt mehr medizinisches Personal pro Einwohner auf als vergleichbare Länder, aber weniger pro Patient. Diese paradoxe Situation liegt daran, dass in der Bundesrepublik viel mehr Patienten in Krankenhäusern versorgt werden als im Ausland. Wie Untersuchungen ergaben, müssten rund ein Viertel der heute in deutschen Kliniken behandelten Fälle nicht stationär versorgt werden.

Zwar ist die konkrete Ausgestaltung der umliegenden ambulanten Strukturen noch offen, trotzdem belegen die Erkenntnisse der Studie, dass es zur Konzentration im Kliniksektor keine Alternative gibt. Zum einen kann eine Qualitätssteigerung nur gelingen, wenn sowohl die Patienten als auch die medizinischen und pflegerischen Fachkräfte in größeren, spezialisierten Kliniken mit mehr Fällen zusammengeführt werden. Auf der anderen Seite wird gut ausgebildetes Personal auch in Zukunft knapp sein. Nur durch die Bündelung könnten Krankenhäuser der Regelversorgung in allen zentralen Abteilungen jederzeit die entsprechende fachärztliche und pflegerische Kompetenz vorhalten.

Projektion und Zielbild

In einem jährlichen Krankenhaus-Rating schreibt das RWI – Leibniz-Institut für Wirtschaftsforschung e. V. in einem Basisszenario den Status quo des Jahres 2019 fort unter Berücksichtigung der Erkenntnisse während der COVID-19-Pandemie in den Jahren 2020 und 2021 sowie der demografischen Entwicklung und bereits beschlossener Gesetzesänderungen bis 2030. Annahme ist eine Rückkehr zum Vor-Krisen-Niveau im Jahr 2022 und eine Zunahme der

Fallzahl in Höhe von 4 Prozent gegenüber 2019 bis zum Jahr 2030. In diesem Szenario würde der Anteil der Krankenhäuser im „roten“ Rating-Bereich bis 2030 auf 26 Prozent und der Anteil der Häuser mit einem Jahresverlust auf 34 Prozent wachsen.

In einem Szenario „Neustart“ wird vom RWI angenommen, dass das Leistungsvolumen nicht mehr das Vorkrisenniveau von 2019 erreichen wird, sondern auf dem Niveau von 2021 stagniert und bis 2030 nur noch marginal ansteigt, sodass die stationäre Fallzahl im Jahr 2030 rund 6 Prozent unter dem Niveau von 2019 liegt. Kombiniert mit einer weiter sinkenden Verweildauer würde die Auslastung der stationären Kapazitäten infolgedessen stark sinken. In diesem Szenario würde sich die wirtschaftliche Lage der Krankenhäuser dramatisch verschlechtern. Nahezu drei Viertel der Häuser schrieben dann bereits ab 2022 Verluste und bis 2030 betrüge das durchschnittliche Jahresergebnis -10 Prozent. Bei kontinuierlichen Struktur- und Prozessoptimierungen sowie einer Anpassung der Krankenhauskapazitäten an das neue niedrigere Leistungsniveau könnte sich die Lage bis 2030 dagegen wieder etwa auf dem Niveau von 2019 stabilisieren.



Health IT Talk: Spannungsfeld Cyberfront

Malware, Verschlüsselungstrojaner, Datenleaks, Passwortdatenbanken: technisches Spezialwissen und komplexe Abläufe sind für Anwender im Krankenhaus nicht mehr komplett zu erfassen. Für höheren Schutz der vernetzten Systeme ist die IT in der Pflicht - interdisziplinär zusammen mit Management und Klinikfachbereichen. Das war Thema beim 124. Health IT Talk Berlin Brandenburg im Juli 2021. Moderator war Dr. Adrian Schuster, Vorsitzender Landesvertretung Berlin-Brandenburg. BVMi e.V. – Berufsverband der medizinischen Informatiker.

IT-Sicherheit ist in der Gesundheitswirtschaft ein Dauerbrenner, dem sich der Health-IT Talk regelmäßig widmet. „Smarte“ Geräte in Kliniknetzen bieten enorme Angriffsfläche für Cyberkriminelle. Weltweit stieg die Zahl der Cyber-Angriffe gegen Krankenhäuser um 45 Prozent im vergangenen Jahr. Alle anderen Sektoren der Weltwirtschaft zusammen ergaben dagegen nur einen Anstieg um 22 Prozent. Global deutlich wird eine weitere Professionalisierung und Industrialisierung der Cybercrime-Welt. Entsprechend müssen Staaten, Organisationen, Unternehmen und Anwender ihre Strukturen, Prozesse und Absicherungen weiter ausbauen. Stefan Maith, Team Leader Public Sector Government/Healthcare/Education bei Check Point Software Technologies GmbH, Köln gab dazu im Health IT Talk einen Überblick.

Ransomware-Angriffe mit Erpressung

Eine Angriffstaktik sind Ransomware-Angriffe mit Erpressung des Opfers. Fakt ist: Die Attacke startet nicht mit der Schadsoftware. Davor steht die Phishing Mail als Einfallstor mit der bekannten Schwachstelle „Mitarbeiter“. Informations- und Cybersicherheit hat branchenübergreifend enorm an Bedeutung gewonnen. Wachstum auf der dunklen Seite der „Cyberfront“ ist zu beobachten. Die Kriminellen sind bemüht, ihre Geschäftsmodelle zu optimieren, um höhere Renditen zu erzielen. Die Sicherheitsforscher von Check Point Research haben bei Cyberkriminellen eine neue Taktik beobachtet, wie diese ihre Lösegeldforderungen noch erpresserischer gestalten. Bereits seit längerem hat sich die doppelte Lösegeldforderung als

gängige Praxis bei Ransomware-Angriffen etabliert. Dabei werden die Daten gestohlen und mit deren Veröffentlichung gedroht. Zeitgleich werden die Daten beim Unternehmen verschlüsselt, so dass sie für das Unternehmen nicht mehr zugänglich sind. Dies wird als doppelte Erpressung bezeichnet. Bei einer weiteren Vorgehensweise erhalten auch Kunden, Lieferanten, Patienten oder Partnerunternehmen des angegriffenen Unternehmens Lösegeldforderungen. Bei ihnen ist ihre Integrität durch die gestohlenen Daten gefährdet. Sie erhalten entsprechende Zahlungsaufforderungen.

Erste Fälle für die dreifache Erpressung fanden im Oktober 2020 in Europa statt. In einer finnischen Klinik für Psychotherapie mit 40.000 Patienten tauchte ein Datenleck in Verbindung mit



Stefan Maith, Team Leader Public Sector Government/Healthcare/Education bei Check Point Software Technologies GmbH, Köln

Ransomware auf. Nachfolgend wurde eine große Summe des Lösegeldes von der Klinik gefordert. Doch auch einzelne Patienten erhielten Lösegeldforderungen in geringerer Höhe. Diese drohten die Kriminellen mit der Veröffentlichung von Aufzeichnungen aus Therapiesitzungen.

Das Angriffsschema mit doppelter Erpressung weist zwei neue Stufen auf. Es sind DDoS-Angriffe (Distributed Denial-of-Service) und Telefonanrufe bei den Geschäftspartnern des angegriffenen Unternehmens, um den Druck auf die Opfer zu erhöhen.

IOT - höherer Schutzbedarf der vernetzten Systeme

Experten warnen davor, dass Kriminelle vermehrt Internet of Things (IoT)-Geräte nutzen, um sich unerlaubten Zugang zu Netzwerken in Krankenhäusern zu verschaffen und lateral durch das System zu bewegen, Daten zu

stehlen (Verkaufspreis pro Electronic Health Record zwischen 250 und 1000 Euro) und diese zu verschlüsseln sowie für den Alltag kritische Funktionen zu sabotieren.

Bei IoT verlangen mehr Geräte und mehr individuelle Verbindungspunkte zum Internet breiteren und höheren Schutzbedarf der vernetzten Systeme. IT und Medizintechnik müssen sich gegen Attacken rüsten. IoT-Geräte in Krankenhäusern vereinfachen Behandlungen, sie übernehmen die Überwachung von Patienten und die Dokumentation intelligent und automatisiert. Jedoch genießt in der Konzeption und bei der Herstellung der einzelnen Geräte die IT-Sicherheit selten eine hohe Priorität. Dieser Umstand, kombiniert mit der Tatsache, dass etwa die Hälfte der angeschlossenen Geräte, wie Ultraschall- und MRT-Geräte, auf veralteten Betriebssystemen laufen, die nicht mehr unterstützt oder gewartet werden, schafft eine entsprechend große Angriffsfläche für Hacker.

Es gilt, die unterschiedlichen Angriffswege zu sperren. Dazu ist volle Transparenz nötig. Ein umfassendes Konzept zum Schutz der Geräte kann erst dann entstehen, wenn die IT-Fachkräfte über alle Geräte, die auf deren Netzwerk zugreifen, vollständig informiert sind. Viele Unternehmen verlassen sich noch darauf, Geräte manuell zu finden und zu identifizieren. Das mag für traditionelle Server und Workstations als Umgebung funktionieren, kann aber nicht mit der Vielzahl der IoT-Geräte mithalten, da dies eine automatisierte Lösung für eine vollständige Abdeckung erfordert.

Sicherheit erhöht eine Zero-Trust-Netzwerksegmentierung. Seitliche

Bewegung bedeutet, dass sich Hacker, sobald sie einmal in dem Netzwerk sind, frei bewegen können und bestimmte Geräte, wie Mailserver, ins Visier nehmen, um Schaden anzurichten oder auf wichtige Informationen zuzugreifen. Es braucht Programme, welche die Segmentierung des Netzwerks vereinfachen, wodurch sichere Bereiche auf der Basis von Zero Trust entstehen, die abgeschottet sind und den Zugriff nur legitimen Geschäftsanforderungen und autorisierten Personen gewähren.

Kernprozesse - und mehr

Gesetze forcieren mit Vorgaben die Weiterentwicklung beim IT-Sicherheitsgesetz 2.0 und KRITIS. Die Betreiber ausgewählter kritischer Infrastrukturen sind über das IT-Sicherheitsgesetz dazu verpflichtet, ein Mindestniveau der IT-Sicherheit einzuhalten. Der KRITISche Stammtisch untersucht seit Jahren dieses Themenfeld und vernetzt die Experten und Anwender. Konrad Christoph, Teamleiter Gesundheitswesen bei SHD, Dresden, und Mike Zimmermann, IT-Sicherheitsbeauftragter des Universitätsklinikums Carl Gustav Carus Dresden, informierten über den aktuellen Stand der gesetzlichen Regelungen sowie bei KRITIS. Der Schwellenwert von 30000 Fallzahlen p.a. als Messgröße bleibt bestehen, im Blick stehen verstärkt dabei Klinikverbünde und -ketten. Was sich ändert: Die Befugnisse des BSI weiten sich aus, mit erweiterten Kontroll- und Prüfungsbefugnissen. Angesagt ist eine aktive Schwachstellen-suche und -beseitigung. Im Bußgeldkatalog steht künftig maximal 2 Millionen Strafzahlung (bisher 100.000 Euro). Bei

Kernkomponenten greifen Standards. Der Gesetzgeber kann Mindeststandards für kritische Komponenten definieren. Herstellerkontrolle umfasst die Einführung einer Vertrauenswürdigkeitserklärung, was die gesamte Zulieferkette betrifft. Ein einheitliches IT-Sicherheitskennzeichen gilt als transparentes Gütesiegel. Doch die Freude über diese Änderungen ist verfrüht. Details sind in den jeweiligen Rechtsverordnungen erst noch zu definieren.

Konrad Christoph wies besonders auf die Komplexität der Informationsverarbeitung und der damit verbundenen Verwundbarkeit hin. Sie betrifft nicht nur den Kernprozess als medizinische Behandlung, sondern auch die Unterstützungs- und Management-Prozesse. Hier sei als Beispiel auf die Gebäudeleittechnik hingewiesen, man stelle sich vor, dass Klimaanlage wird manipuliert, welche Auswirkung das auf dem laufenden Klinikbetrieb wie OP- oder Intensiv-Bereich hätte.



Konrad Christoph, Teamleiter Gesundheitswesen bei SHD, Dresden

Denn auch das Klimaanlage-System hat u.a. Fernwartungszugänge und ist dadurch von außen erreichbar und damit angreifbar. Auch für diesen Mitarbeiterkreis sollte eine regelmäßige Awareness-Schulung geplant und durchgeführt werden.

Konrad Christoph merkte zum Bereich Einkauf an, dass jedes Gerät einen Lebenszyklus besitzt, unabhängig ob Investition oder Leihstellung, der bei der Beschaffung beginnt und bei der Außerbetriebsetzung endet. Hier sei besonders auf das Risiko bei der vernetzten Medizintechnik hingewiesen. Bei Beschaffungsbeginn sollte die DIN 80001-1 und ergänzend MDS2 (Manufacturer Disclosure Statement for Medical Device Security) in der Zusammenarbeit mit der Medizintechnik und IT noch stärkere Berücksichtigung finden.

Impulse beim Health IT Talk Berlin Brandenburg im Juli 2021 gab es genug. Für die Betreiber kritischer Infrastrukturen gilt das IT-Sicherheitsgesetz, wonach effektive Sicherheitsmaßnahmen zu etablieren sind. Merke: IT-Sicherheit ist interne Herausforderung, als Chefsache, und interdisziplinär als Pflicht für die IT zusammen mit Klinikfachbereichen. Die Unternehmensleitung hat die Verantwortung, für eine hinreichende Abwehr des Unternehmens gegen Cyberattacken zu sorgen. Überregionale Kooperation ist angesagt: Auf Grund der sehr großen Herausforderungen der Informationssicherheit in Kliniken sowie der fehlenden hochspezialisierten Ressourcen sollten die Überlegungen einer Zusammenarbeit von mehreren Kliniken – jenseits von Klinikkonkurrenzdenken – mehr Raum finden.

Beim Health-IT Talk am 9.8.2021 steht das Thema „Digitale Reifegradmessung“ auf dem Programm. Im KHZG ist die Reifegradmessung aller geförderten Kliniken im zweijährigen Abstand vorgesehen und wird praktisch durch das Konsortium "DigitalRadar" umgesetzt. Wie sieht das Reifegradmodell aus, wie wird es entwickelt, wie ergibt sich der Bezug zu bereits etablierten (internationalen) Modellen?

Health-IT Talk

Branchenprofis tauschen sich im monatlich stattfindenden Health-IT-Talk Berlin-Brandenburg verbands- und fachrichtungsübergreifend zur Digitalisierung der Gesundheitswirtschaft aus. Die vier Partner (BVMI, KH-IT, SIBB, TMF) beschäftigen sich mit aktuellen Branchenthemen in Fachvortrag und Diskussion.

www.health-it-talk.de

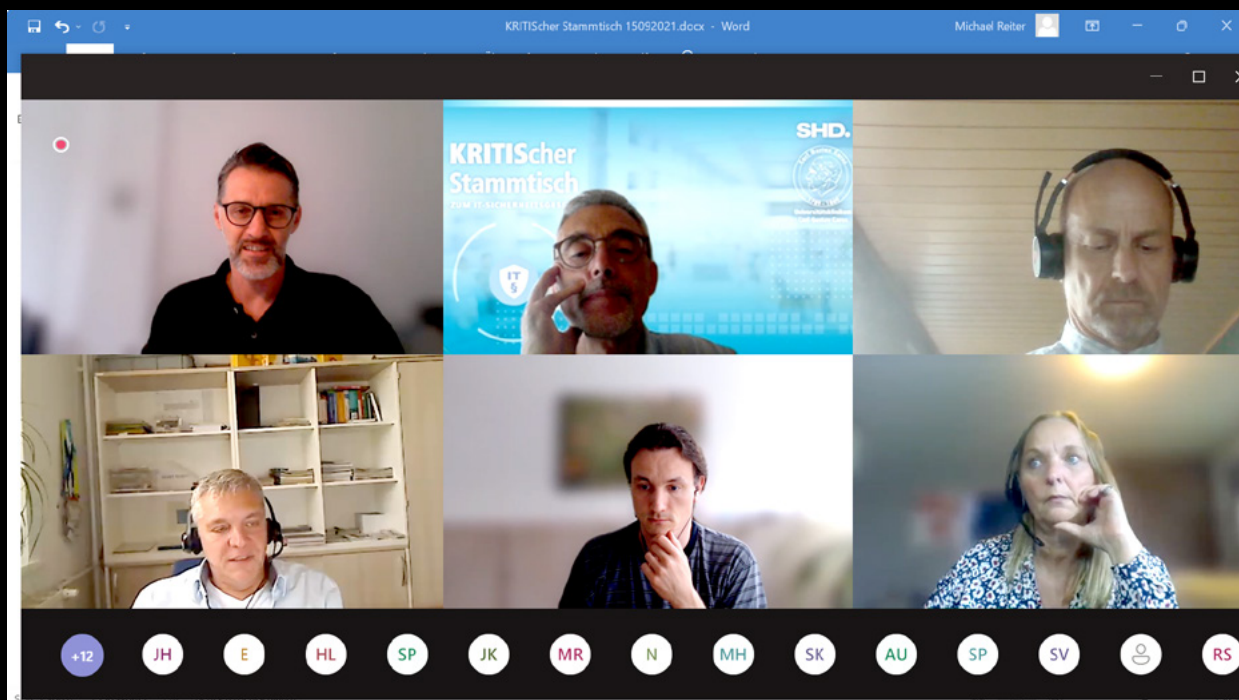


Mike Zimmermann, IT-Sicherheitsbeauftragter des Universitätsklinikums Carl Gustav Carus Dresden

Aktuelle Themen der IT-Sicherheit im Kontext von KRITIS und darüber hinaus

Der 13. KRITISche Stammtisch

Er bringt Informationssicherheitsbeauftragte (ISB), Krankenhaus-IT-Leiter, Vertreter von Verbänden und Behörden sowie der Industrie zusammen: der KRITISche Stammtisch. Zurück geht er auf eine gemeinsame Initiative des Universitätsklinikums Carl Gustav Carus der TU Dresden und der SHD System-Haus-Dresden GmbH im Jahr 2017. Präsentationen und Diskussionen zu IT-Sicherheits-Themen wenden sich nicht nur an Häuser, die unter die KRITIS-Vorgaben fallen, sondern an alle – insbesondere im Kontext der Ausweitung der Geltung des B3S. Längst sind auch Regionen über Mitteldeutschland hinaus vertreten. Von Michael Reiter



Zur 13. Ausgabe begrüßten Konrad Christoph, KRITIS-Experte und Mike Zimmermann, IT-Sicherheitsbeauftragter des Dresdener Universitätsklinikums, im September rund 35 Teilnehmer online. Auf der Agenda standen die Reifegradmessung im Kontext des Krankenhauszukunftsgesetzes (KHZG), die Umsetzung von IT-Sicherheit in Krankenhäusern nach § 75c SGB V, Security Monitoring in IT von Stromversorgern sowie KIM und sichere Kommunikation im Kontext der Telematikinfrastruktur.

Messung des digitalen Reifegrades

Thorsten Schütz berichtete über die Reifegradmessung laut §14b KHZG. Neben der Bereitstellung eines hilfreichen Werkzeuges zur Selbsteinschätzung für die Krankenhäuser ist eine weitere Motivation für die Politik, einschätzen zu können, ob die Fördergelder erfolgreich umgesetzt werden, so der Leiter IT und Betriebsorganisation am Klinikum Itzehoe und Stellvertretender Vorsitzender des Bundesverbandes der Krankenhaus-IT-Leiterinnen/Leiter. Messungen 2021 und 2023 sollen Einblick geben, ob das KHZG tatsächlich die erwarteten Verbesserungen gebracht hat. Verpflichtend sind die Messungen für alle Häuser mit Bedarfsmeldung, für die anderen ist dieses freiwillig. Eigentlich hatte die erste Reifegradmessung im Juni starten sollen; nach verspäteter Projektvergabe ist mit Beginn im Oktober zu rechnen. „DigitalRadar“ heißt das Modell, das das GewinnerKonsortium unter Leitung der HIMSS ausformuliert. Im Expertenbeirat des HIMSS-Konsortiums mit Krankenhäusern unterschiedlichster Größe und Trägerschaft sowie Kostenträgern ist auch der Bundesverband KH-IT vertreten. Das Reifegradmodell soll eine standardisierte und umfassende Bewertung des Digitalisierungsgrads von Krankenhäusern ermöglichen; hierzu dient die

Selbsteinschätzung der Krankenhäuser auf Basis des in Pilotheusern getesteten Kriterienkatalogs. Der Aufwand der Beantwortung der rund 230 Fragen

(Stand 3.8.) wird wohl die ursprünglich veranschlagten 2,5 Stunden deutlich überschreiten, betonte Schütz. Einbezogen werden sollen neben der IT auch Berufsgruppen wie Ärzte, Pflegepersonal und Controller – um festzustellen, wie wirksam IT die Prozesse unterstützt.

Jedes Haus hat einen Verantwortlichen zu benennen.

Umsetzung von IT-Sicherheit in Krankenhäusern nach § 75c SGB V

Mario Beck, Referent Dezernat III – IT, Datenaustausch und eHealth, Deutsche Krankenhausgesellschaft, erläuterte den Stammtischteilnehmern die Anforderungen des Paragraphen 75c SGB V.

Danach sind Krankenhäuser ab dem 1. Januar 2022 verpflichtet, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Informationssicherheit zu treffen. Ziel des Gesetzgebers sei die Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie die weiteren Sicherheitsziele informationstechnischer Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patientendaten maßgeblich sind. Auch sei im Paragraphen 75c SGB V festgelegt, dass Organisatorische und technische Vorkehrungen „angemessen“ dann sind, wenn der erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung des Krankenhauses bzw. der Sicherheit der verarbeiteten Patientendaten stehe, so Beck. Diese Vorkehrungen seien anschließend spätestens alle zwei Jahre an den aktuellen Stand der Technik anzupassen.

In der Zwischenzeit gibt es ein offizielles Update im Kontext von DigitalRadar: Mit einer Veranstaltung am 29. September gab das Konsortium den Abschluss der Pilotphase und den Start der Messung am 5. Oktober bekannt

<https://www.digitalradar-krankenhaus.de/digitalradar-pilotphase-abgeschlossen/>

Erfüllen könnten die Krankenhäuser diese Verpflichtungen insbesondere, indem sie den branchenspezifischen Sicherheitsstandard B3S in der jeweils gültigen Fassung anwenden. Allerdings stünden nicht allen Krankenhäusern die benötigten Ressourcen zur Verfügung, um den B3S von Anfang an vollumfänglich zu erfüllen bzw. wird Unterstützung in der konzeptionellen Ausgestaltung der Anforderungen des B3S benötigt.

Um es allen Krankenhäusern zu ermöglichen, die gesetzlichen Anforderungen zu erfüllen, verfolgt die DKG das Ziel, die im B3S formulierten Anforderungen für Krankenhäuser in geeignete Umsetzungshinweise, Leitfäden und Vorlagen zu übersetzen, die adressatengerecht die für die Umsetzung notwendigen Themen aufgreifen sollen. Hierbei sollen auch bestehende, bereits in der praktischen Anwendung befindliche Projekte, wie beispielsweise die Orientierungshilfe „IT-Sicherheit in Kliniken“ des Landesamtes für Sicherheit in der Informationstechnik Bayern berücksichtigt werden, erläutert Beck.

Security Monitoring in der Stromversorgung

Der Stammtisch bot den vergleichenden Brückenschlag zur Stromversorgung, einer ebenfalls kritischen Infrastruktur. Wie erkennen Übertragungsnetzbetreiber Angriffe? Für das Sicherheitsmonitoring in Information Technology (IT) und Operation Technology (OT) gibt es keine Lösungen „out of the box“, betonte Felix Schiller, IT-Sec Management des Betreibers 50 Hertz Transmission. Die Bedrohung ist enorm – das zeigen Attacken auf das ukrainische und US-Stromnetz. Analysen identifizierten auch Aktivitäten von „APT“ (Gruppen „kompetenter“ Hacker) in Deutschland.

Der Ansatz von 50 Hertz Transmission beinhaltet einen vielschichtigen Monitoring-Setup: mit „Corporate Network“ (IT), „Control System Network“ (IT/OT), und „Remote Systems“ (OT). An einem Punkt werden alle detektierten Informationen zusammengeführt. Bei Identifizieren der schwer zu findenden APT dienen Ursprungsländer der „Anfragen“ potenzieller Angreifer ebenso als Erkennungshilfe wie Anomalien im Nutzerverhalten. So sieht laut Schiller der Weg zum Erfolg aus: Ereignisdaten (Zugriffe, Firewall logs, remote Sessions)

verfeinern, Daten (Missbrauch, Inkonsistenzen) analysieren, Infrastruktur auf Basis der Analysen härten.

„KIM verbindet“

Wie sichere Kommunikation die Telematikinfrastruktur belebt, präsentierte Rene Schubert. Er ist Geschäftsführer der Deutschen Krankenhaus Trust-Center und Informationsverarbeitung GmbH (DKTIG). Mit zunehmender Digitalisierung erfordert die Daten- und Informationssicherheit im Gesundheitsumfeld besondere Aufmerksamkeit, sagte Schubert. In seinem Fokus stand die Kommunikation der Beteiligten innerhalb und außerhalb der sicheren Telematikinfrastruktur.

Vor dem Hintergrund der hohen Anforderungen bietet sich „Kommunikation im Medizinwesen“ (KIM), Herzstück der Telematikinfrastruktur, als sicheres Übermittlungsverfahren nach § 311 Abs. 6 SGB V an. Höchste Sicherheitsstandards werden dank des Zulassungsverfahrens der gematik und des Bundesamtes für Sicherheit in der Informationstechnik gewährleistet – etwa durch Absender- und Empfängerauthentizität, Manipulationsprüfung und Verschlüsselung. Zugelassene KIM-Anbieter

sind im Fachportal der gematik gelistet. KIM, fasste Schubert zusammen, sorgt für sichere und medienbruchfreie Kommunikation und wird die Vernetzung und Kommunikation zwischen den Beteiligten beschleunigen. Mit der Ausbaustufe 2 werden dann die Mehrwerte erlebbar.

Die Diskussion

Eine wertvolle Komponente des Stammtischs ist die Diskussion. Auch dieses Mal fand ein engagierter Austausch von Informationen und Meinungen statt, an dem sich unter vielen anderen das Bundesamt für Sicherheit in der Informationstechnik beteiligte, vertreten durch René Salamon, Sektorverantwortlicher, Bereich Gesundheit. Zur Sprache kamen Herausforderungen wie Personalfindung zum Meistern der anspruchsvollen Aufgaben und das zunehmende Risiko von Haftungsthemen für IT-Abteilungen.

Der KRITische Stammtisch hat nun eine eigene Website: www.kritischer-stammtisch.de. Sie wird weitergeleitet an die SHD-Seite. Jedes Mitglied kann sich registrieren. Jetzt muss die Seite mit Leben gefüllt werden – so die Sprecher von SHD.

**BEI
SPEZIAL-
FRAGEN ...**

**... DIE
SPEZIALISTEN
FRAGEN.**

SANOVIS

■■■■ CONSULTING WITH CARE.

Ihr spezialisierter Partner für **IT-Strategie und IT-Management** in der Gesundheits- und Sozialwirtschaft.

Die Spezialisten für IT-Strategie und IT-Management bei **CURACON**

Unternehmenserfolg durch Nutzen stiftende Digitalisierungsprojekte

15 Jahre ENTSCHEIDERFABRIK - Lösungen für einen reibungslosen Geschäftsprozess

Seit 2006 setzt das Eco-System ENTSCHEIDERFABRIK mit den Krankenhaus-Entscheidern die Chancen der digitalen Transformation um. 36 fördernde Verbände und gewählte Berater, über 800 Einzelstandorte von Kliniken und über 150 Industrie-Unternehmen arbeiten zusammen mit dem Ziel, den Nutzen stiftenden Beitrag von Digitalisierungsprojekten aufzuzeigen.

Das Konzept für eine erfolgreiche Zukunft

Seit nunmehr 15 Jahren hat sich das Konzept der ENTSCHEIDERFABRIK zu einer festen und vor allem erfolgreichen Größe etabliert. Die Inkubator-Funktion für Digitalisierungsprojekte als Format der ENTSCHEIDERFABRIK hat durch eine stetige Weiterentwicklung dieser Arbeits- und Kommunikationsplattform wesentlich zum Wertbeitrag für einen Klinikerfolg beigetragen. Die festen Bausteine der ENTSCHEIDERFABRIK wurden im Laufe der Zeit durch vermehrte Klinik-Nachfrage ausgebaut und erweitert, auch die internationalen Aktivitäten zeigen nachhaltige Resultate.

Der Entscheider-Zyklus eines jeden Jahres, der Leistungserbringer, Industrie und Berater zusammenbringt, besteht aus den Hauptbausteinen:

- Wahl der Digitalisierungsthemen auf dem Entscheider-Event (Februar),
- Ausarbeitung der Digitalisierungsthemen auf dem Sommer-Camp (Juni) und
- Präsentation der Entscheidungsvorlagen für Krankenhaus Unternehmensführung auf der Ergebnis-Veranstaltung auf dem Deutschen Krankenhaustag.

Ergebnis-Veranstaltung auf dem Deutschen Krankenhaustag 2021

Am 16. November 2021, ab 10 Uhr, findet die Ergebnis-Veranstaltung des

Entscheider-Zyklus 2021 sowie der Deutsche Krankenhaustag als digitaler LiveStream statt. An diesem Tag werden zudem die Gewinner des "StartUp-/Digitalisierungspreises", die Berater und Projektleiter für die Betreuung der 5 Digitalisierungsthemen 2021 und die Unternehmens-/Klinikführer*in 2021 verkündet und ausgezeichnet. Anmeldungen und Informationen unter [ENTSCHEIDERFABRIK.com/digitales-live-streaming](https://entscheiderfabrik.com/digitales-live-streaming)

Health Information Exchange Leadership Summit auf Sylt

Vom 15.-16. Dezember 2021 findet der Health Information Exchange Leadership Summit auf der nordfriesischen Insel Sylt statt. Bei diesem Summit lädt der Gründerverband der ENTSCHEIDERFABRIK, die Association of Health Information Management Executives, zum „Health Information Exchange“ ein. Das Summit findet im Wechsel in Österreich, Deutschland und der Schweiz statt. 2022 im USB. entscheiderfabrik.com/2021-health-information-exchange-leadership-summit

Entscheider-Event 2022

Vom 16.-17. Februar 2022 findet der Entscheider-Event, die Auftaktveranstaltung zu einem neuen Entscheider- Zyklus, im Industrie-Club in Düsseldorf statt.

Der Digitalisierungsgipfel der Gesundheitswirtschaft ist ausschließlich der Krankenhaus Unternehmens-, IT-

und Medizintechnikführung, Vertretern der Wissenschaft und den fördernden Industrie-Unternehmen und Verbänden sowie vorbehalten. Ziel der Veranstaltung ist es, die 5 Digitalisierungsthemen der Gesundheitswirtschaft zu wählen. Zur Vorbereitung dazu werden während der zweitägigen Veranstaltung die Ergebnisse des Vorjahres vorgestellt. Informationen unter <https://entscheiderfabrik.com/2021-entscheiderfabrik-15-jahre-digitalisierung-der-deutschsprachigen-gesundheitswirtschaft> oder bei Dr. Pierre-Michael Meier Pierre-Michael.Meier@guig.org

Kongress Krankenhausführung & digitale Transformation

Vom 18.-19. Mai 2022 werden auf dem Kongress in Bad Kreuznach die finalen Ergebnisse der 5 Digitalisierungsthemen der Gesundheitswirtschaft 2021 vorgestellt, in acht Workshops Schwerpunktthemen behandelt und Vorträge zum Thema in vier nationalen und in einer internationalen Session gehalten. Pro Tag ist eine Key Note vorgesehen, d.h. eine zu den aktuellen Herausforderungen in der digitalen Transformation und eine zum Zielbild Krankenhausversorgung.

<https://entscheiderfabrik.com/kh-fuehrung-digitale-transformation-2022>

Allgemeine Informationen zur Hospitalgemeinschaft

Motivation

- Digitale Transformation innerhalb der Kliniken
- Die Institutionalisierung eines „Health Information Managements“ ist der Schlüssel zum Erfolg.
- Die Geschäftsführer initiierten die Hospitalgemeinschaft.

Ziele

- Institutionalisierung über kontinuierliche Betreuung, Bündelung und Organisation des Information Management
- „Smarte Organisation“

Motto

- „Von Hospitälern für Hospitäler“, so soll bei den einzelnen Mitgliedern das Health Information Management erreicht werden.

Rahmenparameter wie Vergütung

- Das Stammhaus zahlt weiterhin Gehalt sowie Unterbringung und Reisekosten.

TRAINEE-PROGRAMM „DIGITAL HEALTH-EXPERT“

Das attraktive Trainee Programm findet bei den Mitgliedshäusern und den Rahmenvertragspartnern der Hospitalgemeinschaft Hosp.Do.IT statt.

Eingangsvoraussetzung ist ein abgeschlossenes Bachelorstudium bzw. eine entsprechende Ausbildung.

In der drei jährigen Laufzeit des Trainee Programms werden Module innerhalb der verschiedenen Mitgliedshäuser und Rahmenvertragspartner im Training on the Job durchlaufen.

Pro Trainee Jahr wird der Trainee ca. neun Monate in seinem Stammhaus und max. 3 Monate bei Mitgliedshäusern und Rahmenvertragspartnern tätig sein. Durch den Wechsel zu den unterschiedlichen Partner sollen verschiedene Blickwinkel und interessante neue Erkenntnisse gewonnen werden.

Die Projektarbeit bei Mitgliedshäusern oder Rahmenvertragspartner wird mit dem Stammhaus jeweils gesondert geregelt.

Der Trainee bleibt Angestellter bei seinem Stammhaus.

Die Lernstoffüberprüfung zum „Digital Health Expert“ wird analog der digitalen Reifegrad Messung erfolgen, d.h. des internen Modells, als auch des Modells des Bundesministeriums für Gesundheit.

Nach dem erfolgreichen Abschluss des dreijährigen Trainee-Programms wird der Titel „Digital Health Expert“ erworben.

Haben wir Ihr Interesse geweckt?

Bitte senden Sie Ihre aussagekräftigen Bewerbungsunterlagen und Ihre bevorzugte Region an: Trainee@Hosp-Do-IT.de

Die drei Gründer in 2015 der Hosp.Do.IT



Seit dem Entscheider-Event im Februar 2018 sind hinzugekommen:



Mit Wachstum an die Spitze

Die Dedalus Gruppe ist in den vergangenen Jahren stark gewachsen und strebt weiter nach oben. Das Unternehmen orientiert sich in Richtung Weltmarktspitze. Zum weiteren Weg äußert sich Winfried Post, General Manager und Geschäftsführer Dedalus HealthCare DACH.

Welche Mission verfolgt die Dedalus Gruppe?

W. Post: Wir wollen Gesundheitseinrichtungen – allen voran Ärzte, Pflegekräfte und anderes Gesundheitspersonal – mit unseren Lösungen dabei unterstützen, ihre Patienten optimal zu versorgen. Darüber hinaus wollen wir jedem die Möglichkeit geben, sich für seine eigene Gesundheit und sein Wohlbefinden zu engagieren. Dafür müssen Gesundheitsdienstleistungen leicht zugänglich sein, wozu wir beitragen wollen. Und wir wollen dabei helfen, die Fragmentierung und die Sektorengrenzen im Gesundheitswesen zu überwinden. Dazu gehört auch eine stärkere Vernetzung und ein nachhaltigeres Arbeiten, was Kosten und Umweltbelastung reduzieren kann.

Health IT hat aber grundsätzlich in allen Bereichen des Gesundheitswesens eine große Bedeutung, auch bei Versicherungen, Apotheken oder ambulanten Pflegediensten. Als Marktführer im Bereich der Krankenhaus-Informationssysteme sind wir Teil dieses dynamischen Marktes. Aufgrund unserer herausgehobenen Position sehen wir uns als Treiber innovativer Entwicklungen. Wir erwarten, dass dies durch das Krankenhauszukunftsgesetz weiter gefördert wird.

Worauf gründet sich die herausgehobene Position?

W. Post: Auf Fakten. 2020 haben wir beispielsweise 20 Krankenhäuser als neue ORBIS KIS-Kunden gewonnen. In den Bereichen Radiologie- und Kardiologie-IT haben wir den höchsten Auftragseingang aller Zeiten erzielt. Auch alle anderen Segmente tragen maßgeblich zum Jahresumsatz von 222 Millionen Euro bei. Heute arbeiten täglich gut 700.000 Anwender in Deutschland, Österreich und der Schweiz mit unseren Systemen, über 40 Prozent aller stationären Fälle werden in Deutschland darüber abgewickelt.

Wir als DACH-Organisation sind ein sehr bedeutender Teil von Dedalus geworden und stehen für ein Drittel des Gesamtumsatzes.

Worauf führen Sie die guten Zahlen zurück?

W. Post: Auf gute Lösungen, unser Know-how und sehr viel Fleiß. Wir konzentrieren uns ausschließlich auf Health IT, also Software, IT-Lösungen und Hightech für das Gesundheitswesen. Wir zählen allein 880 Einrichtungen, die in der DACH-Region mit unserem Krankenhaus-Informationssystem ORBIS arbeiten. Diese Position hilft uns bei der Entwicklung neuer Lösungen, weil wir sie ganz nah an den Bedürfnissen der Anwender ausrichten können.

Nun hat Dedalus vor gut einem Jahr den Big Player Agfa HealthCare übernommen.

Wie verläuft die Integration?

W. Post: Eine Integration ist auf verschiedenen Ebenen immer mit sehr viel Arbeit verbunden. Wir sind aber absolut im Plan. Da Dedalus vorher keinerlei Aktivitäten in der DACH-Region hatte, konnten wir unser gesamtes Produktportfolio beibehalten, ohne Lösungen integrieren zu müssen. Das hat uns eine Menge Zeit und Mühe erspart, die wir in unsere Kunden investiert haben. Notwendige Anpassungen bezogen sich lediglich auf unsere internen Prozesse. Nichts, worüber man sich Sorgen machen müsste.

Nun expandieren Sie weiter.

W. Post: Das stimmt. Zum 1. April haben wir die Health IT-Sparte von DXC Technology übernommen. Damit sind wir nun auch sehr stark in Großbritannien und Irland, Skandinavien, Spanien sowie Australien vertreten. Unser neues Unternehmen steuert etablierte Cloudlösungen bei, die auch für den DACH-Markt interessant werden könnten. Das Unternehmen hat sich bei der Umwandlung traditionell gehosteter Dienste in hochsichere Cloud-Plattform-Services und bei der Sicherung von Versorgungsprozessen durch die Bereitstellung einer einheitlichen Datenplattform bereits einen guten Namen gemacht. Darüber hinaus wird DXC

Technology unser Portfolio um neue Komponenten erweitern, beispielsweise um eine Multi-Ressourcen-Unternehmensplanung und das Closed-Loop-Medikationsmanagement. Auch Technologien wie Künstliche Intelligenz, maschinelles Lernen sowie die Verarbeitung natürlicher Sprache – alles Punkte, die die Diskussion von Klinikmanagern bereits heute bestimmen – bringt DXC Technology ein. Ein Beispiel für die Umsetzung der Technologien ist die Frage, wie man klinische Risiken für bestimmte Bevölkerungsgruppen nahezu in Echtzeit identifizieren kann. Das wird die Gesundheitsversorgung nachhaltig verbessern.

Ebenfalls neu in der Dedalus-Familie ist Amphi Systems. Das 2015 in Aalborg, Dänemark, gegründete Unternehmen bringt seine Lösungen zum Aufbau einer vorklinischen Patientenakte und Software für den Rettungswagen ein.

Und dann sind mit Dosing und OSM auch noch zwei deutsche Unternehmen dazugestoßen?

W. Post: Korrekt. Mit Dosing haben wir einen führenden Anbieter von digitalisierten Software-as-a-Service (SAAS)-Lösungen für die Medikationssicherheit übernommen und damit unser Portfolio um Speziallösungen für medizinische Entscheidungsträger und Patienten entlang des gesamten Medikationsprozesses – von der Therapieempfehlung über die Verordnung bis zu Applikationsangaben und Anwendungshinweisen – erweitert. Die Dosing-Lösungen kommen heute bereits in mehr als 270 Einrichtungen, größtenteils in Deutschland, erfolgreich zum Einsatz. Die Übernahme ist ein wichtiger Schritt, unser Angebot in Deutschland, Österreich und der Schweiz zu komplettieren.

Mit der OSM AG begrüßen wir einen der Marktführer im Bereich von Labor-Informationssystemen in der DACH-Region. Diese Akquisition stärkt unsere überragende Position in der Primärdiagnostik weiter. Das Lösungsportfolio der Firma ist gleichsam der Goldstandard im Laborgeschäft. Zudem gehört OSM, wie wir auch, zu den Pionieren der Digitalisierung im deutschsprachigen Raum. Das technologische Know-how und die hohe Marktakzeptanz, die sich in der großen installierten Basis von 550 Kunden widerspiegelt, tragen maßgeblich zum Erfolg bei. Das Flaggschiff-Produkt von OSM ist das Multi-Labor-Informationssystem Opus::L, ein hochmodernes System, das durch Produkte und Dienstleistungen im Bereich Informationslogistik und Systemintegration ergänzt wird. Nicht zuletzt unterstreicht die Akquisition klar die Bedeutung des DACH-Marktes für die Wachstumsstrategie von Dedalus.

Steht in Sachen Akquisition noch mehr zu erwarten?

W. Post: Wir haben immer gesagt, dass wir zuerst einmal organisches Wachstum generieren müssen, um anorganisch wachsen zu können. Nach dem überzeugenden letzten Geschäftsjahr haben wir uns mit anderen Unternehmen verstärkt. Auch diesen Weg werden wir weitergehen, wenn es Sinn macht und unser Portfolio stärkt. Es ist nicht unsere Absicht, lediglich Marktanteile zu kaufen.

Sehen Sie da überhaupt noch Potenzial, Herr Post?

W. Post: Unbedingt. Die DACH-Region ist unser größter Markt. Hier betreuen wir über 1.500 Krankenhäuser und wachsen in Deutschland, Österreich sowie in der Schweiz gleichermaßen und in allen Bereichen. Der Weg ist aber noch nicht zu Ende. Zum einen hilft uns das Bekenntnis der Regierungen zur weiteren Digitalisierung des Gesundheitssektors, zum anderen hat die Corona-Pandemie uns allen die Defizite noch einmal klar vor Augen geführt. Das Krankenhaus Zukunftsgesetz wird bereits als Anreizsystem für Investitionen wahr- und angenommen. Hier werden sich auch weiterhin viele Möglichkeiten ergeben, wie wir gemeinsam mit unseren Kunden die immer noch vorhandene Digitalisierungslücke schließen können.

Vielen Dank für die Einblicke, Herr Post.



www.dedalusgroup.de



Automatisierte Warenwirtschaft mit RFID – jetzt ganz einfach!

Automatisierte Warenwirtschafts- und Lagerverwaltungssysteme, basierend auf Radio Frequenz Identifikation (RFID), sind schon seit vielen Jahren auf dem Markt.

Kompliziert und kostspielig

In Kliniken und Praxen haben sich diese Systeme jedoch bisher noch nicht durchsetzen können, da sie meist nicht besonders anwenderfreundlich waren und meist zu hohe Kosten im Raum standen. Zudem kommt, dass der Umgang mit den neuesten RFID Technologien, wie zum Beispiel UHF (Ultra High Frequency) eine völlig neue Herangehensweise erfordert als mit den „alten“ etablierten Systemen wie LF (Low Frequency) oder HF (High Frequency).

LF Transponder lassen sich nur einzeln und im Nahfeld lesen. Diese Technologie kann einen Barcode gut ersetzen, da sie orientierungslos und schnell erfasst werden kann. HF Transponder haben den Vorteil, eine etwas größere Lesedistanz zu haben und dabei auch mehrere Produkte gleichzeitig zu erfassen. Der große Vorteil von UHF ist, dass Produkte mit einem solchen Transponder in großer Stückzahl unter Bewegung und auf große Distanzen gelesen werden können. Eine großflächig, automatisierte Bestandsüberwachung schien damit zum Greifen nahe.

Leider zeigte sich schnell, dass der Umgang mit UHF nicht so einfach ist, wie zunächst gedacht, denn die Vorteile der UHF Technologie sind gleichzeitig auch ein Nachteil. Wie soll man

unterscheiden, was sich gerade wo befindet? Welche Teile wurden schon gelesen? Welche Teile sollen nicht gelesen werden? Wie hält man verschiedene Regale oder Lagerorte auseinander? All diese Fragen blieben zunächst unbeantwortet und machten die vermeintlichen Mehrwerte zu Nichte.

Effiziente und anwenderfreundliche Lösung

Industrie und Handel haben es in den vergangenen Jahren jedoch geschafft, einen effizienten Einsatz von UHF möglich zu machen. Im Vordergrund steht dabei immer die Anwenderfreundlichkeit für den Nutzer der Systeme. So werden RFID Lösungen zunehmend „Bottom Up“ designed, damit zuerst die Nutzen der Systeme greifen, bevor aufwendige Integrationen gestartet werden. Denn auch die beste Integration scheitert langfristig, wenn Nutzer und Anwender die Lösungen nicht annehmen.

Zudem kommt, dass man gelernt hat Toleranzen zuzulassen, um damit unnötige Kostensprünge zu vermeiden. So kommen immer mehr Produkte auf den Markt, die schnell und einfach installiert, lokal bedient und dabei ganz individuell eingerichtet werden können.

Vereinfachte Handhabung

Am Beispiel des LeanWave MEDICAB zeigt sich, wie einfach die Anwendung geworden ist. Beim Einrichten des Systems werden die Barcodes der Produkte gescannt, die überwacht werden sollen. Das MEDICAB Einrichtungssystem druckt dann die dazugehörigen Transponder automatisch aus. Dies dauert nur wenige Sekunden und ab diesem Zeitpunkt werden die gekennzeichneten Produkte automatisch vom Schrank erkannt. Bestandsgrenzen für die Produkte können direkt am Schrank eingestellt und jederzeit angepasst werden. Der Schrank scannt nun in regelmäßigen Abständen den Bestand und gleicht in Echtzeit den Soll- und Ist-Bestand ab. Aufgrund der Vollmetallkonstruktion wird sichergestellt, dass keine Produkte außerhalb des Schrankes erfasst werden. Sollte ein Produkt im Schrank mal nicht gelesen werden, hat man im Zweifel einfach ein Produkt zu viel. Es kommt aber nicht mehr vor, dass man zu wenig Produkte hat. Auch Zugangsbeschränkungen und Entnahmedokumentationen sind schnell und einfach möglich.

Wichtige Informationen, wie zum Beispiel das Erreichen einer kritischen Bestandsgrenze wird vom Schrank per E-Mail an einen vordefinierten Verteilerkreis gesendet. Am Schrank selbst kann man sich den aktuellen Bestand jederzeit direkt anzeigen lassen.

Funktionsübergreifende Vorteile

Die Vorteile eines solchen Systems sind vielfältig und funktionsübergreifend. Die Stationsleitungen, sowie Pflegekräfte haben keinen manuellen Aufwand mehr, um Bestände zu checken, Bestellungen auszulösen und zum Beispiel OPs zu planen. Ausfälle von OPs aufgrund nicht vorhandenen Materials werden vermieden und trotzdem sind die Bestände effizient verteilt. Lieferanten können in den Frühwarnprozess, sowie den automatischen Bestellprozess eingebunden werden. Dies verkürzt die Reaktionszeit signifikant. Einkauf und Supply-Chain werden im Prozessfluss weiterhin zu 100% eingebunden, da auch sie im Verteiler aufgenommen werden können. Es wird also sichergestellt, dass Workflows nicht umgangen werden.

Aus IT-Sicht ist die Integration solcher Systeme ebenfalls denkbar einfach. Für die Kommunikation ist der Schrank mit einer eigenen LTE-Verbindung ausgestattet. Alternativ kann natürlich auch das vorhandene WiFi oder Lan-Netzwerk genutzt werden.

Integration in bestehende Verwaltungssysteme

Sollte später eine Integration in bestehende ERP- oder andere übergeordnete Verwaltungssysteme gewünscht sein, lässt sich dies durch die automatisierte Datenerfassung einfach realisieren - auch nachträglich. Die jederzeit aktuellen, elektronisch erfassten und gespeicherten Daten sind flexibel per allen gängigen Schnittstellen und Protokollen übertragbar, und können auch direkt vor Ort automatisch verarbeitet werden. Im Falle eines LeanWave MEDICAB lassen sich aktuelle Bestandsdaten

beispielsweise über eine REST-Schnittstelle jederzeit automatisch an ein Verwaltungssystem übermitteln oder auch passiv abfragen.

Da die RFID-gestützte Datenerfassung in den meisten Fällen komplett ohne manuelle Eingriffe erfolgt, werden insgesamt die damit verbundenen Systeme autonomer und zuverlässiger, wodurch auch das Risiko sinkt, dass sich falsch erhobene Daten durch das Verwaltungssystem ausbreiten.

Wenn bereits ein Warenwirtschaftssystem auf Grundlage von Barcodes realisiert wurde, lässt sich in den meisten Fällen komplett ohne oder nur mit minimalen Änderungen eine Migration bestehender Systeme hin zu einem RFID-gestützten System realisieren. So lässt sich die Identifikationskennung, die in einem Barcode gespeichert sind, meist einfach direkt auf einem RFID-Transponder übertragen, wodurch nur die Lesepunkte ausgetauscht werden müssen. Das Lesen und Beschreiben der Transponder erfolgt dabei mindestens so mühelos wie das Drucken oder Lesen von Barcodes, wenn auf eine vollautomatische Warenerfassung verzichtet wird - bestehende Workflows, wie etwa das Lesen von Barcodes mit einem entsprechenden Handlesegerät, können so auch durch einen Wechsel auf RFID-Handlesegeräte beibehalten werden, wobei man trotzdem von der besseren Erfassung durch RFID profitiert.

Digitalisierung in der Prozessabläufen wird gefördert, wird gebraucht und ist zunehmend einfacher verfügbar. Jetzt ist ein guter Zeitpunkt auf die Technologie umzusteigen.



Karsten Otto, Otto ID Solutions

Enovacom bietet eine Integrationsplattform für Daten von Medizingeräte

Die Reise der Daten

Als Gesundheitsbranche innerhalb der Orange Gruppe hat sich Enovacom seit 20 Jahren als Spezialist für die Übertragung und den Austausch von Gesundheitsdaten in Europa einen Namen gemacht.

Was das Unternehmen nun auf den deutschen Markt treibt, haben uns Geschäftsführer Laurent Frigara, Fabrice Treziny, Outbound Sales Manager, und Mourad Zeghilet, Business Development Manager DACH, erläutert.

Wie genau sieht das Lösungsportfolio von Enovacom aus?

Laurent Frigara: Wir verstehen uns als Anbieter von Lösungen zur Interoperabilität der Informationssysteme im Gesundheitswesen. Als solcher verfolgen wir das Ziel, innovative Lösungen zu entwickeln, mit deren Unterstützung medizinische Fachkräfte den Versorgungspfad und die Patientenerfahrung verbessern können.

Was heißt das genau?

L. Frigara: Wir verfügen über jahrelange Erfahrung bei der Vernetzung von Software-Lösungen für Gesundheitseinrichtungen. In Frankreich sind wir Marktführer und zählen aktuell weltweit über 2000 Kunden. Denen stellen wir eine Interoperabilitätsplattform zur Verfügung, über die sie Informationen und Daten aus unterschiedlichsten Systemen ohne besondere Programmierkenntnisse austauschen können. Ein zweites, nicht minder wichtiges Standbein ist die Vernetzung von Medizingeräten. Da sorgen wir für die reibungslose Übertragung von Vitaldaten eines Patienten in seine elektronische Patientenakte.

In welchen europäischen Märkten sind Sie aktiv?

L. Frigara: Unser Hauptmarkt ist Frankreich, da haben wir einen Marktanteil von 60 Prozent mit unseren unterschiedlichen Lösungen. Daneben sind wir stark in England, Kanada, Belgien, Luxemburg, der Schweiz und neuerdings Finnland. Dort sind wir über einen Partner, einen bedeutenden Medizintechnikanbieter, an einem Riesenprojekt beteiligt und integrieren rund 1.600 Medizingeräte. In Deutschland haben wir nun auch erstes Interesse bei Kliniken geweckt.

Warum der Sprung auf den deutschen Gesundheitsmarkt?

Mourad Zeghilet: Zum Einsatz unserer Lösungen benötigen wir einen gewissen Grad der Digitalisierung, den Deutschland im Gesundheitswesen nun mit Macht anstrebt. Deutschland ist der größte Markt in Europa und mittlerweile reif, weil auch die Regierung mit dem Krankenhauszukunftsgesetz ein bedeutendes Investitionsprogramm gestartet hat.

Enovacom bietet Lösungen für Interoperabilität im Krankenhaus:

- eine Interoperabilitätsplattform für Informationssysteme
- eine Integrationsplattform für Daten von Medizingeräte
- ein Data Repository (Clinical Data Warehouse)



Laurent Frigara

Also hat auch das KHZG Sie bewogen, den Weg nach Deutschland zu gehen?

Fabrice Treziny: Nur sehr indirekt. Es geht nicht in erster Linie um Geld. Für die richtigen Lösungen ist immer Geld da. Vielmehr bemerken wir eine noch höhere Bereitschaft, sich mit Fragen der flächendeckenden Digitalisierung auseinanderzusetzen und den Rückstand der Krankenhäuser aufzuholen. Dazu wollen wir unseren Teil beitragen. Die Einrichtungen investieren derzeit in IT-Systeme und müssen demnach auch die Interoperabilität zwischen den verschiedenen Systemen herstellen. Da kommen wir dann ins Spiel.

Wie sieht Ihr Team in Deutschland aus?

M. Zeghilet: Im Vertrieb sind wir zurzeit zu viert, setzen aber auch auf starke Partner. Bei der Installation und dem Service unserer Lösungen beispielsweise unterstützt uns Maris Healthcare. Wir haben im Januar dieses Jahres begonnen, die deutschen Krankenhäuser zu kontaktieren und auszuloten, ob ein Bedarf für unsere Lösungen besteht. Die Rückmeldungen waren ermutigend.

Welches Feedback haben Sie bekommen?

F. Treziny: Neugierde, aber auch Furcht. Groß ist die Neugierde auf unsere Interoperabilitätslösung zur Integration von Geräten aus dem Patientenmonitoring: Patient Connect. Das gibt es in dieser Form in Deutschland noch nicht. Aus diesem Unbekannten erwächst aber auch die Furcht, ein derartiges Integrationsprojekt umzusetzen. Das kostet Zeit, bindet Ressourcen und stellt gewohnte Abläufe auf den Kopf.

Wie argumentieren Sie dagegen an?

F. Treziny: Indem wir die Lösung präsentieren und zeigen, wie einfach sie ist. Wir hören dann: „Wie schaffen wir das? Wir können nicht selbst programmieren.“ Nein, müssen Sie auch nicht. Jeder, der ein wenig Kenntnisse von Informatik hat, kann die Integrationsplattform einrichten und bedienen – auch ohne Programmierkenntnisse. Man kann sich das wie ein Formular vorstellen. Dort werden in einer Spalte die Systeme eingetragen, die ihre Daten mitsamt des Datenformats übertragen wollen, und in der anderen das System, das diese Daten empfängt. Unsere Plattform übernimmt dann die Übersetzung zwischen den Systemen und sorgt für einen nahtlosen Datentransfer.

Wo genau liegen die Vorteile für die Krankenhäuser?

F. Treziny: Ich verdeutliche das an einem Beispiel. Wenn ein Krankenhaus eine neue Software nutzen will, dann muss eine separate Schnittstelle mit dem Krankenhaus-Informationssystem programmiert werden – für jedes neue System wieder. Setzt die Einrichtung auf unsere Plattform, muss sie sie nur damit verlinken. Das geht schneller, ist billiger und zudem deutlich einfacher zu verwalten. Unsere Lösung erleichtert beispielsweise das Fehlermanagement. Heute ist es so, dass die Softwareanbieter bei Problemen im Datenaustausch gerne mit dem Finger auf den jeweils anderen zeigen. „Es liegt nicht an uns, hier ist alles in Ordnung. Der Fehler liegt beim anderen System.“ Unsere Plattform ist neutral, wir arbeiten mit allen Softwareanbietern und allen Geräther-



Mourad Zeghilet



Fabrice Treziny

stellern zusammen. Wir dokumentieren jeden Datentransfer und können Fehlerquellen genau benennen. Das erspart dem Anwender die aufwendige Analyse und lästige Diskussionen.

M. Zeghilet: Es gibt noch einen weiteren Vorteil. In den meisten Krankenhäusern herrscht Fachkräftemangel. Um dem zu begegnen, muss man entweder viel mehr Pflegepersonal einstellen und ausbilden oder die Prozesse im Klinikalltag weiter automatisieren. Genau das unterstützen wir mit einem reibungslosen Datenaustausch. Ein Beispiel: Während der Corona-Pandemie müssen sich die Pflegekräfte jedes Mal umziehen, wenn sie ein neues Zimmer betreten, um Vitalparameter zu notieren. Allein aufgrund der automatisierten Erfassung und Übertragung von Vitalparametern sparen sie bis zu einer Woche pro Jahr und Mitarbeiter.

Was meinen Sie, wie wird das deutsche Gesundheitswesen in fünf bis sieben Jahren aussehen?

F. Treziny: Die deutschen Gesundheitseinrichtungen werden sehr viel digitaler arbeiten als noch heute. Wenn die Deutschen sich etwas vornehmen, dann geben sie Vollgas und machen, was gemacht werden muss – nicht um gut oder besser zu werden, sondern um perfekt zu werden. Wenn sie starten, kann man sie nicht mehr halten. Und der Startschuss war das Krankenhauszukunftsgesetz. In vielleicht zehn Jahren wird Deutschland Frankreich und England in puncto Digitalisierung und Interoperabilität meines Erachtens hinter sich gelassen haben.

M. Zeghilet: Heute reden wir noch über Digitalisierung als automatische Dokumentation von Pflegeprozessen, eRezept, elektronische Patientenakte und solche Themen. Sehr schnell kommen dann aber auch Big Data, maschinelles Lernen und Künstliche Intelligenz dazu. Und auch da wird Deutschland dann schnell aufholen. Wir wollen Einrichtungen in die Lage versetzen, ein virtuelles Krankenhaus zu etablieren. Das würde dann einen reibungslosen und sicheren Datenaustausch zwischen verschiedenen Einrichtungen voraussetzen, um eine bessere, einfachere und schnellere Patientenversorgung zu gewährleisten.

Herr Frigara, Herr Treziny, Herr Zeghilet, vielen Dank für den spannenden Austausch.

Das Interview führte Ralf Buchholz.

Die Architektur der IT im Gesundheitswesen neu überdenken

Tomaž Gornik, Gründer und CEO, Better d.o.o.
Björn Lehnhoff, Geschäftsführer, Better Deutschland GmbH

Die Versorgung verlagert sich von der Akutversorgung in die ambulanten Bereiche und sogar nach Hause. Gleichzeitig fordern die Bürger mehr Kontrolle über ihre Gesundheit und ihr Wohlbefinden. Und schließlich hat die COVID-19-Pandemie die Gesundheits- und Pflegeorganisationen dazu gezwungen, die Innovation zu beschleunigen und neue Modelle der Leistungserbringung zu übernehmen. Dies alles hat viel Bewegung ausgelöst, die die Gesundheitsorganisationen dazu zwingt, auch die Architektur ihrer IT-Systeme zu überdenken.



Eine Verschiebung in der Pflegeversorgung

Fortschritte bei den klinischen Ansätzen und der Technologie, Verbraucher - die Bequemlichkeit wünschen und Kostenträger - die niedrigere Kosten fordern, beschleunigen die Verlagerung der Versorgung über die klinischen Sektoren hinaus. Gleichzeitig liegt der Schwerpunkt nicht mehr nur auf Krankheit und Behandlung, sondern vor allem auf Prävention und Wellness, was die Verlagerung der Versorgung weg vom Krankenhaus noch verstärkt. Leider wurden die heute verwendeten IT-Systeme für Institutionen und nicht für Patienten entwickelt und können diese neuen Anforderungen nur schwerlich erfüllen.

Engagierte und befähigte Patienten

Der bessere Zugang zu Gesundheitsinformationen ermöglicht es den Patienten, zukünftig selbst eine wichtigere Rolle für

ihre Gesundheit und ihr Wohlbefinden zu spielen. Die Leistungserbringer geben den Patienten aktiv die Möglichkeit, die Verantwortung für das Management ihrer Krankheiten mitzutragen, um die medizinischen Ergebnisse zu verbessern und die Kosten zu senken. Infolgedessen verlangen die Patienten jetzt bequeme und personalisierte Dienstleistungen, was eine große Herausforderung für die derzeitigen IT-Systeme darstellt. Die meisten Gesundheitsdienstleister haben Schwierigkeiten, mit diesen Anforderungen Schritt zu halten, was den Rückstau an nicht gelieferten Lösungen noch vergrößert.

Die COVID-19-Pandemie

Das Gesundheitswesen ist einer der letzten großen Wirtschaftszweige, der sich digitale Technologien zu eigen machen muss, aber die COVID-19-Pandemie hat die Einführung zahlreicher digitaler Anwendungen im Gesundheitswesen, wie Telemedizin und Fernüberwachung, beschleunigt. Es wurde schnell sehr deutlich, dass in einer Krise wie dieser, zugängliche, qualitativ hochwertige Daten ein entscheidender Faktor sind. Und dass Gesundheitsdaten exponentiell leistungsfähiger sind, wenn sie vernetzt, kombiniert und gemeinsam genutzt werden. Dies sind alles Trends, die schon vorher zu beobachten waren, die aber durch die Pandemie erheblich beschleunigt wurden.

Bestehende Lösungen behindern den Wandel und schwächen das Gesundheitssystem

In einem Papier der Mayo Clinic¹ wurde dargelegt, wie die IT den Anforderungen der Pflegeteams nicht gerecht wird: "Die Benutzerfreundlichkeit aktueller EHR-Systeme wurde von den Ärzten mit der Note 'F' ≤ 59 % Zufriedenheit bewertet, wenn sie eine standardisierte Metrik für die Benutzerfreundlichkeit der Technologie verwendeten. Es wurde eine starke Ursache-Wirkungs-Beziehung zwischen der Benutzerfreundlichkeit von EHR-Systemen und der Wahrscheinlichkeit eines Burnouts beobachtet." In ähnlicher Weise² heißt es in einer aktuellen Studie der Gartner Group: "Mit unflexiblen IT-Portfolios löst sich die Fähigkeit zur geschäftlichen Differenzierung auf und die Kapazität für Innovation und Agilität schrumpft. Monolithische und unwirtschaftliche Lösungen für elektronische Gesundheitsakten (EHR) behindern heute die Bemühungen vieler Organisationen im Gesundheitswesen um digitale Transformation. Die Unzufriedenheit mit monolithischen EHR-Systemen und deren Unfähigkeit, schnell zu reagieren und neue klinische und regulatorische Anforderungen zu unterstützen, war noch nie so offensichtlich wie heute." Dem stimme ich vollkommen zu!



Eine Architektur für die Zukunft

Um die oben genannten Probleme zu lösen, muss die IT-Architektur auf einer offenen Plattform beruhen, die ein klinisches Datenarchiv und die erforderlichen Werkzeuge zur Beschleunigung der Entwicklung neuer Anwendungen umfasst. Diese Ansicht wird inzwischen von führenden Beratungsunternehmen wie Ernst & Young (EY) und der Gartner Group geteilt. Die von ihnen vorgeschlagene Architektur basiert auf einer gemeinsamen Datenebene, einem Inventar von Anwendungen und APIs sowie den Tools, die für eine schnelle Zusammenstellung personalisierter Anwendungserfahrungen erforderlich sind.

Sowohl EY³ als auch Gartner⁴ sind sich über drei grundlegende Prinzipien für die Architektur der Zukunft einig: ein einheitliches Anwendungserlebnis, die flexible Bereitstellung von Anwendungen auf der Grundlage eines herstellerneutralen Datenkerns. Werfen wir einen genaueren Blick darauf.

Ein einheitliches Anwendungserlebnis

Die derzeitige Frustration der Pflegeteams mit den aktuellen IT-Systemen ist gut dokumentiert. Diese Pflegekräfte nutzen intuitive, personalisierte und effiziente Anwendungen in ihrem Privatleben und erwarten nicht weniger von den Systemen, die sie bei ihrer Arbeit unterstützen sollen. Gartners Lösung ist ein Modell des Anwendungsdesigns, das Anwendungen als Erfahrungen versteht, die von oder für ihre Benutzer zusammengestellt werden. Der Hauptvorteil ist die Personalisierung: Funktionen und Fähigkeiten, die auf die Besonderheiten des Pflegeteams, des Patienten und der Pflegeumgebung zugeschnitten sind. Das Hinzufügen eines Designsystems ist notwendig, um die Konsistenz der Benutzererfahrung über verschiedene Module hinweg zu erreichen.

Die flexible Bereitstellung von Anwendungen

Im Zuge des digitalen Wandels der Unternehmen wird Software immer strategischer und allgegenwärtiger. Die Nachfrage nach neuen und aktualisierten Anwendungen explodiert förmlich, und

Fachleute, die solche Software entwickeln und betreiben können, sind Mangelware. Um dies abzumildern, haben andere Branchen den Low-Code-Ansatz übernommen, um die Bereitstellung von Anwendungen zu beschleunigen und den Rückstand zu verringern. Neben Softwareingenieuren treten auch Endbenutzer als "Bürgerentwickler" auf, die über das nötige Fachwissen verfügen, um mit Low-Code-Tools schnell die gewünschte Anwendung zu erstellen. Auch hier ist das Gesundheitswesen im Rückstand, aber dieser Ansatz ist eine der wenigen Möglichkeiten, die es hat. Um es klar zu sagen: Die Hauptarbeit wird weiterhin von Software geleistet, die von professionellen Entwicklern geschrieben wird. Mit der Weiterentwicklung neuer Tools werden diese Entwickler jedoch hauptsächlich die komplexeren Funktionen und Möglichkeiten übernehmen.

Ein herstellerneutraler Datenkern

In dem Maße, wie die Pflege aus dem Krankenhaus verlagert wird, müssen die Daten rund um den Patienten gespeichert werden. Leider speichern die derzeitigen Systeme, die für Institutionen

entwickelt wurden, Daten in proprietären Formaten. Dadurch entstehen Silos, die die Datenfluktuation verhindern und die allgemeine Nutzung der Daten erschweren. Künftige Anwendungen, Apps und Algorithmen werden auf einem herstellerneutralen klinischen Datenspeicher basieren, der eine longitudinale Patientenakte von der Wiege bis zur Bahre bietet und als einzige Quelle der "Wahrheit" für die gesamte Lebensdauer des Patienten dient. Solange die Daten eng mit den Anwendungen gekoppelt sind, wie bei den heutigen führenden EHRs, werden wir nur schrittweise Verbesserungen erzielen können.

Wie kommen wir dahin?

Ich habe noch nie CIOs aus dem Gesundheitswesen getroffen, die keine Gesundheitsdaten in einem offenen Format haben wollten. Die Frage war immer die folgende: Wo kann ich Anwendungen kaufen, die diesen Ansatz bieten? Die gute Nachricht ist, dass viele Anbieter jetzt openEHR übernehmen, um die Daten von den Anwendungen zu trennen und sie in einem offenen, anbieterneutralen Format zu speichern.

Dieser Wandel ist nun auch auf den Märkten mit den fortschrittlichsten Gesundheitssystemen zu beobachten. Alle vier führenden nordischen Anbieter von EHR-Systemen - die norwegischen Unternehmen DIPS und PatientSky, das schwedische Unternehmen Cambio und das finnische Unternehmen TietoEvy - verwenden jetzt ein auf openEHR basierendes Datenrepository. Ganze Städte (Moskau) und sogar Nationen (Finnland, Malta, Schottland, Slowenien und Wales) stützen ihre Gesundheitsdateninfrastruktur inzwischen auf openEHR. Dieses Jahr hat Katalonien beschlossen, dasselbe zu tun.

In Deutschland hat sich das Medizininformatik-Konsortium HiGHmed, bestehend aus 8 Universitätskliniken und einem großen Akkutversorger für die openEHR-Datenplattform entschieden, um die unternehmensübergreifende Versorgung und Forschung zu verbessern. Die definierten Ziele „sind eng verbunden mit der Herausforderung, Lösungen innovativer, international interoperabler Datenintegration und Methoden zu integrieren und weiterzuentwickeln, um deren Mehrwert für die Gesundheitsforschung und auch die Patientenversorgung aufzuzeigen.“⁵

Das klinische Datenspeichersystem Better Platform bietet die Grundlage für einen sinnvollen Datenaustausch innerhalb des Konsortiums und darüber hinaus.

"Das Wichtige daran ist, dass wir nicht nur Forschungsdaten, sondern auch die klinischen Anwendungen, die wir auf offenen Schnittstellen aufbauen, gemeinsam nutzen können. So entsteht ein Ökosystem von Anwendungen, und das war während der Pandemie sehr praktisch, weil wir nicht nur die Daten, sondern auch die Anwendungen austauschen können, zum Beispiel das intelligente Infektionskontrollsystem", sagte Michael Marscholke, Professor für Medizinische Informatik an

der Medizinischen Hochschule Hannover und geschäftsführender Direktor des Peter L. Reichertz-Instituts für Medizinische Informatik der TU-Braunschweig und der Medizinischen Hochschule Hannover.⁶

Viele dieser Bereiche sind sehr fortschrittlich und verfügen über jahrzehntelange Erfahrung in der Erhebung hochwertiger Pflegedaten, weshalb sie die Grenzen der derzeitigen Ansätze kennen.

Natürlich wissen wir, dass die derzeitigen Systeme nur schwer zu ersetzen sind. Alle neuen Architekturen werden noch eine ganze Weile mit Altsystemen koexistieren müssen. Die postmoderne elektronische Patientenakte⁷ ist also eine Möglichkeit, die Reise in die Zukunft schon heute zu beginnen, ohne die bestehenden Systeme zu ersetzen. Sie ist perfekt auf den bimodalen IT-Ansatz abgestimmt, der Agilität und Innovation mit Stabilität kombiniert, um das Geschäft gleichzeitig am Laufen zu halten.

Sicherheit und Datenschutz

Gesundheitsdaten müssen als ein äußerst wichtiges Gut anerkannt werden, und ihre Sicherheit und der Schutz der Privatsphäre der Patienten sollten oberste Priorität haben. Deshalb muss ich darauf hinweisen, dass offene Daten nicht gleichbedeutend mit offenem Zugang sind. Offene Datenplattformen (wie openEHR) bieten einen kontrollierten und klar definierten Zugang zu den Daten entsprechend den Richtlinien der einzelnen Organisationen. Darüber hinaus ermöglichen ihre Funktionen und Maßnahmen den Organisationen des Gesundheitswesens, die größtmögliche Sicherheit für die Daten ihrer Patienten zu gewährleisten. Außerdem bieten offene Datenlösungen einen vollständigen Prüfpfad für jeden Benutzer - alle Zugriffe und Aktionen werden nachverfolgt und sicher auf einem separaten Server gespeichert und können überprüft werden.

Zusammenfassung

Eine neue Informationsarchitektur ist der Schlüssel zur Entfaltung der Leistungsfähigkeit digitaler Technologien und zur Schaffung des vernetzten Gesundheitssystems von morgen. Die heutigen Lösungen koppeln Daten eng an ihre Anwendungen. Da Gesundheits- und Pflegedaten lebenslang sind, müssen sie die Anwendungen überdauern, so dass eine klare Trennung zwischen beiden erforderlich ist. Die Architekturen der Zukunft werden eine herstellerneutrale Datenschicht im Zentrum haben, Low-Code-Tools zur Beschleunigung der Anwendungsbereitstellung und auf den Benutzer zugeschnittene Anwendungserlebnisse. Um die Kluft zwischen dem heutigen und dem künftigen Zustand zu überbrücken, müssen alte EHRs und neue, auf offenen Plattformen basierende Systeme nebeneinander bestehen können, was Innovationen während des Übergangsprozesses ermöglicht.



Better



"I am very excited that our subsidiary in Germany is finally open, with our team of four colleagues already supporting our current German customers."



Tomaž Gornik
CEO, Better

Better Deutschland GmbH
Ballindamm 39
20095 Hamburg



Was ist openEHR?

OpenEHR ist eine offene Spezifikation für standardisierte Gesundheitsinformationen. Sie ermöglicht es uns, andere Anwendungen darauf aufzubauen und unterstützt das offene Plattform-Ökosystem. Darüber hinaus besteht die openEHR-Gemeinschaft aus Hunderten von Modellierern (Klinikern) aus 101 Ländern weltweit, die Datenmodelle erstellt haben, die quelloffen und frei nutzbar sind.

OpenEHR wurde bereits in Hunderten von Installationen weltweit getestet und bewährt. Hier sind fünf verschiedene Anwendungsfälle, in denen openEHR eingesetzt wurde:

- eine Gesundheitsdatenplattform für elektronische Gesundheitsakten, Anwendungen und einen gemeinsamen Datenspeicher,
- für Regierungen und eHealth-Programme,
- für Forschung und klinische Entscheidungshilfe,
- als ein Rahmen für klinische Register,
- für ganze Ökosysteme von Gesundheitsanwendungen und -diensten.

Über Better

Better ist der marktführende Anbieter einer offenen Datenplattform für das Gesundheitswesen. Das Unternehmen hat die Better Deutschland GmbH im Sommer 2021 gegründet und

unterstreicht damit sein Engagement, den sich schnell entwickelnden Bedürfnissen der Gesundheitsorganisationen in Deutschland gerecht zu werden. Um den bestehenden und neuen Kunden in Deutschland den bestmöglichen Service zu bieten, steht ein lokales Team von Digital-Health-Experten unter der Leitung des Geschäftsführers Björn Lehnhoff zur Verfügung.

Als Europäisches Unternehmen arbeitet Better mit mehr als 150 Kunden in 16 Märkten zusammen und bietet digitale Gesundheitslösungen an, die klinischen Teams helfen, ihre Arbeitsprozesse zu vereinfachen und die Patientenversorgung und die Ergebnisse zu verbessern. Zu den Kunden gehören das HiGHmed-Konsortium in Deutschland, die Stadt Moskau und mehr als 30 NHS Trusts im Vereinigten Königreich, sowie die Gesundheitsverwaltungen von Slowenien und Malta.

Wenn Sie mehr darüber erfahren möchten, wie der Open-Data-Ansatz dazu beitragen kann, die Arbeit medizinischer Teams zu verbessern, treffen Sie die Vertreter von Better auf den folgenden Veranstaltungen 2021:

- 14. Okt. - HIGHmed Symposium, Berlin/hybrid
- 25. Okt. - Deutscher Interoperabilitätstag, online
- 7./8. Dez. - Das Digitale Krankenhaus, München

1 The Association Between Perceived Electronic Health Record Usability and Professional Burnout Among US Physicians, abgerufen am 5. September unter: <https://www.mayoclinicproceedings.org/article/S0025-6196%2819%2930836-5/fulltext>

2 Predicts 2021: Healthcare Providers Must Accelerate Digital Transformation to Address Disruption, abgerufen am 5. September 2021 unter: <https://www.gartner.com/document/3993573?ref=solrAll&refval=299660984> (Registrierung notwendig)

3 As technology becomes smarter, is your hospital keeping up?, abgerufen am 5. September 2021 unter: https://www.ey.com/en_gl/health/as-technology-become-smarter-is-your-hospital-keeping-up

4 Gartner, Hype Cycle for Healthcare Providers, 2020, Laura Craft, Mike Jones. Veröffentlicht am 5. August 2020

5 openEHR - open data platforms in medical informatics, eine Broschüre, die von HiGHmed im Juni 2018 veröffentlicht wurde

6 Vortrag auf der Week of eHealth - Data spaces and digital transformation in healthcare, 31. August 2021, Ljubljana, Slowenien

7 The Postmodern EHR: What are the enablers?, abgerufen am 5. September 2021 unter: <https://blog.better.care/2016/01/29/the-postmodern-ehr-what-are-the-enabler>





MEDIX-CARE ermöglicht eine intelligente Patient Journey

Patientenportal Plus

Das Krankenhauszukunftsgesetz (KHZG) definiert ein Patientenportal als Instrument, das „ein digitales Aufnahme- und Entlassmanagement sowie das Überleitungsmanagement von Patientinnen und Patienten zu nachgelagerten Leistungserbringern ermöglicht.“ Was wäre, wenn es aber zahlreiche zusätzliche Interaktionsmöglichkeiten sowie ein Patientenentertainment und die Möglichkeit der Patientenbeteiligung über ein Bedside-Terminal bieten würde? Dann wäre es MEDIX-CARE. Die Plattform des gleichnamigen Unternehmens deckt nicht nur alle Muss- und Kann-Kriterien des Fördertatbestandes 2 des KHZG ab, sondern geht noch darüber hinaus.

So sieht eine intelligente Patient Journey aus

Die Reise des Patienten durch das Krankenhaus – anberaumt ist ein operativer Eingriff – beginnt bereits vor der stationären Aufnahme, genau gesagt: zwei Tage vorher. Da bekommt er einen Einladungsbrief mit einem QR-Code, den er einscannt, um dann online die Aufnahmeformalitäten zu erledigen, Anamnesebögen auszufüllen, Wahlleistungen zu buchen und Essen auszuwählen. Darüber hinaus findet er Informationsblätter und -videos zu seiner Behandlung. „Durch den Online-Check-in werden die Mitarbeiter in der Aufnahme entlastet, genauso durch die Auswahl von Wahlleistungen und des Essens. Die Aufklärungsvideos dagegen ersparen den Pflegekräften Zeit“, erläutert Bernd Jaskotka aus der Geschäftsleitung von MEDIX-CARE den Wert für das Krankenhaus.

Kommt der Patient dann in die Klinik, checkt er sich an einem speziellen Kiosksystem im Eingangsbereich oder via QR-Code mit seinem Smartphone ein. Danach wird er automatisch zur Indoor-Navigation weitergeleitet, die ihn auf die richtige Station führt. „So wird eine hohe Arbeitslast von der Anmeldung und dem Hol- und Bringdienst genommen“, sagt Jaskotka.

Hat sich der Patient in seinem Zimmer eingerichtet, stehen diverse Untersuchungen an. In gestaffelten, individuell zu definierenden Abständen wird er per Nachricht in der Journi App oder auf dem Bedside-Terminal daran erinnert. Das reduziert die Wartezeiten für den Patienten und eliminiert Leerläufe im klinischen Workflow.

Vor bestimmten diagnostischen Verfahren muss der Patient einige Dinge beachten. Diese Verhaltensregeln schickt

ihm das System samt Termin-Erinnerungen auf sein persönliches Endgerät oder das Bedside-Terminal. „In bestimmten Paketen erhält er Terminerinnerungen und Aufklärungsvideos zur Behandlung. Gleichzeitig hat er die Möglichkeit, direkt um Hilfe zu bitten“, ergänzt Jaskotka.

Entertainment und mehr

Nach der OP ist dem Patienten Bettruhe verordnet. Ablenkung bietet ihm das Bedside-Terminal oder sein Tablet. Darauf kann er Fernsehen und Videos schauen, Radio und Musik hören, im Internet surfen oder sich ein Wunschmenü wählen. Es dient aber auch der Information zu seiner Krankheit und Behandlung, dem Austausch mit Ärzten und Pflegekräften sowie der Dokumentation seines Heilungsprozesses – und zwar in vielfältiger Weise.

Die Patientenaufnahme beginnt bereits zuhause, etwa um online die Aufnahmeformalitäten zu erledigen, Anamnesebögen auszufüllen, Wahlleistungen zu buchen, Essen auszuwählen und sich zu informieren.



Ein Service sind die bereits erwähnten Aufklärungsbögen und -videos, ein anderer ist die sogenannte digitale Klingel. Damit ruft der Patient beispielsweise eine Pflegekraft oder gibt eine „Bestellung“ auf, etwa eine Decke oder ein Glas Wasser. Diese Nachricht erscheint direkt auf dem Smartphone oder Tablet der Pflegekraft und kann abgearbeitet werden, ohne erst in das Zimmer zu gehen und den Patienten zu fragen, was er wünscht.

Des Weiteren kann der Patient am Bedside-Terminal mit Sprach- und Textnotizen sein Behandlungstagebuch führen. Alle genannten Maßnahmen erhöhen die Patientenzufriedenheit und reduzieren den Aufwand für das Klinikpersonal.

„Wir binden unsere Anwendung in die vorhandene Infrastruktur des Klinikums in das klassische Patientenentertainment ein und erweitern die Möglichkeiten. Das bedarf also keiner zusätzlichen Beschaffung und ist einfach gemacht“, erläutert Bernd Jaskotka.

Nach der OP ist vor der Entlassung

Ist die OP gut überstanden, stehen gleich Nachuntersuchungen und die ersten Rehamassnahmen an. Diese wurden vorher terminiert und dem Patienten

mitgeteilt. Mit einem Klick auf die Wegbeschreibung mittels Indoor-Navigation kann er sich zum Untersuchungs- oder Therapieraum führen lassen. Dadurch wird der Hol- und Bringdienst des Hauses entlastet.

Durch die kontinuierliche Einbindung der Patienten durch die MEDIX-CARE Plattform werden alle Behandlungs- und Pflegeprozesse effizienter und verbessert.

Nach der Entlassung stehen dem Patienten dann alle wichtigen Informationen und Dokumente in seiner Journi App zur Verfügung. Wenn der Patient es möchte, werden die Unterlagen auch den Zuweisern sowie weiterbehandelnden Fachärzten und Einrichtungen zur Verfügung gestellt. Über die App bleibt der Patient auch nach seiner Entlassung für Fragen und eine weitergehende Begleitung mit dem Ärzte- und Therapeutenteam in Kontakt.

Internationale Erfahrung

Weltweit arbeiten gegenwärtig mehr als 80 Krankenhäuser mit MEDIX-CARE. Neben der ständig wachsenden Anzahl ausländischer Kliniken werden auch immer mehr Kliniken in Deutschland mit MEDIX-CARE ausgestattet. Zusätzlich werden auch die ersten deutschen KI-Anwendungen implementiert.

„MEDIX-CARE ist eine smarte Gesamtlösung aus einer Hand, die hoch skalierbar ist, sich leicht implementieren lässt und mit den individuellen Anforderungen einer Einrichtung wachsen kann“, sagt Bernd Jaskotka. „Durch nationale und internationale Anforderungen hinsichtlich Funktionalitäten und Systemintegration ist die Plattform sehr schnell gewachsen. Wir können sicher mit Fug und Recht behaupten, dass wir heute den breitesten Funktionsumfang bieten.“

Wichtig sind dem Geschäftsleitungsmitglied die Offenheit und Interoperabilität der Plattform. Systeme, die bereits im Hause implementiert sind, können genauso wie später hinzukommende Fremdsysteme problemlos über gängige Schnittstellen wie HL7, IHE und FHIR angebunden werden. Ein DSGVO-konformer Austausch aller Daten ist selbstverständlich.

„Wir stellen fest, dass sich mit MEDIX-CARE die Rehospitalisierungen verringern lassen. Darüber hinaus verkürzt sich die Aufenthaltsdauer bei einer gleichzeitig steigenden Patientenzufriedenheit. Das alles ergibt eine hohe Effizienzsteigerung“, blickt Bernd Jaskotka nicht ohne Stolz auf eine erfolgreiche Bilanz der Patient Journey mit MEDIX-CARE.



Snom: Wenn das IP-Telefon für lebensrettende Zeitersparnis sorgt

In Krankenhäusern ist der Wettlauf gegen die Zeit ein alltäglicher Umstand. Snom zeigt auf, welche Vorteile die Optimierung der Krankenhauskommunikation mit sich bringt.

Gerade in Gesundheitseinrichtungen ist eine reibungslose Kommunikation essenziell und sollte auf keinen Fall bei der Umsetzung von Optimierungsmaßnahmen zu kurz kommen: Flexibel einsetzbare Arbeitsmittel sind unerlässlich für jedwede Optimierung, umso mehr in einer hygiene- und zeitkritischen Umgebung.

Der weltweit etablierte Hersteller von Premium-IP-Telefonen Snom erklärt am Beispiel seiner Projekterfahrung im Krankenhausumfeld, wie schnurlose IP-DECT-Telefone konkret dem Personal zu einer relevanten Zeitersparnis verhelfen: Der zuständige Arzt lässt sich über sein Snom-IP-DECT-Telefon kontaktieren und unmittelbar zur richtigen Station beordern, Alarmer werden per Knopfdruck ausgelöst, und das Personal muss sich nicht mehr aufwendig an- und abmelden. Der entsprechende automatische Eintrag in die digitale Zeitkarte und in das Telefonie-System erfolgt durch Betätigen einer Taste. Sollten nun interne sowie externe Anrufe eingehen, werden sie an andere diensthabende Kollegen automatisch durchgestellt.

Zum idealen Umfeld für eine schnelle Genesung gehört natürlich auch die Sauberkeit der Räume. So können Pflegekräfte über das Telefon per Tastendruck signalisieren, dass das Zimmer oder der OP-Saal gerade nicht belegt ist und gereinigt werden muss. Die Reinigungskräfte werden automatisch über ihr DECT-Telefon benachrichtigt und können nach erfolgter Reinigung den Status des Raums ebenfalls per Funktionstaste aktualisieren.

Doch nicht nur damit lässt sich (lebensrettende) Zeit sparen: Die Weiteilufigkeit von Krankenhäusern ist eine weitere Herausforderung. Dank der Integration von Beacons und Tags in Chipgröße sind mobile Arbeitsgeräte metergenau zu lokalisieren. Damit wird die zeitaufwendige Suche nach dem nächsten Rettungs-Kit, Ultraschall- und Blutdruckmessgerät, einem Rollstuhl oder gar einem Krankenhausbett für den hausinternen Transport von Patienten vermieden. Die Snom DECT Einzel- wie Multizellenlösungen sorgen dabei für eine außerordentlich gute Reichweite des DECT-Signals im gesamten

Gebäude, selbst unter den widrigsten baulichen Umständen.

Zu guter Letzt: Nicht nur in Pandemie-Zeiten ist die Hygiene Maßstab aller Dinge im Krankenhaus. Dem trägt der VoIP-Spezialist Snom Rechnung mit seinem IP-DECT-Telefon M90. Das Modell wurde speziell für hygiene-kritische Umgebungen konzipiert und weist als weltweit erstes schnurloses Telefon ein antibakterielles Gehäuse auf, das obendrein nach JIS Z2801 getestet wurde. Damit lässt sich das Gerät nicht nur einfach mit Ethanol-haltigen Desinfizierungsmitteln reinigen, sondern bietet auch keinen Nährboden für Bakterien und Viren. Neben dem speziellen Überzug ist das Telefon außerdem nach IP65 zertifiziert. Stürze aus bis zu 2 m sind ebenfalls kein Problem. Damit wird das kleine, ca. 130 g leichte und handliche Gerät zum perfekten Begleiter im Klinikalltag.

Eine gute Patientenversorgung fängt mit der Anamnese an.

Mit E-ConsentPro connect können Patienten über Ihr Patientenportal die Anamnesedaten bereits zuhause erfassen, sich auf den Eingriff vorbereiten und Ihnen die Daten frühzeitig zur Verfügung stellen.



KHZG
förderfähig

www.thieme-compliance.de/e-consentpro-connect

© bonkam/stock.adobe.com



Intelligente Verbindungen.
Auf höchstem Niveau.