www.medizin-edv.de ISSN 1619-0629 Preis: 12 Euro

Ausgabe 6 / 2019

Krankenhaus-IT JOURNAL

Fakten und Perspektiven der IT im Gesundheitswesen

Elektronische Patientenakte

startklar machen

it-sa

Special ab Seite 84

KH IT Bundesverband der Krankenhaus IT-Leiterinnen / Leiter e. V.

ENTSCHEIDERFABRIK

HL7 IHE DEUTSCHLAND Integrating the Healthcare Enterprise

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

Auch riskante Chancen richtig nutzen

Spätestens 2021 müssen Krankenkassen ihren Versicherten eine elektronische Patientenakte (ePA) zur Verfügung stellen. Durch diese Digitalisierung sollen lebenswichtige Informationen schnell verfügbar und Doppeluntersuchungen vermieden werden.

Das spart Zeit und Geld. Das Ganze ist keine Zukunftsmusik, sondern fast ein alter Hut und schon vor gut anderthalb Jahrzehnten unter der damaligen Bundesgesundheitsministerin Ulla Schmidt formuliert worden. Seitdem dümpelt das ehrgeizige Projekt mehr oder weniger vor sich hin, die Beteiligten auf allen Seiten schoben und schieben sich gegenseitig den schwarzen Peter zu. Einige Krankenkassen entwickelten schon mal ihre eigenen elektronischen Patientenakten, die elektronischen Gesundheitsakten (eGA), nutzbar über bestimmte Apps und mobile Endgeräte. Auch in die Politik scheint nun ein plötzlicher Energie- und Aktivitätsschub gekommen zu sein, nun gilt es, diesen in die richtigen Bahnen zu lenken. Doch da gibt es - mal wieder - unterschiedliche Wegbeschreibungen. Insellösungen sollten vermieden werden und die Sicherheit hat oberste Priorität, handelt es sich doch um extrem sensible Daten! Dass IT-Sicherheit ein großes Thema ist, besonders auch in Einrichtungen des Gesundheitswesens angesichts der aktuellen Hackerangriffe, hat auch die Sicherheitsfachmesse it-sa in Nürnberg wieder gezeigt. In unserem Special im „IT-Sicherheit im Krankenhaus" zeigen wir ab S. 80, welche Lösungen und Strategien bereits am Markt sind, um entsprechende IT-Sicherheit zu geben.

Und die Sicherheit bezüglich der Nutzung elektronischer Patientendaten wird letztendlich auch über deren Erfolg bestimmen. Bei den Rahmenbedingungen scheinen hier noch nicht alle an einem Strang zu ziehen, das verzögert die Einführung der elektronischen Patientenakte und somit den Fortschritt der Digitalisierung.

Die Chancen der Digitalisierung müssen genutzt werden, um die Qualität einer umfassenden Gesundheitsversorgung zu steigern, auch wenn es keine 100%ige Sicherheit geben kann. Und laut einer repräsentativen Umfrage des IT-Branchenverbands Bitkom im Mai dieses Jahres befürworten ja schon 65% der Befragten die Nutzung einer elektronischen Patientenakte.

Wie sieht also die Zukunft aus? Damit beschäftigt sich auch das neue Buchprojekt „Die Health-IT der Zukunft" (siehe S. 42). Es bleibt durchaus spannend!
Doch es gibt noch viel zu tun….

Herzliche Grüße, Dagmar Finlayson

Dagmar Finlayson

Hartmuth Wehrs

Kim Wehrs

Impressum
Antares Computer Verlag GmbH,
Gießener Straße 4, D-63128 Dietzenbach
E-Mail: antares@medizin-edv.de, www.medizin-edv.de
Verlagsleitung und Herausgeber **Hartmuth Wehrs (hw)**,
stellvertr. **Kim Wehrs (kw)**. Tel.:0 60 74/25 35 8, Fax:0 60 74/2 47 86
Redaktion, Chefredakteurin **Dagmar Finlayson (df)** (verantwortlich) 0 60 74/25 35 8
Mitglied der Chefredaktion **Wolf-Dietrich Lorenz**, Berlin
Redaktionelle Mitarbeit **Kai Wehrs** (Fotos und Onlineredaktion) (kaw)
Anzeigen + Verkauf **Kim Wehrs**, D-63128 Dietzenbach, Tel.:0 60 74/2 53 58 (kw)
Layout, Grafik, & Satz **Nebil Abdulgadir**
Lektorat **Maike Buchholz,** Jügesheim
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
S 1, 10, 14 Adobe Stock; S. 29 SoCura; S. 40 Härdtner; S 44, 45 Uslu; S. 47 Bundesdruckerei; S. 48 Intersystems; S. 52, 53 Entscheiderfabrik; S. 54, 55 Lorenz; S. 56, 57 Prosystems; S. 61 Adobe Stock; S. 63 Heydt-Gruppe; S. 64, 65 Agfa HealthCare; S. 66 Maerz AG; S. 68 Nuance; S. 73 Messe Nürnberg; S. 74 Rohde & Schwarz; S. 76 NTT; S. 79 Red Eagle; S. 80 Allegro; S. 81 Axis; S. 82 AlgoSec; S. 83 Check Point Software; S. 86 Forcepoint; S. 92 sayTEC; S. 93 Cryptshare; S. 96, 97 Seculution.

Titelthema

IT-Management

48

Verbandsseiten KH-IT

Neue Medien

Veranstaltungen

Aus dem Markt

74

IT-Sicherheit im Krankenhaus

it-sa Rückblick

Was bei der Digitalisierung im Gesundheitswesen nicht passieren darf

Elektronische Patientenakte

Jeder Mensch ist auch irgendwann einmal Patient. Gerade Menschen mit chronischen oder stigmatisierten Erkrankungen sind die verwundbarsten Mitglieder unserer Gesellschaft. Für Forschungszwecke auf Daten dieser Gruppen zuzugreifen ist zwar sinnvoll und mag langfristig dem Allgemeinwohl dienen, muss aber einhergehen mit einem hohen Schutzniveau der Privatsphäre jedes einzelnen Betroffenen. Ein Zustand der Sustainable Cyber Resilience muss das Ziel sein.

Die elektronische Patientenakte (ePA) steht jedem Versicherten ab Januar 2021 zur Verfügung. Sie ist das zentrale Element der vernetzten Gesundheitsversorgung und der Telematikinfrastruktur und speichert Informationen des Patienten zu Befunden, Diagnosen, Therapiemaßnahmen und Behandlungsplänen. Auch wurde gerade das Gesetz zur Digitalen Versorgung (DVG) im Bundestag verabschiedet. Diese Gesetze und weitere Ansätze zur Digitalisierung im Gesundheitswesen stehen und fallen mit dem Vertrauen der Versicherten in die Sicherheit ihrer Daten. Ein Grundvertrauen der Versicherten in die ePA und in die Ziele des DVG kann jedoch nur mit einer radikalen Transparenz der Datennutzung und Abläufe erarbeitet werden.

Transparenz ermöglicht Cyber Resilience

Die Anzahl der Beteiligten in einem Netzwerk von Datenerfassungspunkten (Arztpraxen), Verarbeitungsknoten (Krankenversicherungen) und Lesestationen (die App des Versicherten), wie sie bei der ePA anfallen, macht das gesamte System komplex. Dementsprechend groß wird die Angriffsfläche für IT-Sicherheitsvorfälle. Wie eine fehlerhafte oder unsichere Installation beziehungsweise Konfiguration der Systeme zur Ursache für ein Datenleck führen kann, haben zahlreiche Beispiele in der jüngeren Vergangenheit gezeigt. Um Fehler bei der Installation oder Konfiguration zu vermeiden, muss für jeden Beteiligten definiert sein, welche Maßnahmen der Informationssicherheit verpflichtend für die Abläufe der Datenverarbeitung anzuwenden sind und welche Grenzen für die Verarbeitung der Daten gelten. Nur durch klare Richtlinien kann die digitale Erfassung von Gesundheitsdaten auch sicher und widerstandsfähig gegenüber Akteuren mit bösen Absichten gemacht werden.

Die digitale Angriffsfläche im Blick zu haben und sie so gering wie möglich zu halten, wird daher die Kernaufgabe aller Beteiligten sein. Sie müssen die Cyber Resilience, die digitale Widerstandsfähigkeit ihrer IT-Systeme, auf ein vertrauenswürdiges Niveau heben und halten. Versicherer und Lösungsanbieter müssen dafür ihre Abläufe transparent darstellen und die dazu genutzten IT-Systeme klar zuordnen können. Denn nur so können diese mit technischen Maßnahmen abgesichert und regelmäßig und automatisch auf ihre Widerstandfähigkeit gegen Angriffe überprüft werden.

Informationssicherheit nicht vernachlässigen

Pseudonymisierung beziehungsweise eine Anonymisierung der Informationen im Gesundheitsbereich ist ein generelles Muss. An einigen sensiblen Stellen sind diese Verfahren jedoch nicht gut genug, da die Technik zur De-Anonymisierung weit fortgeschritten ist. So können veröffentlichte Bilddateien genutzt werden können, um Benutzer sozialer Netzwerke zu de-anonymisieren oder Beziehungen zwischen Nutzern außerhalb des sozialen Netzwerks aufzudecken. Auch durch eine Auslesung des

Digitale Systeme und Abläufe im Krankenhaus

Die digitale Vernetzung im Gesundheitswesen beginnt nicht mit der ePA. Daten werden an vielen Stellen gesammelt und müssen umfassend geschützt werden.

Browserverlaufs und den Abgleich der Daten mit Profilen in sozialen Netzwerken konnten in der Vergangenheit De-Anonymisierungen durchgeführt werden. Für die Pseudonymisierung müssen daher State-of-the-Art-Transformationsverfahren vergleichbar der BSI- oder ENISA-Richtlinie zu Kryptoverfahren verwendet und – insbesondere bei langfristig verwendeten pseudonymisierten Daten – durch jeweils aktuelle Verfahren ausgetauscht werden.

Die häufig getroffene Aussage, dass die Nutzung „einfach" sein muss, ist keine Begründung für eine unzureichende Sicherheit. Denn gerade gut dokumentierte und transparente Sicherheitsmaßnahmen sorgen für Vertrauen in komplexe Systeme. So müssen Betreiber die notwendigen Schritte bei der Einrichtung der ePA für einen Versicherten gut nachvollziehbar darstellen. Dadurch demonstrieren Versicherer und Betreiber, dass sie die Datensicherheit ernst nehmen. Gleichzeitig wird die Ende-zu-Ende Verschlüsselung auf Basis der Public-Key-Infrastructure (PKI) erreicht.

Versprechen durch proaktives Handeln belegen

Transparenz und Widerstandsfähigkeit beim Umgang mit sensiblen Daten sind nicht umsonst Kernelemente der DSGVO. Sowohl für die ePA als auch für das DVG hat der Gesetzgeber ein hohes Maß an Sicherheit versprochen. Die Konzepte der gematik zur ePA sind sehr eng entlang dieser Vorgabe entwickelt worden. Es bleibt jedoch die Aufgabe der Lösungsanbieter und der Betreiber, durch das eigene proaktive Handeln dieses Versprechen vollständig zu erfüllen. Eine 100-prozentige Informations- und Datensicherheit wird es zwar nie geben. Proaktives Handeln und Offenheit bei Vorfällen im Bereich Datenschutz und Informationssicherheit verbunden mit dem stetigen Streben nach hoher digitaler Widerstandsfähigkeit erhöhen das Schutzniveau jedoch nachweislich. So fördern sie das dringend benötigte Vertrauen der Patienten.

Dirk Schrader, Cyber Resilience Strategist & CMO bei Greenbone Networks (CISSP, CISM, ISO27001 Practitioner)

Die Elektronische Patientenakte startklar machen

Nichts Geringeres als das Potenzial, die Digitalisierung und deren Nutzen für gesetzlich Versicherte konkret erlebbar zu machen, verspricht die elektronische Patientenakte (ePA). Ein Überblick über aktuelle Aufgaben auf dem Weg.

Papier ade! Für den Arztbesuch von morgen müssen Patientinnen und Patienten dank digitaler Lösung weder umfangreiche Mappe mit Unterlagen mitbringen, noch lange über die eigene Krankheitsgeschichte referieren. Damit werden Doppeluntersuchungen ebenso vermieden wie gefährliche Wechselwirkungen bei der Verschreibung von Medikamenten. Dieses Zukunftsszenario ist gar nicht weit entfernt: Schon ab 2021 können hierzulande alle 73 Millionen Versicherten der gesetzlichen Krankenkassen auf Wunsch eine ePA nutzen, die all das möglich machen soll.

Suchen und Finden

Eine Herausforderung auf dem Weg dorthin ist die Frage nach einer sinnvollen Strukturierung der Inhalte der ePA. Schließlich sollte die behandelnde Ärztin oder der Arzt im Idealfall schnell und einfach die Information finden, die gerade benötigt wird. Zum jetzigen Stand ist das nur eingeschränkt möglich: Es fehlen Ordner und Fälle oder ähnliche Gruppierungselemente sowie die Möglichkeit, verschiedene Versionen einer Datei abzulegen. Aus diesem Grund wurde die Kassenärztliche Bundesvereinigung (KBV) mit der Ausarbeitung der entsprechenden Spezifikationen beauftragt. Es ist jedoch fraglich, ob sie im Alleingang dieser enormen Verantwortung gewachsen ist oder dabei am Ende das althergebrachte kulturelle Selbstverständnis im Weg sein wird. Der Erfolg wird nicht zuletzt daran gemessen, ob die KBV sich für eine Zusammenarbeit mit den beteiligten Akteuren – darunter unter anderem Krankenhäuser und Industrie – öffnen wird.

Vernetzung ermöglichen

Ein weiterer Bereich, an dem gerade intensiv gearbeitet wird, ist das Thema Standards. Die bisherigen Spezifikationen der Akte wurden isoliert von etablierten Standards (IHE-Profile oder HL7) festgelegt. Daraus resultierten erhöhte Entwicklungsaufwände und zunehmende Entfernung von der internationalen Vernetzung. Im Sinne der Interoperabilität und Praxisorientierung hat die gematik immerhin kürzlich das Signal gesendet, stärker in den Dialog mit Arztpraxen, Krankenhäusern und Verbänden treten zu wollen. So hat sie beispielsweise als erste Maßnahme im Dezember die beteiligten Akteure aus dem Gesundheitswesen Workshop zur Schaffung von Interoperabilität eingeladen. Ein durchaus sinnvoller Schritt, denn von den Erfahrungen und dem Wissen der Akteure aus der Praxis kann die ePA nur profitieren.

Nutzen schaffen

Neben den genannten, eher technischen und funktionalen Aspekten wird ein Faktor erfolgsentscheidend für die ePA sein: der erlebte Mehrwert für die Nutzerinnen und Nutzer. Dessen ist sich auch das Bundesgesundheitsministerium bewusst, weshalb derzeit mit Hochdruck am DVG 2.0 gearbeitet wird. So sollen im zweiten Anlauf ergänzende digitale Anwendungen wie Mutter- und Impfpass integriert werden – beide waren aufgrund von Datenschutzbedenken auf Betreiben des Bundesministeriums für Justiz und Verbraucherschutz auf den letzten Metern aus dem ersten DVG entfernt worden. Zudem ist geplant, dass weitere für den Nutzen der ePa entscheidenden Punkte dort wieder Eingang finden: beispielsweise die Verpflichtung der Ärztinnen und Ärzte, die Akte zu befüllen sowie der Anspruch auf Synchronisation des Notfalldatenmanagements und des elektronischen Medikationsplans.

Es bleibt sowohl für die gematik als auch für das Gesundheitsministerium durchaus noch Einiges zu tun, bevor die ePA umfassend genutzt werden kann. Für ein erfolgreiches Ergebnis ist gerade die Einbeziehung von Partnern aus der Praxis entscheidend. Denn diese können mit ihrem über Jahrzehnte aufgebauten Wissen unterstützen und einen wichtigen Teil dazu beitragen, dass Lösungen an den Bedürfnissen der Nutzerinnen und Nutzer ausgerichtet werden und so Mehrwerte schaffen. Die Mühe muss es allen Beteiligten wert sein, denn ein erfolgreicher Start der ePA wird wegweisend für die Digitalisierung des Gesundheitswesens hierzulande sein.

Sebastian Zilch ist seit Juni 2017 Geschäftsführer des Bundesverbandes Gesundheits-IT – bvitg e. V. mit Sitz in Berlin. Der bvitg vertritt in Deutschland die führenden IT-Anbieter im Gesundheitswesen.

Vernetzen Sie sich mit Ihren Patienten

TELEHEALTH
Zuverlässige Betreuung aus der Ferne
Steigende Patientenzahlen und zu wenig medizinisches Fachpersonal: Auswege aus diesem Dilemma bieten telemedizinische Anwendungen. Sie ermöglichen virtuelle Konsile und eine intersektorale Patientenbetreuung.
Für Ihre vernetzten Versorgungsmodelle schaffen wir die technologische Basis. Absolut zuverlässig und nach höchsten deutschen Sicherheits- und Datenschutzstandards.
www.telekom-healthcare.com/telehealth

T · ·

HEALTHCARE SOLUTIONS

Die ePA muss die Basis einer integrativen Gesundheitslösung werden

Wie kann die ePA auf Erfolgskurs gebracht werden? Die ePA blickt auf eine recht lange Geschichte zurück, warum hat sie noch keine wirkliche Marktreife erlangen können? Ein Statement von *Dr. Hans Unterhuber*, Vorstandsvorsitzender der SBK Siemens-Betriebskrankenkasse

Anfang 2021 kommt sie endlich – die elektronische Patientenakte (ePA). Sage und schreibe seit dem Jahr 2003 wird das Konzept einer wie auch immer gearteten, zentralen Zusammenführung von Gesundheitsdaten verfolgt. Dabei liegen die Vorteile auf der Hand: Die ePA ist ein Schritt in Richtung Demokratisierung der Medizin. Sie sorgt für Transparenz über Krankheits- und Behandlungsverläufe und gibt dem Patienten damit ein wichtiges Instrument zur Entscheidungsfindung an die Hand. Sie unterstützt Compliance. Und sie reduziert – richtig umgesetzt – Bürokratie.

Warum also dauert das alles so lange? Warum brauchen wir in Deutschland 18 Jahre für die Verwirklichung dieses Projektes? Meine Antwort: Weil sich die verschiedenen Akteure zu sehr auf Besitzstandwahrung konzentriert haben. Weil wir uns nicht gemeinsam hingesetzt haben und eine Vision entwickelt haben, auf die wir gemeinsam hinarbeiten. Die Vision, die ich verfolgen möchte, stellt den Versicherten ganz klar in den Mittelpunkt: Die ePA muss dem Patienten einen Mehrwert bieten.

Einen Mehrwert bietet eine ePA, die als Echtzeit-Daten-Kommunikationszentrum funktioniert. Sie darf nicht zum Ablageplatz veralteter PDF-Dokumente werden. Es braucht dazu eine Verpflichtung zeitnah Informationen zur Verfügung zu stellen; es braucht eine Anbindung aller Akteure, die an einer Behandlung beteiligt sind; und es braucht Standards für eine strukturierte und verständliche Darstellung aller Inhalte. Auch der weltweiten Vernetzung der Arbeits- und Lebensbedingungen muss die ePA Rechnung tragen. Es bedarf grenzüberschreitender Vernetzungsmöglichkeit.

In dieser Vision ist ePA zudem kein isoliertes Angebot, kein Tool unter vielen – sondern die Basis einer integrativen Gesundheitslösung, die eRezept, eMedikationsplan und alle

SO WIRD IHR IT-BUDGET ZUM HERBSTMEISTER

Mit gebrauchten
Software-Lizenzen
in Top Form

software broker

Unter unseren Kunden verlosen wir
3 x 2 VIP-Tickets
für ein Bundesligaspiel inkl.
Luxushotel

Starten Sie jetzt Ihre Schlussoffensive und landen Sie mit Ihrem restlichen IT-Budget einen Volltreffer: Investieren Sie in gebrauchte Software-Lizenzen - zum Hammerpreis! Überzeugen Sie sich im Rahmen einer Websession im Vorfeld von der Qualität und Rechtssicherheit unserer Lizenzen. Rufen Sie uns an: **+49 211 547 671 20**

Microsoft Office Professional Plus 2019

ab **139,00 €** netto
pro Einzel-Lizenz*

Microsoft Office Professional Plus 2019 und CoreCAL per User Bundle

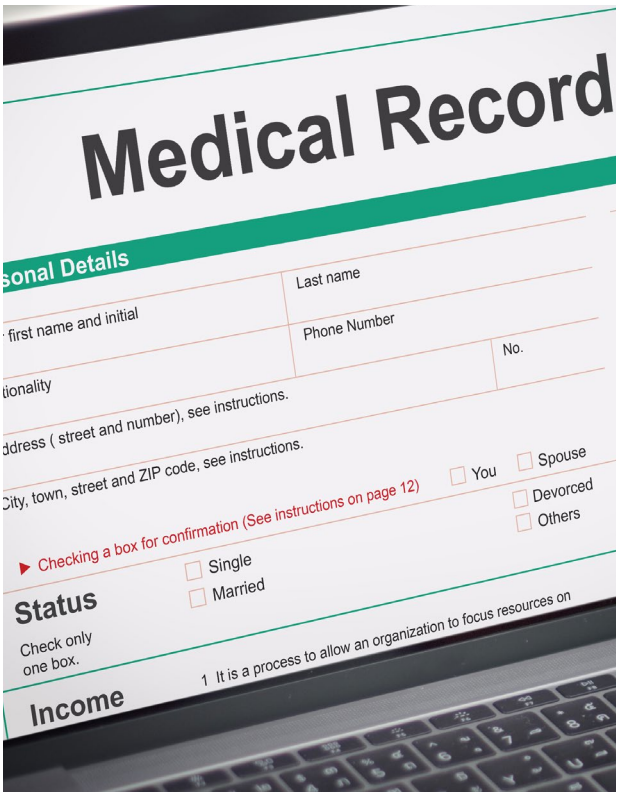
ab **169,00 €** netto
pro Bundle*
aktuelle Zugriffslizenzen für Microsoft Server

* Beide Angebote richten sich ausschließlich an Unternehmen und sind bis zum 31.12.2019 gültig.
Mindestabnahme pro Angebot: 10 Stück. Solange der Vorrat reicht.

Weitere Aktionsprodukte verfügbar!

Alles Weitere unter: www.lizenzmeisterschaft.de

SB Software-Broker GmbH • info@software-broker.com • +49 211 547 671 20



zukünftigen Vorhaben vereint. Kein Patient will zwanzig verschiedene Zugangswege, sich zwanzig Mal anmelden, zwanzig Applikationen, die im schlimmsten Fall noch nicht mal miteinander sprechen.

Das gleiche gilt übrigens auch für Leistungserbringer, die schließlich ebenfalls Nutzer der ePA sind. Auch sie wollen sich nicht durch unsortierte PDF-Berge wühlen und den bürokratischen Aufwand haben, Informationen in unzählige Systeme einzutragen. Denn das ist keine Digitalisierung – das ist ein einfaches Übertragen analoger Prozesse in die digitale Welt.

Ich würde mir wünschen, dass die gematik hier in Zukunft eine treibende Rolle übernimmt. Ich stelle mir das so vor, dass sie als nationale eHealth-Agentur fungiert und eine systematische, transparente Zusammenarbeit aller relevanten Stakeholder koordiniert. Und Stakeholder sind für mich nicht nur IT- oder Gesundheitsexperten, sondern auch die Patienten. Sie müssen in die Gespräche mit einbezogen werden. Ein solches Vorgehen kann nicht nur Garant für eine nutzerzentrierte Weiterentwicklung sein, sondern auch Akzeptanz schaffen. Und nur, wenn wir bei allen Menschen - also Patienten genauso wie Behandlern – eine solche Akzeptanz erreichen, dann wird das Ganze ein Erfolgsprojekt.

Mit Sorge beobachte ich daher die öffentliche Diskussion über die ePA und die Digitalisierung im Gesundheitswesen. Sie ist nicht Chancenorientiert. Im Vordergrund stehen Bedenken – allen voran in Sachen Datenschutz. Natürlich ist das Thema wichtig. Die Patienten müssen Herr ihrer Daten sein und bleiben. Aber man darf den Datenschutz nicht als Ausrede nutzen. Anstatt Probleme zu suchen, sollten wir an Lösungen arbeiten.

www.sbk.org

Über die SBK:

Die Siemens-Betriebskrankenkasse SBK ist die größte Betriebskrankenkasse Deutschlands und gehört zu den 20 größten gesetzlichen Krankenkassen. Als geöffnete, bundesweit tätige Krankenkasse versichert sie mehr als 1 Million Menschen und betreut über 100.000 Firmenkunden in Deutschland – mit mehr als 1.500 Mitarbeitern in 94 Geschäftsstellen.

Seit über 100 Jahren setzt sich die SBK persönlich und engagiert für die Interessen der Versicherten ein. Sie positioniert sich als Vorreiter für einen echten Qualitätswettbewerb in der Gesetzlichen Krankenversicherung. Voraussetzung dafür ist aus Sicht der SBK mehr Transparenz für die Versicherten – über relevante Finanzkennzahlen, aber auch über Leistungsbereitschaft, Beratung und Dienstleistungsqualität von Krankenkassen. Im Sinne des Kunden vereint die SBK darüber hinaus das Beste aus persönlicher und digitaler Welt und treibt die Digitalisierung im Gesundheitswesen aktiv voran.

Dr. Hans Unterhuber, SBK-Vorstandsvorsitzender

PHILIPS

Klinische IT

Vernetzt arbeiten.
Umfassend versorgen.

Im Zuge der Digitalisierung werden immer mehr gesundheitsbezogene Daten erfasst. Um die Daten nutzbar zu machen, müssen diese aufgerufen, analysiert, interpretiert, geteilt und archiviert werden. Das stellt enorme Herausforderungen an die klinische IT. Intelligente Systeme sollen die riesigen Datenmengen auswerten, Routineaufgaben automatisieren und bei der klinischen Entscheidungsfindung unterstützen. Es gibt immer einen Weg, das Leben besser zu machen.

Informationen zu unserer klinischen IT finden Sie auf der Website **www.philips.de/healthcare.** Mehr über unsere KI-gestützten Lösungen erfahren Sie unter **www.philips.de/KI**

innovation you

Elektronische Patientenakte aus dem Digitale-Versorgung-Gesetz ausgegliedert

Aufgeschoben und nicht *aufgehoben?*

Angetreten als Vorzeigeprojekt des Bundesgesundheitsministeriums, bleibt die bahnbrechende Wirkung des Digitale-Versorgung-Gesetzes (DVG) nach der Ausgliederung der elektronischen Patientenakte (ePA) aus. Die erwartete Hebelwirkung in Sachen Digitalisierung des Gesundheitswesens verpufft. Denn im neuen, nun verabschiedeten Entwurf zum DVG hat das Bundesgesundheitsministerium alle geplanten Regelungen zur ePA gestrichen. Verblieben ist lediglich die Absichtserklärung, zeitnah ein zusätzliches Gesetz auf den Weg zu bringen, das die ePA umfassend regeln soll, damit Versicherte wie geplant bis 2021 von der elektronischen Patientenakte profitieren können. Wie konnte es zu dieser Situation kommen? Und warum ziehen die Beteiligten nicht an einem Strang?

TÜV SÜD: Vertrauen schaffen in digitale Technologien.

Ihr Partner für Cyber Security Services, Sealed Cloud Lösungen und Trainings für IT-Sicherheit und Datenschutz.

TÜV SÜD unterstützt Unternehmen dabei, die Chancen der Digitalisierung zu nutzen. Dabei richten wir unser Augenmerk auf die Anforderungen und Risiken. Cyber Security und Datensicherheit sind Teil unserer Kernkompetenz. Wir bieten:

- Security-Check für Medizinprodukte
- Industriespezifische Erfahrung, Know-how und Experten, die zu den Besten zählen
- Umfassende Unterstützung von der Risikoanalyse über die Beseitigung von Sicherheitslücken bis zur dauerhaften Absicherung Ihrer Geschäftsprozesse
- Mitarbeiter-Schulungen

Vertrauen Sie TÜV SÜD: Rund um die IT-Sicherheit Ihres Unternehmens.

www.tuvsud.com/de-securitymedizinprodukte

Mehr Wert.
Mehr Vertrauen.

TÜV SÜD AG Westendstr. 199, 80686 München, Deutschland
Tel. +49 89 5791-0 www.tuvsud.com

TÜV®

Datenschutzkeule

Aufgrund von datenschutzrechtlichen Bedenken aufseiten des Justizministeriums in der Ressortabstimmung hat das Gesundheitsministerium die Regelungen zur ePA aus dem Entwurf zum DVG gestrichen. Vor allem ging es um die Annahme, dass sensible Informationen zum Gesundheitszustand stärkere Schutzmechanismen bräuchten. Das Gesundheitsministerium entschied sich daher für die Aufspaltung des Digitalisierungsgesetzes, um die anderen Elemente des Vorhabens zügig durchzubringen – und opferte dafür zunächst die ePA. Nun soll ein eigenes Datenschutzgesetz mit den Regelungen zur elektronischen Patientenakte das erklärte Ziel sein. Es bleibt die Frage, warum grundlegende Datenschutzfragen überhaupt zu einer Aufsplittung des DVG führten und sich die Verantwortlichen erst jetzt ausführlicher mit dem Thema auseinandersetzen. So oder so ist die gematik für die technischen Einzelheiten zuständig. Daher bleibt ungewiss, weswegen solche Einzelheiten auf Gesetzesebene gebracht werden müssen. Dies lässt nur einen Schluss zu: Das Justizministerium traut der gematik nicht zu, simple Grundsätze zum Datenschutz auf dem neuesten Stand der Technik zu regeln. Hier entsteht beinahe schon der Eindruck, bei der ursprünglichen Version des DVG handele es sich um ein äußerst brisantes Gesetz, dass das Justizministerium gezwungenermaßen aufgrund des mangelnden Datenschutzes blockieren müsse. Zurück bleibt der schale Nachgeschmack, dass es sich bei der Blockade um den klassischen Einsatz der Datenschutzkeule handelt.

Schwierige digitale Mission

Der Bundesgesundheitsminister hat sich die Digitalisierung der Sozial- und Gesundheitsbranche ganz klar auf die Fahne geschrieben. Allerdings findet aufgrund divergierender Interessen der Beteiligten regelmäßig eine Aushöhlung seiner begrüßenswerten Digitalisierungsvorhaben statt. Darunter leiden letztlich die Versicherten – die ePA befindet sich nun über eine Dekade in der Diskussion und noch immer ist sie nicht nutzbar. Scheinbar geht es den Verantwortlichen nicht wirklich um die positiven Effekte für die Bürger, sondern vor allem um eigene Vorstellungen und Interessen. Denn warum sonst sollte der Gesetzentwurf das Flaggschiff ePA verlieren? So schrumpft die elektronische Patientenakte zu einem Vorhaben, das sich getrost weiter aufschieben lässt. Klar ist: Niemand darf ohne Grundlage mit sensiblen Daten arbeiten. Umso paradoxer, dass sich eine solche Gesetzesgrundlage überhaupt durch den Datenschutz ausbremsen lässt. Vor dem Hintergrund, dass Gesundheitsdaten für die Versorgung und den medizinischen Fortschritt von erheblichem Wert sind und nur so Patienten von einer zeitgemäßen Versorgung profitieren könnten, erscheint die Vertagung der ePA in einem noch schlechteren Licht. Neben dem durchaus wichtigen Thema Datenschutz gerät die Sorge um die Versicherten aus dem Blickfeld. Mit einer einheitlichen ePA ließen sich viele Baustellen auf einem Schlag lösen – von Arzneimittel-Wechselwirkungen, Behandlungsfehlern über Informationslücken bis hin zu unnötigen Doppeluntersuchungen. Auf einen Blick könnten Mediziner und Einrichtungen alle wichtigen Daten zur Krankheitsgeschichte erhalten, ohne umständlich Befunde anzufordern. Bei der Digitalisierung des Gesundheitssystems ziehen die Ministerien offensichtlich nicht an einem Strang. Entweder die Verantwortlichen glauben nicht an den Erfolg digitaler Prozesse oder sie empfinden die Vorhaben als zu schwierig und kompliziert. Wann genau das neue Gesetz zur Regelung der elektronischen Patientenakte kommen soll, ist noch offen. Hoffentlich werden die Funktionen der ePA durch die gesonderte Richtlinie nicht allzu sehr gestutzt – sonst geht schlimmstenfalls eine bloße Attrappe ohne Nutzen für die Patienten an den Start. Erinnerungen an den interessengeleiteten Umgang mit der elektronischen Gesundheitskarte werden wach.

Weitere Informationen unter: www.techniklotsen.de

Karsten Glied ist Geschäftsführer der Techniklotsen GmbH, die sich auf maßgeschneiderte IT- und Technik-Lösungen für die Sozial- und Gesundheitswirtschaft spezialisiert hat. Als studierter Diplom-Betriebswirt entwickelte er schon lange vor dem Megatrend „Digitalisierung" Strategien für eine bessere Verzahnung von IT mit den fachlichen und wirtschaftlichen Anforderungen eines Unternehmens. Zudem tritt er als Vortragender auf internationalen Konferenzen auf und referiert rund um die Themen Digitalisierung und „IT Business Alignment".

Think Medical!
Act Digital!

DMEA

Connecting Digital Health

21.–23. April 2020

Messegelände Berlin

www.dmea.de

GOLD Partner

AGFA HealthCare · Cerner · CGM CompuGroup Medical · ID Information und Dokumentation im Gesundheitswesen · medatixx Damit die Praxis läuft. · Meierhofer · T · · · HEALTHCARE SOLUTIONS

SILBER Partner

3M · BEWATEC · D·M·I Archivierung · Hewlett Packard Enterprise · InterSystems · i-SOLUTIONS Health · Meona Die klinische Software · nexus/ag · PHILIPS · RZV · SIEMENS Healthineers · VISUS · vitagroup Health Intelligence

Veranstalter

bvitg

Organisation

Messe Berlin

In Kooperation mit

BVMI Berufsverband Medizinischer Informatiker e.V. · gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Unter Mitwirkung von

KHIT · CIO-UK

KI-gestützte Vermittlung von Krankenhauslaboren für Ärzte und Patienten

Willkommen im Labor-Dschungel

Wenn es um Lösungen für den Einsatz im Krankenhauslabor geht, dreht sich nicht nur alles um genaue Testergebnisse und saubere Aufträge. Krankenhäuser nutzen zusätzlich zur Labortechnik oft auch sogenannte Labor-Outreach-Programme, um die Vermarktung und den Verkauf von Tests und anderen Labordienstleistungen an lokale Arztpraxen oder andere Anbieter zu ermöglichen. Allerdings hängt vieles von dem verwendeten Labor-Outreach-System ab.

Der Dschungel der elektronischen Gesundheitsakten

Labore möchten auch unabhängig der Services im Zusammenhang mit der elektronischen Patientenakte (Electronic Medical Record, EMR) ein hohes Maß an digitalen Services bieten. Dazu sollten Labor-Outreach-Systeme alle Formen elektronischer Gesundheitsakten (Electronic Health Record (EHR) und EMR) unterstützen. So ist gewährleistet, dass sich Labore schnell mit jedem Arzt oder jeder Klinik vernetzen und ihre Unterstützung anbieten können.

Vor allem aber muss das System Aufträge senden und empfangen sowie Ergebnisse zwischen Labor und Patient oder Arzt sicher und effektiv abwickeln können. Die meisten Systeme liefern bereits angemessene Ergebnisse, dennoch stellt die Bereitstellung eines Auftrags-Workflows für viele Outreach-Systeme eine Herausforderung dar, sofern der Prozess von einer Klinik übernommen wird. Für das Unternehmen ist es unerlässlich und kann sogar den Return on Investment (ROI) erhöhen, wenn alle Rechnungs- und Bestellregeln inklusive der Beseitigung von Fehlern, Rückruf- und Erstattungsproblemen korrekt eingehalten werden.

Fünf Ansätze für Outreach- und Laborintegration

Integrationsmaschinen

Integrationsmaschinen bieten grundlegende Funktionen für das Routing und die Umformatierung von Aufträgen und Ergebnissen. Allerdings fehlt es ihnen oft an den Möglichkeiten, sicherstellen zu können, dass eine Bestellung die erforderlichen klinischen Inhalte wie beispielsweise die Begründung von Diagnosen, Angaben zu erforderlichen Versicherungen oder Autorisierungscodes enthält.

Laborportale

Laborportale wurden dazu entwickelt, die Probleme bei der Auftragsabwicklung und der fristgerechten und lesbaren Auswertung von Testergebnissen digital zu lösen. Die meisten Arztgruppen haben EMRs allerdings als Verwaltungsplattform für die gesamte Patientenversorgung gewählt, da ihre Aufträge so in der EMR angelegt werden. Arbeitet das Laborportal außerhalb der EMR, so erhöht es den Zeit- und Verwaltungsaufwand im Workflow des Arztes. Schickt eine große Klinik beispielsweise Tests an viele Labore basierend auf dem Test-Typ oder der Patientenversicherung, muss sie mit zahlreichen verschiedenen Portalen und Systemen arbeiten.

Labor-Middleware

Die meisten Labor-Middleware-Lösungen sind entstanden, weil Anbieter von Laborportalen ihre Lösungen weiterentwickelten, um eine umfassendere Funktionspalette anbieten zu können. Werden Middleware-Lösungen in der Klinik eingesetzt, können Plebologen Angaben zum Haftungsverzicht (ABN-Checks) prüfen und AOE-Fragen (Ask at Order Entry) abschließen. Doch zwischen den verschiedenen Systemen gibt es oft Informationsunterschiede, da sie nicht einheitlich innerhalb der EMR behandelt werden. In einigen Fällen sind höherwertige Dienste wie patientenfreundliche Berichte nur über das Lieferantenportal der Middleware verfügbar, das sich auch außerhalb des EMR-Systems der Klinik befinden kann.

End-to-End-Laborplattformen für die Öffentlichkeitsarbeit

End-to-End-Labor-Outreach-Lösungen wie OpenText EMR-Link bieten nicht nur die vollständige Klinikintegration für das Labor, sondern lassen sich auch direkt in den EMR-Workflow

des Arztes integrieren. Dadurch erreichen End-to-End-Laborplattformen eine möglichst enge Auftrags- und Ergebnisintegration zwischen jeder EMR und dem Labor. Ist diese eingebettete Integration vorhanden, werden Bestellungen innerhalb der EMR automatisch auf medizinische Notwendigkeit überprüft. Darüber hinaus werden Bestellungen an das richtige Labor weitergeleitet. Dadurch arbeitet die gesamte Klinik effizienter, und die Akzeptanz der eigenen Ärzte wird gefördert.

Patientenfreundliche Ergebnisse und personalisierte Behandlung

Nicht nur Ärzte setzen bei ihrer Einschätzung der Patientensymptome auf Laborergebnisse. Auch Pflegefachkräfte sind auf Dosierungsangaben zur Behandlung angewiesen. Sie konzentrieren sich nicht nur auf die Arztbriefe, sondern auch auf das Empfinden des Patienten und die eigene Erfahrung. Es ist wichtig, dass ein Labor patientenfreundliche Berichte verfasst und Ärzte und Patienten bei der Interpretation der Ergebnisse unterstützt. Patienten verlangen schließlich schnelle und transparente Ergebnisse, die sie als Laie verstehen können.

Die Laborarbeit wird mit Labor-Outreach-Lösungen zur Rolle eines Informationsanbieters. Dadurch wird sie den sich wandelnden (digitalen) Bedürfnissen von Ärzten und Patienten gerecht. Sie helfen dabei, das effektivste Testprotokoll zu identifizieren und die Ergebnisse genau zu interpretieren, um die Entwicklung personalisierter Behandlungspläne von Patienten zu ermöglichen.

Labor-Outreach-Lösungen verbinden also Labore mit der Klinik-EMR, mit Krankenhäusern, die noch auf Papier arbeiten, und stellen ebenso eine Plattform für jede Krankenschwester, jeden Facharzt und jeden Labortechniker dar, die an dem Ergebnis-Workflow des Laborauftrags beteiligt sind. Mit nur einer einzigen Verbindung zum Labor sind Labor-Outreach-Programme in der Lage, die Verbindungen zu allen niedergelassenen Ärzten zu verwalten und so eine zielgerichtete Patientenversorgung mit den benötigten Fachärzten und Laboren zu gewährleisten.

Janet Russell, Senior Manager Product Marketing für Healthcare Solutions

Der ISMS-Ratgeber – ein Leitfaden für die Praxis (Teil 8)

Unser mehrteiliger Praxis-Ratgeber stellt Ihnen alle erfolgsrelevanten Bausteine eines systematischen Informationssicherheits-Managements vor, um einen wirksamen Schutz von Informationen und Systemen im Hinblick auf Vertraulichkeit, Integrität und Verfügbarkeit aufbauen und dauerhaft gewährleisten zu können.

Erfahren Sie in dieser Ausgabe, wie ein konsequenter Umgang mit Sicherheitsvorfällen und eine systematische Steuerung von Aktivitäten zur kontinuierlichen Verbesserung dabei helfen, ein ISMS nachhaltig erfolgreich zu betreiben.

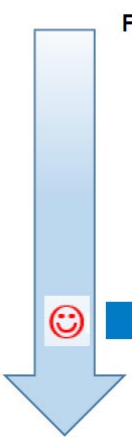
Erfolgsbaustein 13: Sicherheitsvorfall-Management

Eine Einrichtung ist unvermeidbar Sicherheitsvorfällen ausgesetzt, was sich unmittelbar auf den Betrieb und die Weiterentwicklung eines ISMS auswirkt. Sicherheitsrelevante Vorfälle sind in der Regel Nichtkonformitäten, die einen entscheidenden Einfluss auf den kontinuierlichen Verbesserungsprozess (KVP) und den Reifegrad des ISMS haben. Denn letztlich gilt: Nur wer Fehler erkennt und aus ihnen lernt, also seine Aktivitäten und Strategien überdenkt und beispielsweise unwirksame Maßnahmen entfernt oder ersetzt, bestehende Sicherheits-Konzepte anpasst oder neue Sicherheits-Lösungen umsetzt, erzielt langfristig den bestmöglichen Nutzen eines ISMS, das in einem hochdynamischen und nicht immer vorhersehbaren Umfeld bestehen muss.

Ihr Navigator zum „ISMS-Ratgeber - ein Leitfaden für die Praxis“

Was gab's schon? Wo stehen wir jetzt? Wie geht's weiter?

Mit diesem Navigator behalten Sie beim mehrteiligen ISMS-Praxis-Ratgeber stets den Überblick - der Smilie ☺ weist auf den Inhalt der aktuellen Ausgabe hin:



Folge	Inhalt
1	Intention und Überblick
2	Kontext der Organisation / Führungsverhalten und Verpflichtung
3	Informationssicherheits-Ziele / Informationssicherheits-Leitlinie
4	Rollen, Verantwortlichkeiten und Kompetenzen / Risiko-Management
5	Erfolgskontrolle & KPIs / Dokumentation
6	Kommunikation / Fähigkeiten und Awareness
7	Lieferantenbeziehungen / Interne Audits
8	**Sicherheitsvorfall-Management / Kontinuierliche Verbesserung**
9	Zertifizierungs-Option / Dauerhafter Nutzen

Erfolgreich agieren und reagieren

Vorfälle, die die Informationssicherheit gefährden, lassen sich auch mit einem leistungsfähigen ISMS nie völlig vermeiden. Umso sinnvoller ist es deshalb, sich entsprechend vorzubereiten.

Damit die Informationssicherheit auch in widrigen Situationen aufrechterhalten werden kann, ist es wichtig, bereits im Vorfeld Verantwortlichkeiten, Abläufe und Behandlungsoptionen festzulegen und entsprechend einzuüben.

Das grundsätzliche Ziel bei der Behandlung von Informationssicherheitsvorfällen (Information Security Incidents) ist ein möglichst koordiniertes, zielgerichtetes und damit effizientes Reagieren beim Eintreten einer Sicherheitsverletzung, z.B. bei einer Cyber-Attacke.

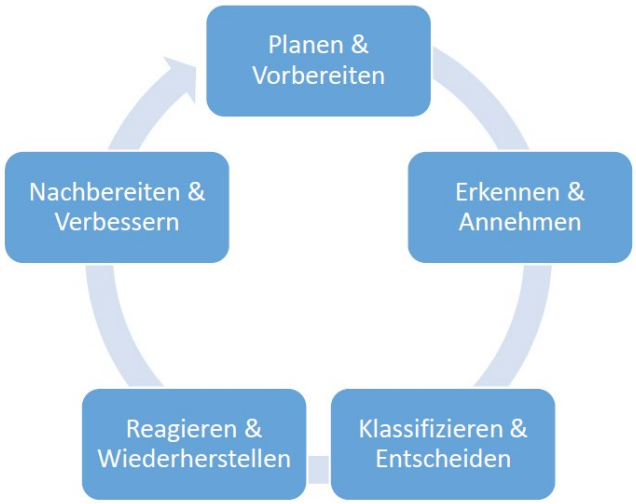


Bild 1: Phasenmodell zum Incident Response Management

Hilfreich sind dabei folgende Aktivitäten:

- Stimmen Sie den Prozess zur Sicherheitsvorfallbehandlung und dessen Detaillierungsgrad auf das Risikomanagement in Ihrer Einrichtung und auf die für das ISMS geltenden Rahmenbedingungen ab. Hier liegt auch der Schlüssel für die Wirtschaftlichkeit einer wirksamen Sicherheitsvorfallbehandlung.

- Legen Sie eine sinnvolle Kategorisierung für Vorfälle fest, die eine praktikable und vernünftige Abgrenzung des Schweregrads ermöglicht – z.B. eine Unterscheidung zwischen Störungen, Sicherheitsvorfällen, Notfällen und Krisen.

- Verfassen und kommunizieren Sie einen Sicherheitsvorfall-Behandlungsplan (Incident Response Plan), in dem die wesentlichen Abläufe nachvollziehbar geschildert sind. Verfeinern und entwickeln Sie diesen weiter auf Basis von Erkenntnissen und Erfahrungen, die sich im Laufe der Zeit ergeben – am besten gemeinsam mit anderen Betroffenen.

- Regeln Sie Funktionen, Rollen, Verantwortlichkeiten und konkrete Ansprechpartner bereits im Vorfeld, da in einer Notfallsituation meist keine Zeit zur Klärung bleibt.

- Stellen Sie auch sicher, dass alle Betroffenen vor und insbesondere während eines Notfalls Zugriff auf benötigte Informationen (z.B. Incident Response Plan, Sofortmaßnahmen, Wiederanlaufplan) haben.

- Üben Sie regelmäßig das richtige Verhalten im Notfall, beispielsweise durch Simulation verschiedener Notfall-Szenarien. Das fördert dank eines Routine-Effekts einen sicheren Umgang bei allen Beteiligten und hilft dabei, Defizite bei der Organisation und beim eigenen Handeln bereits vor einem realen Ernstfall aufzudecken mit der Chance, diese Defizite rechtzeitig zu beseitigen.

Das folgende Phasenmodell skizziert einen typischen Ablauf bei der Informationssicherheitsvorfall-Behandlung:

Erläuterung der Phasen

Planen & Vorbereiten

- Um das grundsätzliche Ziel zu erreichen, sind für alle operativen Phasen des Prozesses Präventivmaßnahmen zu treffen, die die Einrichtung und das Personal auf einen solchen Fall bestmöglich vorbereiten.
- Neben generischen Problemlösungsstrategien sind vorab insbesondere relevante Bereiche, Ansprechpartner und Eskalationswege zu definieren.

Erkennen & Annehmen

- Sicherheitsvorfälle sollten unabhängig vom konkreten Meldeweg (E-Mail, Telefon usw.) stets bei einer zentralen Meldestelle eingehen und dort protokolliert werden.
- Allen relevanten Gruppen, bei denen Vorfälle auftreten können, ist ein eindeutiger Meldeweg anzubieten - etwa Verwaltungsmitarbeitern, Stationen/MVZs, Lieferanten, Partnern.
- Regeln zum korrekten Verhalten bei sicherheitsrelevanten Vorkommnissen einschließlich Anlaufstellen und Meldeplänen sollten zielgerichtet bereitgestellt werden.

Klassifizieren & Entscheiden

- Die Meldestelle entscheidet, ob das gemeldete Ereignis nach aktueller Einschätzung
  - offenkundig ein Sicherheitsereignis darstellt,
  - ein Ereignis ohne Sicherheitsbezug ist, für das bereits eine Lösungsbeschreibung vorliegt („Known Error"),
  - ein Notfall vorliegt, der idealerweise im Notfallplan behandelt wird.
- Im Zweifelsfall muss eine Eskalation erfolgen.
- Die Meldestelle ist entsprechend zu instruieren und zu schulen.
- Alle eingehenden Vorfallsmeldungen sollten dokumentiert und mindestens die nachfolgenden Informationen erfasst werden:
  - Eindeutige Identifikationsnummer
  - Datum der Annahme und Eintritt des Sicherheitsvorfalls
  - Angaben zum Melder, zu betroffenen Personen/Bereichen und Systemen
  - Beschreibung des Sicherheitsvorfalls (z.B. Symptome, Ausbreitung, bisherige Auswirkungen)

- Alle Sicherheitsvorfälle müssen bei Meldungseingang nach einem zuvor abgestimmten Schema klassifiziert werden, um eine Priorität ableiten zu können. Abhängig von der Priorität sind vorab definierte Sofortmaßnahmen einzuleiten und die verantwortlichen Personen (z.B. Informationssicherheitsbeauftragter, IT-Leiter, Stations- oder Krankenhausleitung) zu informieren.
- Die idealerweise in einem (Ticket-)System dokumentierten Sicherheitsvorfälle sollten überwacht werden (Monitoring), um Gegenmaßnahmen besser zu steuern und beispielsweise auch die Bearbeitung niedrig klassifizierter Ereignisse zu gewährleisten, die ansonsten aus dem Blickfeld verschwinden könnten.

Reagieren & Wiederherstellen (Incident Response)

- Eindämmung und Beweissicherung: Schadensbereich analysieren, weitere Ausbreitung durch geeignete Maßnahmen eindämmen, potenzielle Hinweise und Belege sichern - bei Bedarf durch forensische Analysen und im Vorfeld festgelegte Vorgehensweisen.
- Beseitigung und Wiederherstellung: Maßnahmen zur Wiederherstellung der gewünschten Zielkonfiguration einleiten, z.B. über Wiedereinspielen (Restore) einer zuvor angefertigten Datensicherung (Backup).
- Ursachenermittlung und Beweissicherung: Ursache des Ereignisses ermitteln und potenzielle Hinweise und Belege sichern, eventuell mit Hilfe weitergehender forensischer Analysen.

Nachbereiten & Verbessern

- Damit ein Sicherheitsvorfall ausreichend nachvollziehbar ist, muss dazu ersichtlich sein,
  - wie der aktuelle Status der Bearbeitung lautet,
  - welche Mitarbeiter mit der Bearbeitung beauftragt sind,
  - welche Maßnahmen zur Problemlösung aktuell geplant sind,
  - wann die Umsetzung der erforderlichen Maßnahmen vorgesehen ist.
- Alle dokumentierten Sicherheitsvorfälle müssen im Nachgang analysiert werden, ob durch eine Optimierung im Vorfallbehandlungsplan oder durch Änderungen in der Aufbau- und/oder Ablauforganisation (u.a. Erstellung bzw. Anpassung von Handlungsanweisungen) in Zukunft ein verbesserter Umgang mit Vorfällen erreicht werden kann.
- Im Anschluss an die Bearbeitung von Sicherheitsvorfällen muss ein Bericht verfasst werden, in dem dargestellt wird, wie derartige Vorfälle in Zukunft vermieden oder zumindest in ihrer Auswirkung minimiert werden können. Daraus lassen sich möglicherweise (zusätzliche) technische und organisatorische Maßnahmen ableiten, die im Regelbetrieb anzuwenden sind.

Erfolgsbaustein 14: Kontinuierliche Verbesserung

Ein Managementsystem für Informationssicherheit (ISMS) stellt üblicherweise ein Konstrukt dar, das zu einem bestimmten Zeitpunkt auf Basis der dabei geltenden Voraussetzungen und Rahmenbedingungen erstellt bzw. optimiert wurde. Da sich diese Parameter mehr oder weniger absehbar ändern, wird klar, dass das ISMS entsprechend angepasst werden muss. Dazu sind die vorhandenen Abläufe und die dabei praktizierten Verfahren zu analysieren und stetig den eigenen Bedürfnissen anzupassen. Im Sinne der Norm ISO/IEC 27001 sind insbesondere aus festgestellten Nichtkonformitäten entsprechende Verbesserungspotenziale für das ISMS abzuleiten. Dieser Prozess ist als kontinuierlicher Verbesserungsprozess (KVP) geläufig.

Eine Einrichtung, die ein normkonformes ISMS betreiben möchte, muss dazu organisatorische Maßnahmen festlegen, auf deren Basis eine kontinuierliche Verbesserung gezielt und planmäßig stattfindet (z.B. fest geplante Quartalsgespräche zwischen IT/Security und Stationsleitung). Die Durchführung dieser Maßnahmen und die jeweiligen Ergebnisse sind hierbei zu überwachen und angemessen zu dokumentieren. Darüber hinaus hat die Einrichtung nachzuweisen, wie sie bei festgestellten Mängeln dafür sorgt, dass sich diese nicht wiederholen (z.B. Maßnahmen- und Umsetzungsplan, Revisionsprotokolle).

Bewährtes Vorgehensmodell

Eine empfohlene Herangehensweise zur konsequenten Sicherstellung einer kontinuierlichen Verbesserung des ISMS folgt dem PDCA-Zyklus, mit dem die Entwicklungsphasen eines solchen Systems modelliert werden: das Planen („Plan"), das Umsetzen („Do"), das Überprüfen („Check") und das Schlussfolgern/Entscheiden („Act").

Sicherheitsvorfall-Management - Hinweise zur Dokumentation:

In der ISO/IEC 27001 sind keine normativen Anforderungen an die Dokumentation des ISMS im Hinblick auf Sicherheitsvorfall-Management festgelegt.

Darüber hinaus haben sich in der Praxis folgende Dokumente als zielführend und hilfreich erwiesen:

- Sicherheitsvorfall-Behandlungsplan (Incident Response Plan) mit Kontaktlisten und Eskalationsplänen
- Zusammenstellung von Verhaltensregeln bei sicherheitsrelevanten Unregelmäßigkeiten
- Prozessbeschreibungen und Arbeitsanweisungen für die Sicherung von Beweisen
- Berichte über Sicherheitsvorfälle

Dabei lassen sich diese Phasen folgendermaßen beschreiben:

Plan
• Etablierung von Maßnahmenzielen und Verantwortlichkeiten für deren Erreichung • Etablierung der Sicherheitsmaßnahmen zur Erreichung der Maßnahmenziele und der operativen Prozessverantwortlichen für diese Maßnahmen • Definition der Leistungsindikatoren, die eine Leistungsmessung gegen die Maßnahmenziele erlauben • Definition des Prozesses zur Messung der Leistung inklusive der Messpunkte, Berechnungsmethode des Indikators und der Norm- und Toleranzbereiche • Definition der Korrekturmaßnahmen, um die Sicherheitsmaßnahme im Normbereich zu regeln
Do
• Kontinuierliche Messung der Maßnahmenzielerreichung mit Lieferung an das Security Controlling innerhalb des ISMS • Einleitung von Korrekturen bei festgestellten Mängeln oder Nichtkonformitäten
Check
• Überwachen der einzelnen Sicherheitsmaßnahmenindikatoren und Vergleichen der einzelnen Leistungsfähigkeiten mit den Maßnahmenzielen • Aufsicht über die eingeleiteten Gegenmaßnahmen und deren Verantwortliche, wenn eine Sicherheitsmaßnahme den Normbereich der Effektivität verlassen hat. • Erstellen von Sicherheitsberichten mit Key-Performance- Indikatoren für das Management, basierend auf den Maßnahmenzielen und Sicherheitszielen. Diese Berichte sollten Handlungsoptionen für notwendige Managemententscheidungen enthalten, die Sicherheitsmaßnahmen stärken, die regelmäßig in den Toleranzbereich laufen oder den Schwellwert zur Ineffektivität überschreiten.
Act
• Treffen von notwendigen Managemententscheidungen, um die Effektivität von Sicherheitsmaßnahmen oder ganzen Maßnahmenzielen wiederherzustellen. Entscheidungen werden an den operativen Betrieb zur Umsetzung weitergegeben. • Die getroffenen Entscheidungen werden mit Begründungen angemessen dokumentiert, beispielsweise über das Security Controlling.

Bild 2: PDCA-Maßnahmen zur kontinuierlichen Verbesserung des ISMS

Sinnvolle Aktivitäten

Die Verbesserung des ISMS erfolgt in der Regel durch die Identifikation von Abweichungen zu den Anforderungen aus der Norm und durch daraus abgeleitete Korrekturmaßnahmen. Gleichwohl können – auch ohne eine vorliegende Abweichung - Verbesserungsvorschläge direkt bewertet und umgesetzt werden.

Auch folgende Aktivitäten erweisen sich oft als hilfreich und zielführend:

- Maßnahmen aus dem KVP sollten in einen übergreifenden Umsetzungs- bzw. Risikobehandlungsplan aufgenommen werden, um einen besseren Überblick zu erhalten und auf Zusammenhänge aufmerksam zu werden.
- Des Weiteren führen die regelmäßig vorzunehmenden Risikoanalysen zu einer ständigen Verbesserung des ISMS. Die Ergebnisse der Risikoanalysen stellen einen wesentlichen Bestandteil der Verbesserung des ISMS dar, da hierbei risikominimierende Maßnahmen identifiziert und in Risikobehandlungspläne zur Umsetzung aufgenommen werden. Außerdem wird über die Risikobehandlung die Umsetzung dieser Maßnahmen überwacht und deren Wirksamkeit bewertet.
- Festgestellte Mängel und/oder Nichtkonformitäten müssen korrigiert bzw. abgestellt werden. Um das erneute Auftreten desselben Fehlers zu verhindern, ist es erforderlich, eine nachhaltige Ursachenermittlung zu betreiben und Korrekturmaßnahmen festzulegen.

Kontinuierliche Verbesserung– Hinweise zur Dokumentation:

In der ISO/IEC 27001 sind folgende Mindestanforderungen zur Dokumentation festgelegt:

- Nachweise über die Art von Nichtkonformitäten sowie über alle entsprechenden Korrekturmaßnahmen, die umgesetzt wurden
- Nachweise über die Ergebnisse der Korrekturmaßnahmen (Wirksamkeitsnachweis)

Darüber hinaus haben sich in der Praxisfolgende Dokumente als zielführend und hilfreich erwiesen:

- Beschreibung der Verfahren für Korrekturmaßnahmen (ab Abschnitt 10.1 c)
- Beschreibung des Incident-Managements und der Verfolgung von Korrekturmaßnahmen
- Hinweise zum Umsetzungsstatus von Korrekturmaßnahmen – idealerweise mit Hilfe eines Werkzeugs zur Nachverfolgung

Sascha M. Zaczyk, Senior Consultant für Informationssicherheit und Governance, International Certified Lead Auditor ISO 27001, zertifizierter Lead Auditor EN 50600, zertifizierter (Agile) ITIL-Experte & Datenschutzbeauftragter, Professional Scrum Master, iTSM Group, *www.itsmgroup.com*

Klinische Abläufe werden nur lückenhaft durch IT unterstützt

Zwischenauswertung von Nutzerdaten des Analysetools Check IT

Mit dem vom Marburger Bund und dem Bundesverband Gesundheits-IT entwickelten Analysetool Check IT haben Ärztinnen und Ärzte seit Ende Mai 2019 die Möglichkeit, eine systematische Nutzenbewertung von IT-Lösungen in 88 klinischen Einzelprozessen vorzunehmen. Mehr als zweihundert Krankenhausärzte haben inzwischen Check IT genutzt und mit der umfangreichen Checkliste gearbeitet. Basierend auf dem Stand vom 2. Oktober 2019 liegt nun eine erste Zwischenauswertung vor, die auf fundierten Daten zur Prozessunterstützung (Verfügbarkeit & Nutzung), Nutzbarkeit (Usability) und dem Nutzen (Wirkung) von IT-Lösungen in klinischen Arbeitsprozessen fußt.

Digitaler Reifegrad: 48 Prozent

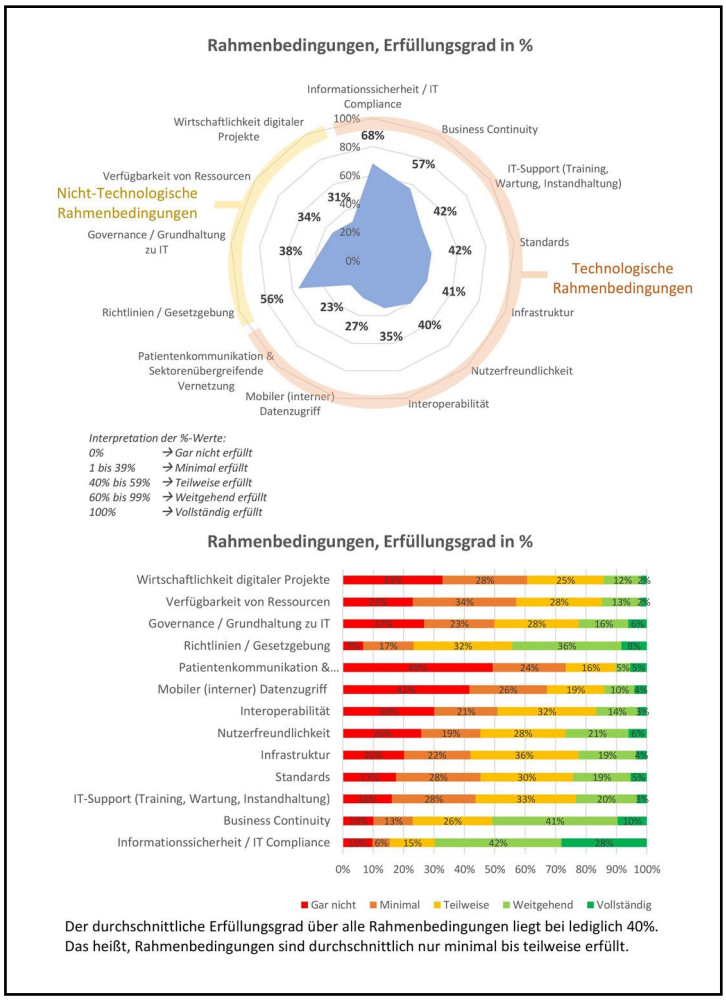
Der durchschnittliche digitale Reifegrad der teilnehmenden Kliniken liegt bei 48 Prozent. Im Gesamtergebnis werden klinische Prozesse nur teilweise und lückenhaft durch IT unterstützt, einerseits aufgrund fehlender Verfügbarkeit, andererseits aufgrund eines Nebeneinanders von analogen und digitalen Prozessen oder einer unzureichenden Funktionalität zur vollständigen Prozessunterstützung. Etwa die Hälfte der Teilnehmer gibt an, dass die notwendige Software nicht überall verfügbar ist, wo sie benötigt wird.

Die technologischen und nicht-technologischen Rahmenbedingungen sind nach Auffassung der Teilnehmer meist nur minimal bis teilweise erfüllt. Nur 16 Prozent der Teilnehmer stimmen weitgehend oder vollständig der Aussage zu, dass mobile Endgeräte und damit nutzbare klinische Programme verfügbar sind. Etwas besser sieht es mit einer WLAN-Verfügbarkeit aus – diese ist für 26 Prozent der Teilnehmer weitgehend oder vollständig erfüllt.

Die mit deutlichem Abstand am ehesten erfüllten Rahmenbedingungen sind: kontrollierter Datenzugriff, IT-Sicherheit und Datenschutz. Leider wirkt sich das nicht fördernd auf die Nutzenentfaltung von IT aus. Etwa ein Drittel aller Teilnehmer schätzt diese Rahmenbedingungen sogar als hemmend ein.

Vom Feedback zum Relaunch

Check IT hat in wenigen Monaten mehr Resonanz erfahren, als zu erwarten war. Durch die vielen Rückmeldungen konnte die Checkliste für die Anwender weiter verbessert werden, sodass nun am 8. November 2019 die neueste Version von Check IT an den Start ging. Einzelne Verbände und Krankenhausträger haben Interesse bekundet, das Analysetool in ihrem Bereich



Rahmenbedingungen

bekannt zu machen und einzusetzen. Weitere Gespräche werden folgen, um den Anwenderkreis stetig zu erhöhen.

Als ebenso hemmend wird die fehlende Unterstützung durch IT-Programme gesehen, die häufig nicht die benötigten Funktionen haben, um alle Arbeitsschritte digital umzusetzen. Die Teilnehmer bemängeln auch die Nutzerfreundlichkeit von Hard- und Software, vielfach gelten ihnen die digitalen Arbeitsmittel als veraltet. Auch die unzureichende sektorenübergreifende Vernetzung wird als sehr hinderlich wahrgenommen.

Auffallend ist, dass die Teilnehmer vor allem bei der Bewältigung von Dokumentationsaufgaben schon jetzt eine erhebliche Entlastung durch digitale Anwendungen erfahren. Zudem sind IT- Lösungen eine große Hilfe bei organisatorischen Prozessen und beim Austausch von Daten.

DIE 10 AM HÄUFIGSTEN IN KLINISCHEN PROZESSEN ERSCHLOSSENEN NUTZEN

- Die Dokumentationsqualität erhöht sich.
- Die Verfügbarkeit von klinischen Informationen wird verbessert.
- Bessere Bewältigung von Dokumentationspflichten und Bürokratie.
- Der Status von Aufträgen und Verordnungen kann besser verfolgt werden.
- Die Patientensicherheit wird höher.
- Arbeitsabläufe werden durch Standardisierung von Behandlungsprozessen unterstützt.
- Der Einsatz von Personal, Zeit, Raum und Material kann besser gesteuert werden.
- Es erfolgt eine Standardisierung der klinischen Dokumentation in Struktur und Terminologie.
- Die interdisziplinäre Zusammenarbeit wird verbessert.
- Ein kontinuierliches Qualitätsmonitoring wird ermöglicht und verbessert.

www.mb-checkit.de

Patient IT: Kann die Cloud das Heilmittel sein?

Modernisierungszwang versus Kostendruck – kaum eine Branche leidet mehr unter diesem Zielkonflikt als das Gesundheitswesen im Allgemeinen und die Krankenhäuser im Besonderen. Doch anders als in den meisten Branchen kann die Cloud hier kaum die Lösung sein – es sei denn, sie kommt in die Rechenzentren der Kliniken. ***Von Markus Biesinger, EMEA Healthcare Systems Engineer, Nutanix***

eHealth heißt das Ziel in der IT der Gesundheitsbranche, das jedoch immer noch in weiter Ferne zu liegen scheint. Die Vision ist eine durchgängige digitale Infrastruktur vom Patienten bis zu den Gesundheitsträgern. Diese muss nicht nur hoch performant sein, sondern vor allem auch sicher und hochverfügbar. Doch anstatt Berichte über Erfolge auf dem Weg, diese Vision Wirklichkeit werden zu lassen, bestimmen andere Schlagzeilen die Berichterstattung: Erpressersoftware legt die IT in Kliniken lahm, sensible Bilddateien von Patienten sind im Internet ungeschützt abrufbar – nur zwei Beispiele, die den Eindruck hinterlassen, dass der wahre Patient im Gesundheitswesen die IT ist.

Um schneller neue Applikationen bereitzustellen und die steigenden Erwartungen der Anwender an Bedienkomfort, Schnelligkeit und Zuverlässigkeit zu erfüllen, haben in den vergangenen Jahren die Unternehmen und Organisationen aus anderen Branchen verstärkt auf die verschiedenen Angebote der Public Cloud zurückgegriffen – von der Infrastruktur über Plattformen für Entwicklung, Tests und Bereitstellung neuer Anwendungen bis zur bedarfsorientierten Nutzung kompletter Softwareangebote.

Hindernisse auf dem Weg zur Genesung

Im Gesundheitswesen und insbesondere in den Kliniken im deutschsprachigen Raum schlägt diesen Angeboten weiterhin Skepsis entgegen. Und dies aus gutem Grund, ist der Weg zur Genesung der Krankenhaus-IT doch voller Hindernisse: Nach wie vor sind die meisten IT-Applikationen im Klinikbetrieb nicht Cloud-nativ. Das heißt, sie wurden nicht für den Betrieb in der Cloud geplant oder optimiert. Eine Vorstufe zu „Cloud-nativ" ist die Virtualisierung. Zwar können die allermeisten klinischen Workloads heutzutage auf Basis von virtuellen Maschinen betrieben werden. Doch es finden sich immer noch Anwendungen, die nicht virtualisiert werden können oder etwa aufgrund komplexer Lizenzierungshürden nicht virtualisiert werden sollen.

„Langsame" WAN-Verbindungen mit hohen Latenzzeiten sind eine weitere große Hürde auf dem Weg in die Cloud. Informationen können deshalb nicht schnell genug in die Cloud geschickt oder von dort wieder abgerufen werden. Dabei können selbst wenige Millisekunden entscheidend sein: Gerade bei großvolumigen Dateien, z. B. bei bildgebenden Diagnostikverfahren, verhindert dieser Flaschenhals ein effizientes Arbeiten.

All diese Hürden ließen sich prinzipiell durch finanzielle Anstrengungen aus dem Weg schaffen – wenn nur genügend Geld zur Verfügung stünde. Doch auch hier sieht speziell in den Krankenhäusern die Wirklichkeit anders aus: IT-Budgets stehen, selbst wenn sie nicht gekürzt werden, unter einem enormen Kostendruck. Sparen statt investieren scheint hier die Devise zu lauten. Und dort, wo Budgets erhöht werden, reichen diese Steigerungen nicht aus, um die vorhandenen Infrastrukturen grundlegend und in einem überschaubaren Zeitraum zu modernisieren. Denn die Wahrheit ist: Für Innovationen hat man weder Personal noch Budget. Nahezu alle Ressourcen werden dafür verwendet, lediglich den Betrieb am Laufen zu halten.

Hinzu kommt noch eine weitere Schwierigkeit, die oftmals in der Diskussion zu kurz kommt. Leistungen in der Public Cloud werden nach Verbrauch abgerechnet. Daher erscheinen sie auf den ersten Blick oft günstiger, als wenn sie in den Rechenzentren der Krankenhäuser erbracht würden. So allgemein formuliert, ist diese Aussage jedoch irreführend. Spätestens wenn Cloudservices mit ähnlichen Verfügbarkeiten wie im eigenen Rechenzentrum abgesichert werden sollen, also im 24-Stundenbetrieb in der 7-Tage-Woche, erreichen die Kosten schnell neue Dimensionen. Nicht genutzte Serverinstanzen, ein geringerer Rechen- und Speicherbedarf als ursprünglich angenommen, eine nur unregelmäßige Abstimmung der Abonnements auf den tatsächlichen Bedarf und steigende Ausgaben für zusätzliche Services, um die Public Cloud an die eigenen spezifischen Bedürfnisse anzupassen – all das lässt den Rechnungsbetrag höher ausfallen als geplant. Von der steigenden technologischen Abhängigkeit von einem oder mehreren Public-Cloud-Anbietern ganz zu schweigen.

Und dennoch: Die öffentliche Cloud hat einen neuen IT-Standard gesetzt mit ihren unschlagbaren Vorteilen:

- Plattformen, Dienste oder Applikationen können innerhalb von Sekunden bereitgestellt und konsumiert werden
- abgerechnet wird nur das, was benötigt wird und nur für die Dauer der Nutzung
- Bedienung und Verwaltung erfolgt hochautomatisiert, tiefes Fachwissen für die zugrundeliegende Infrastruktur ist nicht notwendig
- Innovation findet kontinuierlich und im laufenden Betrieb statt; neuere und bessere Funktionen verbessern ständig die genutzten Dienste

Die Ziele für die Krankhaus-IT sind damit klar und deutlich formuliert. Doch wie gelingt die vollständige Genesung – auch und gerade im Hinblick auf die im Gesundheitswesen so essenziellen Themen IT-Sicherheit und Datenschutz? Schließlich ist der Betrieb hunderter klinischer und nichtklinischer Applikationen kaum zu beherrschen, so dass Patches oder Updates nur sehr zeitverzögert oder gar nicht implementiert werden. Das öffnet Kriminellen und Spionen Tür und Tor.

Ist der Patient IT also noch zu retten, auch wenn er sich das Heilmittel Public Cloud nicht leisten und nicht einnehmen kann? Oder gibt es ein Generika-Medikament, das zwar dieselben Wirkstoffe enthält, jedoch in einer anderen Darreichungsform sowie zu einem günstigeren Preis erhältlich ist?

Generika statt Placebo

Diese Medizin existiert und sie heißt Private Cloud auf Basis einer hyperkonvergenten Infrastruktur (HCI). HCI basiert durchweg auf Standard-Hardware: x86-Server, die nur über Ethernet miteinander verbunden sind. Komplizierte SAN-Systeme, FC-Netzwerke für Storage Systeme oder andere teure Spezialkomponenten gehören damit der Vergangenheit an. Alles basiert auf Standard-Server-Komponenten. Die eigentliche Intelligenz ist die Software, die auf allen Servern läuft und die Ressourcen verwaltet. Doch zu einer soliden Private-Cloud Strategie gehört viel mehr als nur HCI:

- ein vollständig automatisierter Update-Prozess für Hardware (BIOS und Firmware) und Software
- Unabhängigkeit von Hardware
- Unabhängigkeit von Hypervisoren
- verschiedenste Storage-Technologien (NAS, Object, iSCSI) können einfach per Software freigeschalten und genutzt werden

zusätzlich zu dem Betrieb von virtuellen Maschinen können moderne Container-basierte Anwendungen – z. B. auf Basis von Kubernetes – auf derselben Plattform betrieben werden automatisiertes Bereitstellen und Verwalten von Applikationen mit Self-Service Funktionalität.

Überwachung und Absicherung des Datenverkehrs

HCI ermöglicht einen sehr flexiblen und skalierbaren IT-Betrieb. Scale-Out ist hier das Schlagwort. Benötigt ein Service mehr Ressourcen, können diese schnell und unkompliziert

hinzugefügt werden; sind Ressourcen frei oder ungenutzt, lassen sie sich entfernen oder für anderes Services verwenden. Dadurch wird Infrastruktur sehr granular planbar und erweiterbar. Besonders anschaulich lässt sich das am Beispiel einer PACS (Picture Archiving and Communication System)- oder VNA (Vendor Neutral Archive)-Lösung darstellen. Im klassischen Rechenzentrum wurde ein solches Projekt oft auf fünf Jahre oder länger ausgelegt. Das heißt, dass der berechnete notwendige Speicherplatz für die gesamt Projektlaufzeit bereits ab dem ersten Tag bereitgestellt und bezahlt wurde. Im Umkehrschluss bedeute das, dass ein Großteil der Gesamtkapazität bis zum Ende der Laufzeit ungenutzt blieb. Mittels Cloud-Technologie lässt sich die Infrastruktur granularer planen und bereitstellen, so dass nur sehr wenige Ressourcen ungenutzt bleiben. Erweiterungen erfolgen in HCI-Infrastrukturen unterbrechungsfrei und in kleinen Schritten, und zwar nur dann, wenn es wirklich notwendig wird. Angesichts des anhaltenden und deutlichen Preisverfalls bei IT-Komponenten wird schnell deutlich, dass dadurch enorme Kostenersparnisse realisierbar sind.

Ganzheitliche Medizin

Offenheit ist eines der grundlegenden Prinzipien von HCI-Infrastruktur. Zu dieser Offenheit gehört zum Beispiel die Fähigkeit, Services bei Bedarf auch in die Public Cloud oder aus der Public Cloud zurück ins eigene Rechenzentrum zu verschieben. Das ist insbesondere bei Anwendungen interessant, deren Ressourcenverbrauch starken Schwankungen unterliegt und schwer vorhersehbar ist, beispielsweise Forschungsprojekte im akademischen Umfeld. Damit aber dieser dynamische Ressourcenverbrauch nicht zu unerwünschten Kosteneffekten führt, sollte eine moderne Cloud-Plattform ein zentrales Management sämtlicher Workloads anbieten – ob in der öffentlichen Cloud oder auf Basis von HCI im eigenen Rechenzentrum. IT-Silos und Medienbrüche aufgrund unterschiedlicher Technologie-Stacks gehören damit der Vergangenheit an. Eine echte private Cloud auf Basis von HCI ist die beste Medizin für den Patient IT, weil ihr ein ganzheitlicher Ansatz zugrunde liegt. Damit nicht mehr der Betrieb einer veralteten Infrastruktur im Zentrum der Krankenhaus-IT steht, sondern die Applikationen, die das Klinikpersonal zum Wohle der Patienten optimal unterstützen.

Details der KH-IT-Herbsttagung 2019

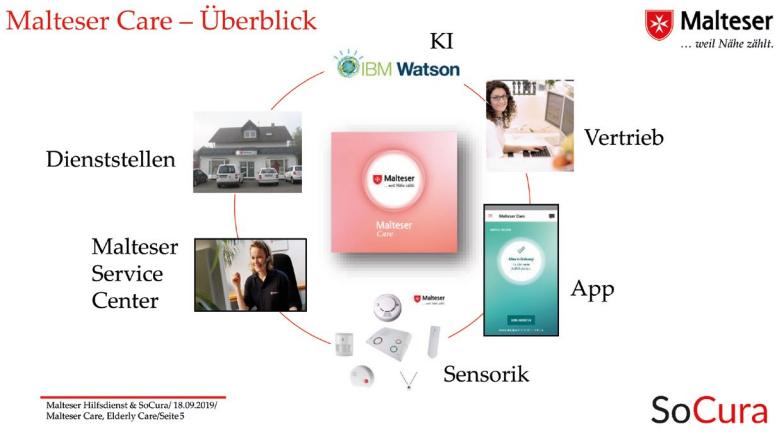
Elderly Care/Malteser Care – Realität und Potenzial

Nahezu alle Betreuungsleistungen für ältere Menschen werden im häuslichen Umfeld erbracht. Die Ziele sind klar: Menschen optimal und proaktiv begleiten; Eigenständigkeit und Lebensqualität so lange erhalten wie möglich. Smarte Technologien können einen wertvollen Beitrag leisten, das Management von Unterstützungsleistungen möglichst effizient zu gestalten. Dazu müssen wir auf innovative Technologien setzen – ebenso aber auch unsere Prozesse kritisch hinterfragen und an die Erfordernisse der Praxis anpassen. Die Autoren *Bernd Falk*, Bereichsleiter Malteser Service Center, und *Uta Knöchel*, CTO, SoCura, präsentierten das Thema auf der Herbsttagung des Bundesverbandes KH-IT e.V. am 18. und 19. 9. 2019 im Universitätsklinikum Erlangen.

Vernetzung lautet das Zauberwort! Vernetzte Systeme, intelligente Tools, sektorübergreifende Plattformen – alles Ansätze, die verfügbaren Ressourcen noch besser zu nutzen. Schauen wir uns den Hausnotruf (HNR) im Detail an. An ihm lässt sich auch aufzeigen, wo noch Potenziale vorhanden sind. Bereits der klassische HNR erhöht die Sicherheit in der häuslichen Pflege, oft auch im Anschluss an eine Krankenhausbehandlung. Das aktive Auslösen eines Alarms, z. B. über einen Notfallknopf, alarmiert ein Service Center, das Hilfe auf den Weg schickt.

Diese Art des Hausnotrufs ist gleichwohl limitiert: Nicht immer sind Hilfsbedürftige in der Lage, aktiv einen Alarm auszulösen. Genau hier setzt unser neuer Service Malteser Care an. Das Pilotprojekt mit 17 Teilnehmern wurde im September erfolgreich abgeschlossen, seitdem hat die Rollout-Phase und eine weitere Evaluation mit 40 Teilnehmern zusammen mit der GKV unter universitärer Begleitung begonnen. Neben der Notruf-Basisstation wurden in Wohnungen von älteren Menschen Sensoren angebracht und vernetzt: Bewegungs- und Kontaktsensoren, Sensormatten, Feuchtigkeitssensoren und Feuermelder.

Die Sensoren erkennen bestimmte Events, wie z. B. Fenster öffnen oder schließen, und lösen anhand vorher festgelegter Kriterien Alarme aus. Kritische Alarme, die aktiv durch einen Teilnehmer ausgelöst werden, wie das Auslösen des Brand- oder Wassermelders, lösen direkt einen Notruf zum Malteser Service Center aus oder verständigen im Brandfall die Feuerwehr. Bei unkritischen (aber eben kritisch werden könnenden) Alarmen wird über eine App ein Angehöriger verständigt. Neben Statusangaben zur Wohnung und auch Information zu Notrufen unterstützt eine Chat-Funktion die Kommunikation, eine Alarmierung des Malteser Service Center ist jederzeit direkt möglich. Reagiert ein angehöriger nicht zeitgerecht, bekommt das Malteser Service Center einen Hinweis und kann reagieren.



Malteser Care im Überblick – nur im Zusammenwirken der Sensorik mit der KI Watson sowie mit dem Malteser Service Center (MSC), der Angehörigen – App und den Dienststellen vor Ort (DST) kann ein qualitätsgesicherter Service erbracht werden

Das System ist GKV-zugelassen. Die Kommunikation der Sensoren mit der Basisstation wird über Funk-Frequenzen, der Basisstation mit der Zentrale über GSM für Sprach- bzw. 3G für die Datenübertragung umgesetzt. Zeitnah kommt LTE zum Einsatz.

Malteser Care arbeitet mit der KI IBM Watson, die individuelle Bewegungs- und Handlungsprofile erheben und so eine noch genauere Steuerung der Unterstützungsleistung ermöglichen soll. Im Moment stehen hier die regel- und musterbasierten Analysen im Zentrum der Analytik, erst mit zunehmenden Datenpool werden auch über Big Data Analysen immer mehr Rückschlüsse möglich. Gerade im Anlern-Modus ist es wichtig, dem Qua-

Modell einer „Malteser Care"-Wohnung. Im Vordergrund die Basisstation, der Notruf-Button und je 2 Kontakt- und Bewegungssensoren (Quelle: SoCura)

litätsanspruch gerecht zu werden und nicht durch „unnötige" Alarme Aufwand im Service Center zu erzeugen oder die Hausnotruf-Nutzer zu erschrecken. Neu eingehende Daten werden mit individuellen Profilinformationen abgeglichen und Vergleichsprofile für die Ermittlung der „next best action" herangezogen.

Die Potenziale des Systems sind bei weitem noch nicht ausgeschöpft: Die KI wird im Laufe der Zeit auch Verhaltensveränderungen erkennen, die auf bestimmte Krankheiten (wie etwa Demenz) hindeuten. Aber auch die selbständige Identifizierung von Notfallsituationen sind vorstellbar.

Im Projektverlauf waren diverse Stolpersteine zu überwinden: Bei Akkus, Schnittstellen und Sensortechnik wurde zunächst Lehrgeld bezahlt. Natürlich gab es auch den einen oder anderen Fehlalarm; mittlerweile funktioniert die Sensortechnik zuverlässig. Die SoCura, IT-Tochter der Malteser, konnte die Herausforderungen im Schnittstellenumfeld lösen.

Malteser Care kann spürbar für die Entlastung von Nutzern und Angehörigen durch ein höheres Sicherheitsempfinden sorgen sowie ein „länger zu Hause leben" unterstützen; aber es gibt auch Bedenken. Mal losgelöst von Datenschutzfragen: Wie empfinden die Patienten rein subjektiv diese „Überwachung"? Und könnte die „Ruhe im Kopf" bei den Angehörigen dazu führen, dass weniger zwischenmenschlicher Kontakt entsteht?

Richtig angewendet sind Assistenzsysteme eine wertvolle Hilfe für Pflegebedürftige und ihr Umfeld. Im Zusammenspiel mit dem Mobilen Notruf, Telemedizin-Zentren oder auch im Einsatz der Sensorik im Krankenhaus ergeben sich interessante Ansätze für die Diskussion.

Malteser Hilfsdienst

Der Malteser Hilfsdienst mit seinen ehrenamtlichen und hauptamtlichen Mitarbeitern (insgesamt ca. 100.000 Mitarbeiter, ca. 900 Einrichtungen, mit Malteser Deutschland auch im Krankenhausbereich aktiv) bietet ein deutschlandweites Netz mit umfassenden Unterstützungsleistungen an – von ambulanter bis stationärer Pflege – sowie Versorgungsleistungen – von Menü- über Fahrdienst bis hin zum Hausnotruf. 2019 zählte das Malteser Service Center ca. 120.000 Hausnotruf-Kunden.

Die Malteser übernehmen dabei die Funktion des „Kümmerers", denn nur funktionierende und einfach zu handhabende Technik wird wirklich genutzt. Die Brücke zu bauen, die von komplexen Systemen zu einer einfachen Nutzung führt, ist eine wichtige Aufgabe.

SoCura

Die SoCura GmbH ist eine Tochtergesellschaft des Malteser Verbundes. Sie bietet Dienstleistungen aus einer Hand für die Bereiche Buchhaltung, Personal-Service und IT. Das Unternehmen aus Köln betreibt die gesamte IT-Landschaft der Malteser in Deutschland. Dabei betreut die SoCura insgesamt 25.000 IT-Arbeitsplätze und leistet First-Level- bis Third-Level-Support für mehr als 200 Fachanwendungen.

Bernd Falk, Bereichsleiter, Malteser Service Center
Quelle: Bernd Falk

Uta Knöchel, CTO, SoCura
Quelle: UKSH

Details der KH-IT-Herbsttagung 2019

Das Krankenhaus der Zukunft

Unser Gesundheitssystem und insbesondere die Krankenhäuser stehen gesellschaftlichen, organisatorischen, medizinischen und finanziellen Herausforderungen gegenüber und müssen sich den stetig verändernden Rahmenbedingungen anpassen (siehe Abbildung 1). Neben dem demographischen Wandel und der damit verbundenen Multimorbidität zählen hierzu steigende Anforderungen an Qualität und Dokumentation, Ambulantisierung und Patientenerwartungen. Weiter verschärft wird die Situation durch enormen Kostendruck und akuten Fachkräftemangel. Der Autor Julian Schiele „ Universität Augsburg, präsentierte das Thema auf der Herbsttagung des Bundesverbandes KH-IT e.V. am 18. und 19. 9. 2019 im Universitätsklinikum Erlangen.

Inspiriert vom Konzept der Industrie 4.0 können technische und organisatorische Innovationen auch im Krankenhaus einen wertvollen Beitrag zur Bewältigung dieser Herausforderungen leisten. Basierend auf cyberphysikalischen Systemen und Datenanalytik werden die Support- und Kernprozesse im Krankenhaus der Zukunft automatisiert, digitalisiert, personalisiert, integriert und vernetzt sein. Das Krankenhaus der Zukunft wird sich durch weniger Bürokratie, effizientere Prozesse, höhere Mitarbeiterzufriedenheit, mehr Zeit für wertschöpfende Aufgaben und Patienten, bessere Medizin und eine bessere Behandlung auszeichnen.

Da jedoch im Gegensatz zur Industrie 4.0 nicht ein Produktionsprozess, sondern ein Diagnose- und Therapieprozess im Mittelpunkt steht, wird die menschliche Komponente stets unerlässlich bleiben und das Konzept vielmehr als Unterstützung statt als Ersatz dienen. Wir am UNIKA-T haben eine umfassende Umfrage mit mehr als 265 Krankenhaus-Experten wie Managern, Ärzten, Krankenschwestern und IT-Experten durchgeführt, um die Vision für das Krankenhaus der Zukunft im Jahr 2040 zu schärfen und um individuelle Erfahrungen aus der Praxis zu erweitern. Bei den Teilnehmern handelt es sich zu je ungefähr einem Drittel um Mediziner*innen, Manager*innen und IT-Fachkräfte aus unterschiedlichen Kliniken, vorwiegend in öffentlicher Trägerschaft (65% der Teilnehmer), Maximalversorger (59%), mit mehr als 1,500 Betten (31%) und mit Fokus auf Deutschland (95%). Große Universitätskliniken wie beispielsweise Charité, UK Hamburg-Eppendorf und das neu gegründete UK Augsburg wurden ebenso befragt wie kleinere Kliniken und Krankenhausketten. Abbildung 2 veranschaulicht, wie sich die Teilnehmer das Krankenhaus der Zukunft vorstellen.

Der aktuelle Stand unterscheidet sich stark zwischen den einzelnen Häusern, jedoch zeichnet sich überall ein großer Nachholbedarf ab (siehe Abbildung 3). Viele Krankenhäuser sind noch auf papierbasierte Dokumentation und Faxgeräte angewiesen, während andere bereits mit Pflegerobotern und 3D-Druckern experimentieren. In einem durchschnittlichen Krankenhaus werden heutzutage 33% der Prozesse manuell, 52% IT-unterstützt (z.B. Excel) und 15% automatisiert durchgeführt. Die Umfrage offenbart, dass Krankenhäuser hohe Ambitionen für die Zukunft haben und große Vorteile erwarten (93%). Die Mehrheit (85%) plant eine zeitnahe Umsetzung des Konzepts, davon die meisten (62%) schon innerhalb der nächsten 2 Jahre. Nicht wenige Krankenhäuser haben bereits mit der Entwicklung, Detaillierung und Umsetzung ausgewählter Anwendungsfälle begonnen. Zu den häufigsten Anwendungen zählen die digitale Patientenakte, Krankenhausinformationssysteme, digitale Überwachung von Vitalparametern und OP-Roboter. Einige Teilnehmer erwähnten auch automatisierte Personaleinsatzplanung, digitale OP-Planung, automatische Bilderkennungsverfahren, Telemedizin und Unit Dose Systeme in der Apotheke. Auch wenn diese einzelnen Leuchttürme innovativ und nützlich sind, so fehlt den meisten Krankenhäusern doch eine ganzheitliche Strategie auf dem Weg zum Krankenhaus der Zukunft.

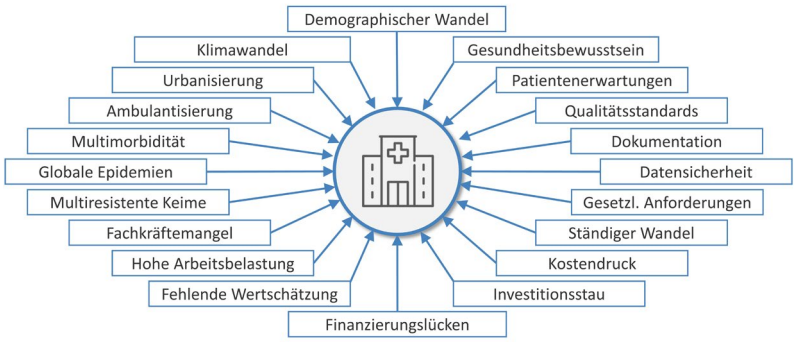


Abbildung 1: Gesellschaftliche, organisatorische, medizinische, und finanzielle Herausforderungen

Abbildung 2: Visionen für das Krankenhaus der Zukunft (basierend auf Umfrage)

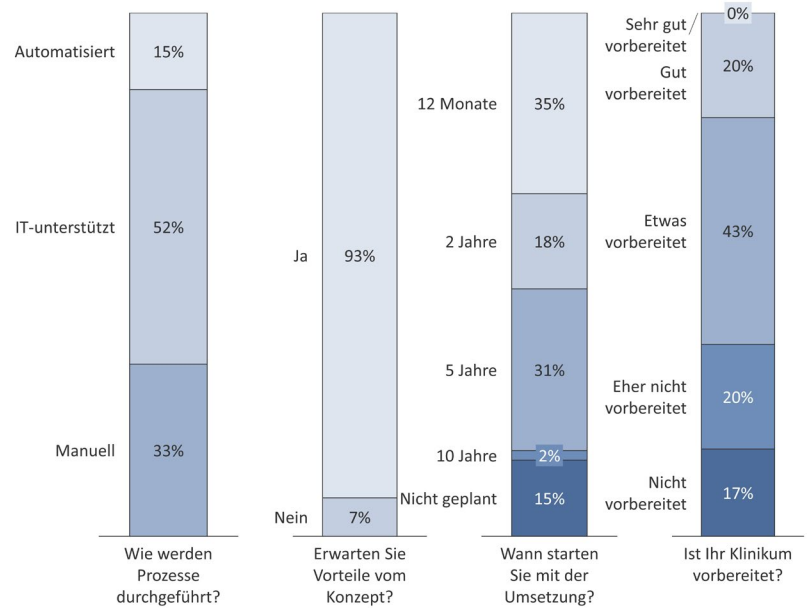


Abbildung 3: Aktueller Stand und Ambitionen für die Zukunft

Um das Krankenhaus der Zukunft greifbarer zu machen, haben wir am UNIKA-T unter Leitung von Prof. Dr. Jens O. Brunner ein konzeptionelles Framework entwickelt, das in 32 Dimensionen entlang von sieben Bereichen strukturiert ist. Damit die Vision Realität werden kann, werden zudem vier Enabler vorausgesetzt: Mitarbeiterfähigkeiten, IT Infrastruktur, eine ganzheitliche Strategie sowie eine geeignete Steuerungsform. Wir entwerfen momentan ein Tool, mit welchem sich Krankenhäuser selbst einschätzen und mit anderen Häusern vergleichen können. Unsere Arbeit soll Krankenhausmanagern als Orientierungshilfe dienen, um ihr Krankenhaus strukturiert und nachhaltig in das neue Zeitalter zu führen.

Julian Schiele
„Universitäres Zentrum für Gesundheitswissenschaften am Klinikum Augsburg (UNIKA-T), Lehrstuhl für Health Care Operations/Health Information Management, Wirtschaftswissenschaftliche Fakultät
julian.schiele@unikat.uni-augsburg.de

UNIKA-T im Profil

Das Universitäre Zentrum für Gesundheitswissenschaften am Klinikum Augsburg (UNIKA-T) ist ein vom Universitätsklinikum Augsburg, der Universität Augsburg, der Technischen Universität München und der Ludwig-Maximilians-Universität München gemeinsam getragener Forschungsverbund mit Sitz in Augsburg. Der Lehrstuhl für Health Care Operations/Health Information Management von Prof. Dr. Jens O. Brunner befasst sich schwerpunktmäßig mit der Planung und Analyse von strategischen und operativen Dienstleistungsprozessen im Gesundheitssektor, vor allem in Krankenhäusern.
Weitere Informationen: ***www.unika-t.de/brunner***

Digitalisierung im Neubau – Innovation und strategische Planung

In der Universitätsmedizin Göttingen steht die Erneuerung und Modernisierung der zentralen Gebäude der Krankenversorgung wie auch der Forschung und Lehre an. Sukzessive werden neue Gebäude errichtet und mit Abriss des alten Gebäudes wird jeweils Raum für die nächste Bauphase geschaffen. Zeitgleich wurde der Bedarf an einer zukunftsfähigen IT-Infrastruktur deutlich, ohne die die strategischen Ziele einer zeitgemäßen Krankenversorgung, sowie angestrebte neue Konzepte aus der Wissenschaft nicht erreichbar sind. Die Autoren Bernd Behrend und Alexander Koch präsentierten das Thema auf der Herbsttagung des Bundesverbandes KH-IT e.V. am 18. und 19. 9. 2019 im Universitätsklinikum Erlangen.

Mit der Erkenntnis, dass eine exzellente und zukunftsweisende Krankenversorgung sich nur mit einem hohen Digitalisierungsgrad und daher mit einer zukunftsfähigen IT-Infrastruktur erzielen lässt, wurde die strategische IT-Entwicklung als integraler Baustein in die Generalentwicklungsplanung aufgenommen und mit der Hospitaltechnik Planungsgesellschaft ein dedizierter Fachplaner für die Digitalisierung in das Planungsteam berufen.

Mit der Digitalisierungsstrategie der UMG wird das Ziel verfolgt, sich in ein intelligentes bzw. „smartes" Krankenhaus weiterzuentwickeln (siehe Definition der ENISA). Aufbauend auf einer IKT-Umgebung miteinander vernetzter Anlagen wird sich die UMG als intelligentes Krankenhaus auf optimierte und automatisierte Prozesse stützen, um die Patientenversorgung bestmöglich zu unterstützen. Dazu wird eine IKT-Umgebung von miteinander verbundenen Anlagen, im Sinne des Internets der Dinge (IoT), entwickelt.

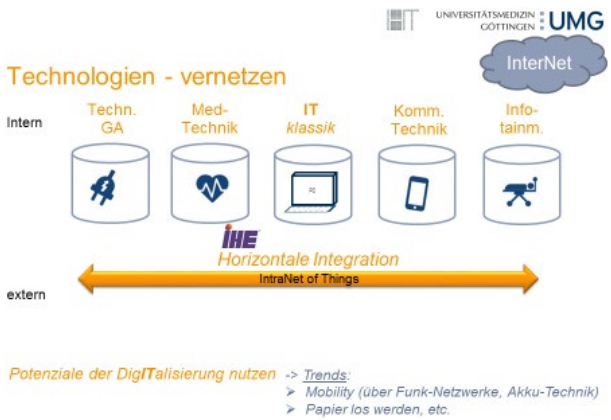
Regulatorische Anforderungen erfüllen

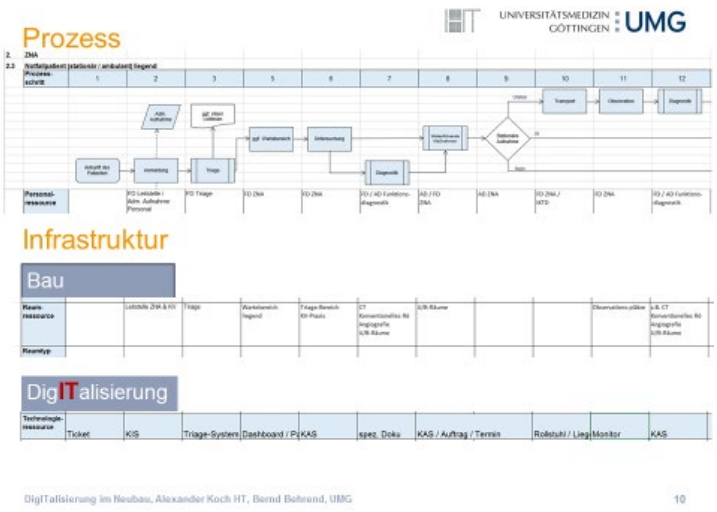
Gleichzeitig müssen die steigenden regulatorischen Anforderungen z. B. aus dem Medizinproduktegesetz oder der europäischen Datenschutzgrundverordnung berücksichtigt werden. Die UMG trägt als Klinikum der Maximalversorgung besondere Verantwortung im Rahmen der kritischen Infrastrukturen („KRITIS") und stellt sich mit einer resilienten und zertifizierten IT-Infrastruktur den steigenden Anforderungen der IT-Sicherheit. Oberste Priorität hat die Systemintegration mit der Zusammenführung von Informationstechnologie, Gebäudetechnik und Medizin- bzw. Forschungstechnik.

Mit den rasanten Fortschritten der Digitalisierung führt das Verschmelzen der verschiedenen Technikperspektiven zu neuen Formen von Steuerung, Überwachung und Automation. Kurz gesagt ist eine reibungsfreie Integration aller Geräte „Things" mit Display und Datenübertragung per Kabel oder Funk gefordert. Neben einfachen Anwendungen wie Fernwartung oder Zeitsynchronisation wird sich damit eine Vielzahl von Innovationen und Potenzialen zur Optimierung der Prozesse in der Klinik ergeben.

Potenziale für verbesserte Arbeitsabläufe

Während die Masterplanung zur baulichen Entwicklung einen Ausblick über die kommenden zwei Jahrzehnte bietet, sind die Entwicklungen der Digitalisierung wesentlich schwerer einschätzbar. Dennoch eröffnen Trends wie die zunehmende Vernetzung sowie – verbunden mit effizienterer Akku- und Funk-Technik – auch die zunehmende Mobilisierung neue stark wachsende Potenziale zur Gestaltung verbesserter Arbeitsabläufe. Sensoren halten nicht nur Einzug in die Gebäudeautomation, sondern auch in weitere Technikbereiche. Mit intelligenten Algorithmen lassen sich Aktoren immer präziser steuern, z.B. in der Medizintechnik entwickeln sich neben der Robotik im OP-Saal auch intelligente Prothesen oder gar Smarte Patientenbetten. Derartige Entwicklungen können bereits heute für die strategische Planung der Digitalisierung berücksichtigt werden. Allerdings sind Neubauprojekte typischerweise nach der HOAI in die klassischen Leistungsphasen Grundlagenermittlung, Vorentwurf, Entwurf, Ausführungsplanung etc. gegliedert und der Planungsprozess folgt einer strikten sukzessiven Verfeinerung der Planung von einer Phase zur nächsten und das im Rahmen eines klassischen starren Projektmanagements nach der Wasserfallmethode. Beide Herangehensweisen sowohl die inhaltliche als auch die von Seiten des Projektmanagements sind heute für Digitalisierungs-Themen nicht oder nicht mehr zielführend. Die Digitale Transformation von Krankenhäusern erfordert eine frühzeitige umfassende und detaillierte Auseinandersetzung mit Prozessen und Technologien, die im





wenig wie nötig“ verfolgt werden. Notwendig ist hierzu eine enge Verflechtung der Betriebsorganisation mit Bau und Technologie-Planung. Die Erfahrung zeigt, dass insbesondere bei der Prozessbetrachtung und –planung die verschiedenen Planungsbeteiligten sich auf die jeweils unterschiedlichen Vorgehensweisen und Bedürfnisse hinsichtlich der Detailschärfe in den Planungsphasen erst einstellen und Kompromisse finden müssen. Hier sind Planungsbeteiligte mit Erfahrung in diesen Themen sehr von Vorteil.

Sinne agiler Methoden iterativ an sich ändernde Anforderungen und Randbedingungen angepasst werden.

Innovative Technologien strukturiert einplanen

Mit der Analyse der administrativen und klinischen Arbeitsabläufe lassen sich die technologischen Möglichkeiten in die Planung integrieren. Ein guter Überblick über die erforderlichen Prozesse bietet die Möglichkeit, innovative Technologien strukturiert für die Verbesserung von Qualität und Effizienz einzuplanen.

Sind die Arbeitsschritte erst einmal transparent, können sie effektiver mit den Nutzern abgestimmt werden. Mit der Frage WO soll WAS geleistet werden (und in welcher zeitlichen Abfolge), lässt sich hinsichtlich der Architektur der Bedarf an Räumen ermitteln. Damit einhergehend kann zeitgleich die Frage geklärt werden, mit welchen technischen Arbeitsmitteln die Arbeitsschritte erledigt werden, d.h. auch die Ausstattung kann ermittelt werden. Wenn diese typischen Schritte der Planung gut miteinander vernetzt werden, lässt sich im Vorfeld eine gute Vorstellung der zukünftigen Ressourcen anhand eines „digitalen Zwillings“ entwickeln. Mit Methoden der „Building Information Modelling“ (BIM) lässt sich ein gutes Zielbild in mehreren Dimensionen entwickeln und mit den Nutzern abstimmen.

Unter Aspekten der Wirtschaftlichkeit sollte dabei der Grundsatz „so

ITK als Innovator und Moderator

Während der Bau sich auf die Anordnung und Ausstattung von Räumen fokussiert, bedient die Digitalisierung die Kommunikations- und Informationsbedürfnisse (ITK) aller beteiligten Berufs- und Personengruppen. Ihr kommt eine maßgebliche Rolle als Innovator und Moderator von effizienteren Arbeitsabläufen zu.

Die Digitalisierung und ihre Auswirkungen müssen dabei ganzheitlich unternehmerisch und nicht nur technisch betrachtet werden. Denn die notwendige Transformation der Organisation benötigt genauso so viel Zeit und Ressourcen wie der Bau und ist in der Projektplanung zu berücksichtigen. Nur so lassen sich die Potentiale der Digitalisierung identifizieren und durch eine auf das Bauprojekt abgestimmte Zeit- und Kostenplanung realisieren.

Alexander Koch, Bernd Behrend,

Stromkosten, Betriebskosten, Umweltkosten

Green-IT als Standortfaktor für Krankenhäuser

„Green-IT“ bedeutet für Krankenhäuser: Erheblich verbesserte Prozessunterstützung und optimierter Betrieb bei deutlich reduzierten Kosten. Dem hohen Energieverbrauch des smarten Internets sehen Klimaexperten mit Sorge entgegen. Innovative Klimatechnologien werden immer mehr zum wirtschaftlichen Standortfaktor. IT-Unternehmen denken über Digitalisierung als Problemlöser nach.

In Hamburg-Harburg ging im Mai 2019 die 92. Umweltministerkonferenz (UMK) zu Ende. Die Minister sowie Senatoren der Bundesländer und die Bundesumweltministerin haben u.a. Beschlüsse zu den Themen Klima, Düngung und Green-IT gefällt.

Zu „Green-IT“ lautet es in Top 24: Die Digitalisierung bietet große Chancen, ist aber auch mit einem hohen Energieverbrauch und CO2-Ausstoß verbunden. Die Konferenz bat den Bund, eine klimafreundliche IT-Nutzung in den Klimaplan des Bundes zu integrieren. Wichtige Punkte sind dabei die Energie- und Ressourceneffizienz von Rechenzentren (Kühlung, Abwärmenutzung), smarte Produktionsprozesse (Industrie 4.0), eine klimaschonende Beschaffung und Entsorgung von Hard- und Software sowie die effiziente Nutzung von Video- und Telefonkonferenzen zur Vermeidung von Dienstreisen.

Nachfrage nach Rechenleistung

Unter "Green-IT" sind umweltverträgliche Produkte und Dienstleistungen der Informations- und Kommunikationstechnik (IKT) sowie der Nutzung von IKT zur Umweltschonung zu verstehen. Dies umfasst die Berücksichtigung des gesamten Lebenswegs von IKT-Produkten sowie deren Auswirkungen auf das Klima und andere Umweltwirkungen, wie zum Beispiel die Inanspruchnahme kritischer Rohstoffe.

In Deutschland betrug der Stromverbrauch der IKT in vergangenen Jahren rund 47,8 Terawattstunden (TWh) und damit 8 Prozent des gesamten Stromverbrauchs des Landes. Obgleich Energieeffizienzsteigerungen in einigen Bereichen der IKT zum Beispiel durch die Green-IT-Initiative des Bundes oder die Einführung der Europäischen Ökodesign-Richtlinie erzielt werden konnten, steigt der Energiebedarf für Rechenzentren weiter erheblich an. Nach Expertenschätzungen wird vor allem der Energiebedarf der Server durch die hohe Nachfrage an Rechenleistung in deutschen Rechenzentren bis zum Jahr 2025 um mehr als 60 Prozent steigen.

Wichtiger Punkt: die Server werden immer dichter „gepackt“. Die Bauteile werden kleiner, aber der Energiebedarf steigt aufgrund der höheren Leistung. Gleichzeitig steigt die erforderliche Kühlleistung. Wesentlicher Punkt für Green-IT ist daher die bessere Energieeffizienz der Prozessoren, die immer noch die meiste Abwärme produzieren.

Mehr Effizienz erforderlich

Dem hohen Energieverbrauch des allgegenwärtigen Internets sehen indes nicht nur Klimaexperten mit Sorge entgegen. Der Trend geht zu immer größeren Rechenzentren, den Hyperscale-Rechenzentren. IT-Unternehmen bereitet der Stromhunger große Sorgen. Denn die Stromkosten verursachen hohe Betriebskosten. Nicht nur die Kosten sind kritisch, bereits die Bereitstellung der benötigten elektrischen Leistung stellt die Energieversorgung vor immense Probleme.

Immer mehr Unternehmen suchen daher nach Möglichkeiten, wie sie ihre Rechenzentren effizienter gestalten könnten. Im Fokus steht dabei die Kühlung der Server. Erste Erfolge zur Stromkosteneinsparung gibt es bereits: Eine moderne Technik hält höheren Temperaturen stand, das heißt die Geräte müssen dadurch weniger gekühlt werden. Früher wurden RZ auf 18 Grad herunter gekühlt. Heute gelten 24 Grad Raumtemperatur als Grenzwert. In den Systemen bedeutet das oft Kerntemperaturen von 60 Grad und mehr.

Einsparpotentiale bestehen auch in einer effizienteren Auslastung der Server. Anpassung der Leistung an die IT-Last lautet die Devise. Ist die Auslastung eines Servers gering, geht ein Teil in einen Stand-by-Betrieb, was weniger Strom verbraucht. Auch durch die Zusammenlegung kleiner Rechenzentren ließe sich Strom sparen.

Im Hinblick auf den IKT-Energieverbrauch öffentlicher Anwender gilt es, diese Steigerungen zu berücksichtigen und zu dokumentieren. Um dies sicherstellen zu können, verabschiedete der IT-Rat im Sommer 2017 den Beschluss 2017/14, in dem die Ziele der Initiative bis zum Jahr 2022 festgelegt wurden:

- Konsolidierung des durch den IT-Betrieb verursachten Energieverbrauchs in der Bundesverwaltung mit dem Ziel, den Wert von 350 Gigawattstunden pro Jahr bis zum Jahr 2022 nicht zu überschreiten
- Umsetzung einer nachhaltigen IT-Beschaffung, orientiert an den Vorgaben der Architekturrichtlinie und der Blaupause für die IT-Beschaffungsstrategie
- Anwendung der Kriterien des "Blauen Engels" bei der Bewertung der Energie- und Ressourceneffizienz in Rechenzentren Die IT-Dienstleister orientieren sich beim Ausbau ihrer Dienstleistungszentren an diesen Kriterien und berichten jährlich.

Green-IT erstreckt sich über mehrere Levels

- Energieeffizienz der Chips: CPU's werden immer kleiner und leistungsfähiger, verbrauchen dabei aber mehr Energie. Die geringe Baugröße bereitet Schwierigkeiten bei der Ableitung der erzeugten Wärme. Dem höheren Wirkungsgrad bei der Leistung kommt daher hohe Bedeutung zu.
- Energieeffizienz der Geräte: die Kühlung der Geräte durch von außen zugeführte Kaltluft ist nach wie vor Standard, Kühlung mit Wasser eher für Höchstleistungssysteme. Die Energieeffizienz eines Gerätes lässt sich durch optimale Luftführung durch das Gerät noch deutlich verbessern.
- Energieeffizienz der RZ: Früher wurde der gesamte Raum des RZ gekühlt, heute arbeitet man eher mit Kalt- und Warmgängen. Es gibt bereits Ansätze, bei denen die Kühlung noch näher am Gerät eingeblasen wird, so dass nicht einmal der Luftraum der Kalt- und Warmgänge gekühlt werden muss.
- Bereitstellung der Energie: Ökologisch ist es fragwürdig, aber ein RZ z.B. in der Arktis hat den Vorteil, dass kalte Luft ausreichend zur Verfügung steht – zur Kühlung wird keine Energie verbraucht. Allerdings ist die Langzeitwirkung einer solchen „Heizung" in kalten Gegenden wenig erforscht und sicher nicht gut.
- Konsequente Nutzung erneuerbarer Energiequellen spielt eine große Rolle, was große RZ-Betreiber bereits erkannt haben.

Wolf-Dietrich Lorenz, Chefredaktion Krankenhaus IT-Journal, Ehrenmitglied KH-IT

Jürgen Flemming, Vorstand KH-IT, Presse- und Öffentlichkeitsarbeit

Update Telematikinfrastruktur

Grundlage für die Roadmap der gematik [1] ist der Roll-Out der Telematikinfrastruktur (TI) als sichere Plattform. Während dieser für den vertragsärztlichen Bereich weitgehend erfolgt ist, stellt sich für die Krankenhäuser die Frage, ob und wann es einen leistungsfähigen RZ-Konnektor geben wird. Mehrere Ansätze sind in der Diskussion bzw. im Angebot: (I) Weiterentwicklung eines Einbox-Konnektors zu einem RZ Konnektor, (II) 19" Rack mit mehreren Einbox-Konnektoren (bis zu acht) und übergreifender Administration oder (III) Bereitstellung der benötigten "Konnektorleistung" über einen Dienstleister, der dafür Einbox-Konnektoren einsetzt.

Da die Verfügbarkeit eines zertifizierten RZ-Konnektors nicht absehbar ist, wurde der gesetzte Termin (31.12.2019, §219 Absatz 2b) im Beschluss des Bundestags [2] auf den 31.12.2020 verlängert. Damit erhält die Empfehlung der DKG, mit der Beschaffung entsprechender Komponenten abzuwarten [3] eine rechtliche Grundlage. Dieser Termin entspricht zudem der im DVG für die Krankenhäuser vorgesehenen Frist zum 1.1.2021 [2] die Anbindung an die TI und die Ausstattung für die Anwendung „elektronische Patientenakte" gemäß §291a umzusetzen.

Für die elektronische Patientenakte nach §291a hat die gematik zum Ende des Jahres 2018 eine umfangreiche Spezifikation vorgelegt und in Revisionen vom Januar, Mai, Juni und November 2019 weiterentwickelt. Diese erlaubt dem gesetzlich Versicherten eine §291a Akte i. d. R. bei seiner Krankenkasse zu führen, die gemäß Terminservice und Versorgungsgesetz (TSVG) [4] zum 1.1.2021 von Krankenkassen angeboten werden muss. Der Zugriff auf die Akte erfolgt aus Sicht des Patienten über ein Patientenportal; aus Sicht des Leistungserbringers über sein Primärsystem, in das die Aktenfunktion integriert wird und das mit dem zugehörigen Fachmodul im Konnektor kommuniziert. Obwohl die Spezifikation auf IHE Profile setzt, weicht sie in wesentlichen Aspekten von den Vorgaben von IHE ab, zum Beispiel werden grundlegende IHE Profile wie CT (Consistent Time) oder ATNA (Audit Trail and Node Authentication) nicht verwendet. Ebenso werden IHE XDS Beziehungen („associations") zwischen Dokumenten ausgeschlossen, die üblicherweise zur Historisierung von Dokumenten genutzt werden. Eine detaillierte Aufstellung findet sich in der Stellungnahme von IHE Deutschland [5]. Damit ist Nutzung vorhandener IHE Implementierungen auf Seiten der Hersteller zur Umsetzung einer §291 Akte sowie eine einfache Anbindung einer Leistungserbringerinstitution bei vorhandener IHE Infrastruktur eingeschränkt.

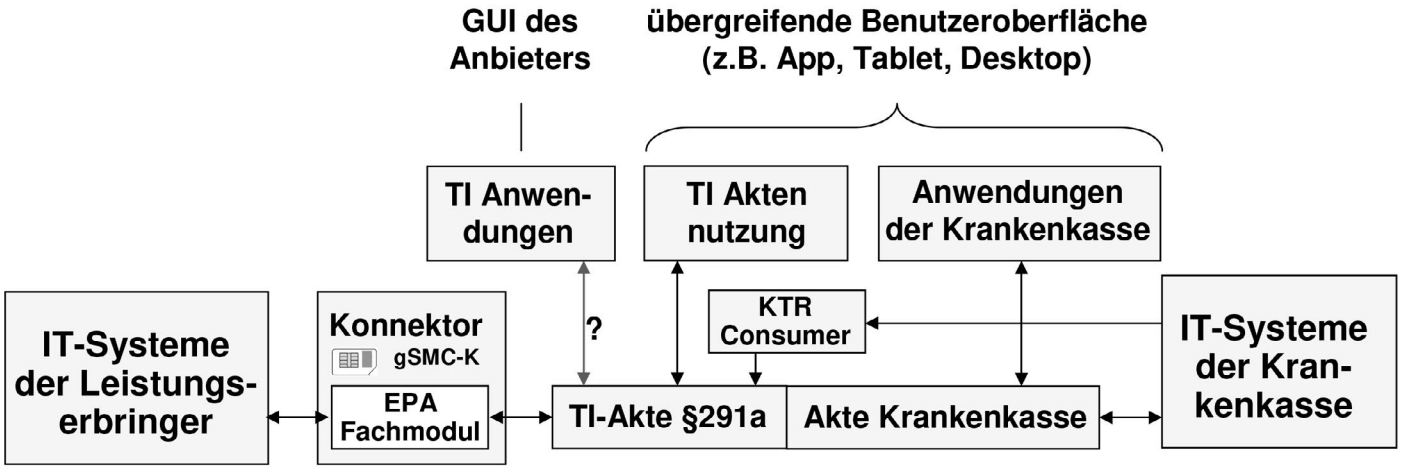


Abbildung: Integration der §291a Akte mit der Aktenlösung einer Krankenkasse

Tabelle: Vergleich der beiden Dienste KV-Connect und KOM-LE

Kriterien	*KV-Connect*	*KOM-LE*
Dienst	KV-Connect Dienst	KOM-LE Fachdienst
Verzeichnisse	KV-Safenet Nutzer KV-Connect Dienst Nutzer	TI Verzeichnisdienst KOM-LE Nutzer
Zugang	KV-SafeNet Router, TI Konnektor	TI Konnektor
Transport	KV-SafeNet, TI Netzwerk	TI Plattform
Autorschaft	via HBA (je nach Dienst)	SMC-B, Nutzer
Schnittstelle	SMTP/POP3, REST API	SMTP/POP3
Verfügbarkeit	gegeben siehe [7]	noch nicht
TI Bestätigung	Antrag aAdG eingereicht [9]	gegeben

Die Spezifikation erlaubt Nutzern, sich gegenüber der §291a Akte auszuweisen, dabei wird jedoch auf die gesamte Akte berechtigt. Dieses Vorgehen wurde vom Bundesjustizministerium richtigerweise moniert [6], so dass Vorgaben zur §291a Akte im Referentenentwurf zum DVG wieder gestrichen werden mussten und die Spezifikation entsprechend zu überarbeiten ist. Datenobjekte können in der §291a Akte gesucht, eingestellt und heruntergeladen werden. Die Beschränkung der Datenobjektgröße auf 25 MB ist für übliche Dokumente ausreichend. Bilddaten sind jedoch nicht nur wegen dieser Beschränkung nahezu ausgeschlossen, sondern auch dadurch, dass DICOM als Datenformat nicht zugelassen ist. Ebenso werden in der Spezifikation bilddatenbezogene IHE Profile (wie XDS-I, XCA-I), die eine Referenzierung auf Bilddatenobjekte ermöglichen würden, bisher nicht verwendet. Die Einbindung der Akte in die Primärsysteme erfordert eine tiefe Integration, da nicht nur der Aufrufkontext (Mandant, Patient, …) bereitgestellt werden muss, sondern auch ein Mithalten des Akten-/Dokumentstatus im Primärsystem notwendig ist. Hintergrund ist, dass die §219a Akte keine Benachrichtigungsfunktion z. B. beim Eintreffen von Befunden vorsieht und der aktualisierte Status nur über eine Nachfrage („polling") möglich ist. IHE sieht hierfür das IHE Profil DSUB (Document Metadata Subscription) vor, dass aber in der Spezifikation der §291a Akte nicht verwendet ist. Es bleibt zu hoffen, dass die Fortschreibung der Spezifikation die obigen Punkte berücksichtigt.

In Bezug auf die Aktenstruktur der §291a Akte setzt die gematik auf die von IHE Deutschland publizierten „value sets" für IHE XDS Metadaten [7] und hat diese um wenige Codes ergänzt. Konkrete Zuordnungen liegen für spezifische Dokumente (Arztbrief, Medikationsplan und Notfalldaten) bereits vor, die weitere Strukturierung ist mit dem TSVG der KBV übertragen worden. Unabhängig wie diese gestaltet wird, muss bei der Nutzung der §291a Akte als Austausch- und Speicherplattform zwischen Institutionen eine Abbildung der beim Sender und Empfänger vorliegenden Datenobjekt- / Dokumentarten bzw. Registerstruktur auf die Vorgaben der §291a Akte erfolgen. Die Erfahrung aus IHE Plattform Projekten zeigt, dass eine 1:1 Abbildung für die Vielzahl klinischer Objekte nahezu ausgeschlossen ist, andererseits diese Abbildung aber mit Sorgfalt durch die Einrichtungen in dem jeweiligen Primärsystem erfolgen muss, damit die zukünftige Suche nach Informationen erfolgreich verlaufen kann.

Aus Sicht der Krankenkassen, die zum Jahresende eine §291a konforme Akte anbieten müssen, stellt sich die Frage nach der Integration mit ihren eigenen Aktenentwicklungen (wie AOK Nordost bzw. AOK DiGeN, TK mit TK-Safe, Vivy Akte als Lösungsansatz für Krankenkassen, Barmer mit eCare). Es zeichnet sich ein Parallelbetrieb der §291a Akte und der jeweiligen Akte der Krankenkasse ab, da diese ihre eigene Lösung für ihre spezifischen Interessen (wie Versicherten Interaktion, Coaching, u.v.a.m.) nicht aufgeben werden. Die Abbildung stellt die absehbare Integration dar.

Auf der Ebene des Benutzers sind beide Akten bzw. deren Anwendungen transparent verfügbar. Die Krankenkasse kann über den so genannten KT Consumer (Abrechnungs-)Daten in die links dargestellte §291a Akte einstellen. Ein lesender Zugriff der Krankenkasse auf die §291a Akte ist technisch ausgeschlossen.

Problematisch sind derzeit noch die geplanten TI-Anwendungen (NFDM (Notfalldatenmanagement), eMP / AMTS (elektronischer Medikationsplan), eRezept), deren Entwicklungsverantwortung auf mehrere Organisationen aufgeteilt war, so dass die aktuellen Spezifikationen die Speicherung auf der eGK aber keine Integration mit der §291a Akte vorsehen. Eine mögliche Abhilfe wäre beim Erstellen eines Notfalldatensatzes, eines eMP oder eines eRezepts diese Informationen in einem weiteren Prozessschritt innerhalb des Primärsystems in die §291a Akte zu übertragen. Sinnvoller wäre jedoch die unmittelbare Weitergabe an die §291a Akte über die zugehörigen Fachmodule im Konnektor.

Neben der §291a Akte plant die TI seit langem die sichere Kommunikation zwischen Leistungserbringern, konkret mit KOM-LE (Kommunikation Leistungserbringer). Der Dienst KV-Connect der KV Telematik GmbH bietet bereits heute eine vergleichbare Funktionalität und ist bereits in viele Arztpraxissysteme integriert und zugelassen[8]. Der Vergleich in der folgenden Tabelle auf S.37 zeigt weitgehende konzeptionelle Übereinstimmungen.

Dazu haben sowohl Dr. Lyck-Dieken (Geschäftsführer der gematik GmbH) als auch Dr. Fuhrmann (Geschäftsführer der KV Telematik GmbH) auf einer Tagung im September 2019 ihre Absicht bestätigt, die Dienste zusammenzuführen, um möglichst schnell eine verlässliche und sichere Kommunikation für Leistungserbringer bereitzustellen. Dies zeigen auch die Beantragung einer Bestätigung als aAdG (andere Anwendung des Gesundheitswesens) für KV-Connect durch die KV Telematik [9] und die Ermächtigung der KBV als Anbieter eines „sicheren Verfahrens zur Übermittlung medizinischer Dokumente“ im §291b Absatz 1e [2].

Zusammenfassend befindet sich die TI in einem Wandel von der Bereitstellung der administrativen Anwendung VSDM (Versichertenstammdatenmanagement) zu medizinisch relevanten Anwendungen wie KOM-LE, §291a Akte, NFDM, eMP und eRezept. Der Weg dahin ist klar vorgezeichnet und bietet Deutschland die Chance im internationalen Vergleich die letzten Plätze im Ranking zu verlassen. Auch wenn die Umsetzung und Integration dieser Anwendungen den IT-Verantwortlichen und Herstellern noch einiges abverlangen wird, spricht alles für eine zeitnahe Umsetzung, um endlich eine sektorbezogene und -übergreifende Kommunikation zwischen Leistungserbringern bereitzustellen und eine aktive Teilhabe des Versicherten bzw. Patienten durch eine Akte und ihre Funktionen zu gewährleisten.

Prof. Dr. Martin Staemmler, Hochschule Stralsund, Fakultät ETI, wissenschaftlicher Beirat des KH-IT

Quellen:

[1] https://www.gematik.de/aktuelles/roadmap/ letzter Zugriff 17.10.2019

[2] http://dip21.bundestag.de/dip21/btd/19/148/1914867.pdf, letzter Zugriff 16.11.2019

[3] Rundschreiben 452/2019 der Hessischen Krankenhausgesellschaft e.V., 20.9.2019

[4] BGBL I 2019 S 646, verfügbar unter http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl119s0646.pdf letzter Zugriff 22.10.2019

[5] http://www.ihe-d.de/wp-content/uploads/2019/03/IHE-D-O%CC%88ffentliche-Stellungnahme-zur-IHE-Nutzung-in-den-Gematik-Spezifikationen-07-03-2019.pdf, letzter Zugriff 22.10.2019

[6] https://www.aerzteblatt.de/nachrichten/103226/Elektronische-Patientenakte-soll-zunaechst-mit-eingeschraenkten-Patientenrechten-kommen, letzter Zugriff 22.10.2019

[7] IHE Deutschland, Value Sets für IHE Metdaten, http://www.ihe-d.de/download/value-sets-fuer-xds-metadaten/, letzter Zugriff 28.10.2019

[8] https://www.kv-telematik.de/fileadmin/DOWNLOADS/Partner-Softwarehaeuser/%C3%9Cbersicht_Audit.pdf, https://www.kv-telematik.de/fileadmin/DOWNLOADS/Partner-Softwarehaeuser/%C3%9Cbersicht_Audit.pdf

[9] https://e-health-com.de/details-news/kv-connect-einreichung-fuer-aadg-bestaetigungsverfahren, https://e-health-com.de/details-news/kv-connect-einreichung-fuer-aadg-bestaetigungsverfahren

Was tun, wenn die IT-Security versagt?

Es ist das Horror-Szenario, das jeder IT - Leitung einen Schauer über den Rücken jagt. Nach einer Erpresser-Email tauchen erste Störungen im Netzwerk der Klinik auf, nach und nach sind weitere IT-Systeme befallen. Der Blackout steht bevor.

Wie verhält man sich nun in so einem Fall? Kann man sich darauf überhaupt vorbereiten? Um diesen Fragestellungen nachzugehen, haben sich 25 Teilnehmer des Seminars „Cyberwar-Game für Kliniken" am 7. November in Wiesloch in der „Akademie im Park" eingefunden. Das LKA Baden-Württemberg, der KH-IT und das Psychiatrische Zentrum Nordbaden haben es sich an diesem Tag zur Aufgabe gemacht, den Ernstfall zu proben.

Zu Beginn des Tages rüttelt Herr Ortmann (ein Gastredner) die Teilnehmer mit einem Impulsvortrag zum Thema Social Engineering auf. Er erläutert, wie sich die Bedrohungslage in diesem Bereich zugespitzt hat. Die Täter fokussieren sich auf die Grundbedürfnisse wie Liebe, Macht, Wertschätzung sowie Spaß und nutzen dies mit gezielten Attacken aus. Social Engineers sind spezialisierte Hacker, die sich nicht auf technische Systeme fokussieren, sondern auf anderer Ebene angreifen. Die Erfolgsquote dieser neuen Taktik ist um ein Vielfaches höher.

Nun führt Herr Reinhard vom LKA-ZAC (Zentrale Ansprechstelle Cybercrime) in die Thematik ein. Er teilt die Akteure in 4 Gruppen ein, alle bekommen das gleiche Szenario. Eine Erpressermail wird in der Info@ Adresse der Klinik gefunden. Mal ehrlich, wie häufig prüft diese Inbox schon jemand? Die Teams erarbeiten in Räumen das Szenario auf, das Spiel findet in Echtzeit statt. Im Laufe des Tages überschlagen sich die Ereignisse, die Zeitabstände für Reaktionen werden immer kürzer. Immer, wenn man denkt, „aber jetzt haben wir es geschafft", geschieht ein weiterer Vorfall. Nach jeder Phase treffen sich die Gruppen im Plenum, um ihre Arbeitsergebnisse zu vergleichen.

Das LKA gibt immer wieder Tipps zu Vorgehensweise und erläutert klare Fehler von Entscheidern in diesen Phasen. Wir hören nicht „das machen sie falsch", es geht viel mehr um „haben sie daran schon gedacht?". Viele Kliniken fürchten um ihre Reputation und melden Vorfälle gar nicht oder viel zu spät. Oft hat man auch Angst davor, dass jemand denken könnte, man hat nicht genug für die IT-Sicherheit getan. „Technische Schutzmaßnahmen sind essenziell, um ihre Klinik zu schützen. Doch bedenken Sie, kein System bietet hundertprozentigen Schutz, Sie sind angewiesen auf die Achtsamkeit Ihrer Mitarbeitenden!" klärt uns Herr Reinhard auf. Nicht nur im Ernstfall ist das jeweilige LKA der Bundesländer ein guter Ansprechpartner. Alleine schon bei der Klärung, ob nur ein Spam-Mail oder tatsächlich eine ernstzunehmende Bedrohung vorliegt, kann die Polizei hier hilfreich zur Seite stehen. Was nimmt man also mit, nach einem langen Tag, bei dem es rund um das Thema Krisenmanagement und Umgang mit Cybercrime geht, frage ich die Teilnehmer bevor sie sich auf die Heimreise machen. „Ich werde mehr auf die Hilfe des ZAC setzen, schon bei der Analyse ob eine Bedrohung vorliegt," antwortet mir ein direkter Kollege. „Der Spagat zwischen noch mehr Schaden verhindern und irgendwie den Klinikbetrieb aufrecht erhalten, fand ich interessant," antwortet ein Anderer. Der letzte Seminarteilnehmer, der den Raum verlässt, bringt es auf den Punkt. „Vor

dem Seminar war das ein Angstszenario für mich. Ich wusste nicht, wie ich mich verhalten sollte. Jetzt fühle ich mich sicherer und denke, dass ich im Ernstfall damit umgehen kann".

Inhaltlich möchte und darf ich Ihnen nicht so viel von unserem interessanten Tag erzählen. Vielleicht gibt es ja den einen oder anderen, die sich auch noch mit diesem Szenario beschäftigen möchte. Diesen Kollegen*innen möchte ich den Erfahrungswert und den kollegialen Austausch nicht vorweg nehmen. Zum Schluss möchte ich Ihnen noch meinen persönlichen Apell mitgeben: Trauen sie sich, sich außerhalb ihrer Komfortzone zu bewegen und vor allem auch mit unangenehmen Themen zu beschäftigen. Es lohnt sich wirklich!

Autorin: Alexandra Heimel, Leiterin IT-Abteilung, Psychiatrisches Zentrum Nordbaden, Wiesloch

Health-IT-Talk Bayern

Process Mining im Gesundheitswesen

Am 17.9.2019 konnten die Koordinatoren des Health-IT-Talks Bayern, Herr Michael Musick (BVMI) und Dr. Manfred Härdtner, wieder zahlreiche Interessenten aus Krankenhäusern und innovativen Unternehmen des Health Care Bereichs begrüßen.

Das Thema „Process Mining im Gesundheitswesen" hatte bei vielen die Neugierde geweckt. Die Veranstaltung fand in den Räumlichkeiten des Zentrums Digitalisierung.Bayern (ZD.B, https://zentrum-digitalisierung.bayern.de) auf dem Forschungscampus der TU-München in Garching bei München statt. Frau Maria Marlene Bohrer-Steck hieß die Anwesenden herzlich willkommen und stellte das ZD.B mit seinen Aufgabenschwerpunkten den Zuhörern vor. Das ZD.B versteht sich als Marktplatz rund um innovative Ideen zur Förderung der Digitalisierung. Es ist ein Kooperations-, Forschungs-, und Gründungsnetzwerk. Das ZD.B hat zum Ziel, die Forschungs- und Realisierungskompetenz Bayerns im Bereich der Digitalisierung weiter zu stärken und das Tempo digitaler Entwicklungen zu erhöhen.

Im Vorfeld standen folgende Fragen im Raum:

- Wie kann Process Mining im Gesundheitswesen eingesetzt werden?
- Wie können auf der Basis von Daten die (Geschäfts-) Prozesse rekonstruiert und visuell dargestellt werden?
- Können dadurch wirklich Prozessineffizienzen erkannt werden?
- Und wie können diese dann behoben werden?
- Welche Rolle spielt dabei KI?

Auf diese Fragen gaben Herr Alexander Endres, Strategic Growth Account Executive, Celonis SE, und Herr Nils F. Wittig, Geschäftsleitung CXO, K|M|S in ihren Vorträgen einen Einblick. Herr Alexander Endres von der Firma Celonis fasste es wie folgt zusammen: „Wir machen die Welt effizienter. Celonis hat ein ganz einfaches Ziel: die Prozesse von heute zu analysieren, damit die Welt von morgen effizienter ist. Als führender Process Mining Anbieter nutzen wir die vorhandenen digitalen Event Logs in bestehenden IT-Systemen, um datenbasiert die gesamten Geschäftsprozesse zu rekonstruieren und visuell darzustellen. Dies ermöglicht Unternehmen aller Branchen Patienten-, Produkt-, Steuerungs- und Supportprozesse zu visualisieren und Transparenz darüber zu erhalten, wie diese Prozesse wirklich laufen. Neueste KI-Technologie und intelligente Algorithmen unterstützen die Mitarbeiter bei der Auswertung von Analysen, decken selbstständig Schwachstellen auf und ermöglichen eine vollautomatisierte Root-Cause-Analyse, um Prozessineffizienzen, wie Nacharbeiten, manuelle Tätigkeiten und ineffiziente Genehmigungsstufen zu erkennen sowie zu beheben." Am Beispiel einer IT-Serviceeinheit demonstrierte Herr Endres anschaulich die Funktionen, Arbeitsweise und die Möglichkeiten der Datenanalyse. Besonders hilfreich ist dabei die grafische Darstellung der Prozesse und die Visualisierung der Abläufe.

Die Produkte der Firma Celonis bilden heute einen Baustein für die Arbeiten der Firma K|M|S mit Sitz in Unterhaching. Sie ist seit über zwei Jahrzehnten ein bedeutender Schrittmacher neuer Technologien für das Wissensmanagement in der deutschen Gesundheitswirtschaft. Als Partner unterstütz K|M|S Krankenhäuser in ihren Arbeits- und Entscheidungsprozessen und hilft Transparenz und Entscheidungssicherheit herbeizuführen. Am Beispiel der Datenanalyse für eine typische Krankenhausbehandlung zeigte Herr Wittig plastisch auf, wie viele Varianten der Verlauf bei den Patienten in einem Zeitraum tatsächlich annimmt. Durch Zoomen in verschiedenen Freiheitsgraden wie Zeitspanne der Betrachtung, Altersspektrum oder Geschlecht der Patienten sowie die Tiefe der Betrachtungsebene lassen sich, grafisch sehr anschaulich, die realen Prozesse erkennen, analysieren und mit den Nutzern gemeinsam bewerten.

Ein zentraler Punkt, um den es sich in der anschließenden Diskussion drehte, war die Frage nach der Qualität und Aussagekraft des zugrundliegenden Datenmaterials. Da es sich ja um Daten handelt, die nicht speziell für eine bestimmte Analyse erfasst und kontrolliert werden, sondern quasi Abfallprodukte aus dem tatsächlich ablaufenden Prozessgeschehen sind, ließ sich die Frage nicht eindeutig beantworten. Einerseits ist sie als hoch zu bewerten, da die Daten den tatsächlichen, in den Systemen vorhandenen Ereignissen entsprechen. Andererseits ist zu vermuten, dass sie nicht immer präzise sind, was den Zeitpunkt betrifft. Der Erfassungszeitpunkt im System kann durchaus gegenüber Zeitpunkt der Ausführung einer Tätigkeit differieren. Es werden eben manchmal Sachverhalte erst später nachgetragen. Letztendlich war man sich darüber einig, dass es sich bei der Analyse ja nicht um einen einmaligen Vorgang handeln sollte, sondern um eine regelmäßige Beobachtung und daraus abgeleitete Beeinflussung des Prozessgeschehens. Wichtig ist es, eklatante Fehler zu erkennen. Die gezeigten Werkzeuge und Methoden geben hierzu ein gutes Handwerkszeug in die Hand.

Letzteres warf die Frage auf, wer in den Unternehmen in der Lage ist den Daten und den daraus abgebildeten Abläufen die richtigen Schlussfolgerungen zu ziehen? Bei der Breite der möglichen Einsatzfelder der Werkzeuge ließ sich, außer im betriebswirtschaftlichen Bereich die Controller, keine spezielle Berufsgruppe identifizieren. Konsens bestand darin, dass die Berufsbilder um das Thema Datenanalyse ausgeweitet werden müssen.

Im Anschluss tauschten sich die Anwesenden bei einem kleinen Imbiss untereinander und mit den Vortragenden sowie den Veranstaltern aus. Insgesamt war es für alle eine gelungene Veranstaltung.

Autor: Dr. Manfred Härdtner, Stellv. IT-Leiter, Klinikum rechts der Isar

Verbandstermine 2020

18.03.2020 – 19.03.2020
Frühjahrstagung im Deutschen Krebsforschungszentrum Heidelberg: Vernetzung und Integration

Health-IT-Talk in Berlin-Brandenburg
13.01.2020 Pflege, AAL, IT nah am Patienten und Robotik
10.02.2020 Thema noch offen

Health IT-Talk Nordbayern in Nürnberg
18.2.2020 Plattformstrategie für den Umbau des KIS auf Basis von IHE der Klinikum rechts der Isar TU München

Health-IT in Baden-Württemberg
(nach Ankündigung Region Stuttgart)
Regionalveranstaltungen in Bayern
(nach Ankündigung, München)
Regionalveranstaltungen in Sachsen/Sachsen-Anhalt
(in Planung)
Weitere Regionalveranstaltungen in Vorbereitung

Alle bekannten Termine und Inhalte auf der Website des KH-IT (www.kh-it.de), des Health-IT-Talk Berlin-Brandenburg (www.health-it-talk.de) und in der XING-Gruppe.
Einladungen zu den Regionalveranstaltungen erfolgen über die teilnehmenden Verbände und Mailinglisten.
Die Kooperationen sind regional unterschiedlich ausgeprägt.

Bundesverband der Krankenhaus-IT-Leiterinnen/Leiter e.V.
Jürgen Flemming
Vorstandsmitglied/Pressereferent
www.kh-it.de – flemming@kh-it.de

Die Inhalte der Verbandsseiten werden redaktionell erstellt und betreut vom BV KH-IT. Der Bundesverband der Krankenhaus-IT-Leiterinnen/Leiter e.V. kurz KH-IT ist der führende Berufsverband der Krankenhaus-IT-Führungskräfte. Der KH-IT steht allen leitenden und/oder verantwortlichen Mitarbeitern der Krankenhaus-IT offen.

Medizinstrategie in Theorie und Praxis

Marktorientierte Gestaltung des Krankenhausleistungsprogramms

Die Publikation „Marktorientierte Gestaltung des Krankenhausleistungsprogramms“ von *Nico Kasper* gibt eine umfassende theoretische und empirische Analyse des Leistungsmanagements in deutschen Krankenhäusern. Sie zeigt die Entwicklung einer schlüssigen Struktur des Krankenhausleistungsprogramms. Interviews mit führenden deutschen Krankenhausmanagern vervollständigen die fachliche Darstellung. Zielgruppen sind Wissenschaftler mit den Schwerpunkten Gesundheitsökonomie, -management sowie der Medizin und des Pflegemanagement.

Die aus dieser gesellschaftlichen Bedeutung resultierenden steuernden Eingriffe des Gesetzgebers und die Komplexität des Produkts „Gesundheitsdienstleistung" an sich machen das Management des Angebotsprogramms eines Krankenhauses zu einer der größten Herausforderungen in der Betriebswirtschaftslehre. Daher müssen die Krankenhausbetriebswirte und die Krankenhausbetriebslehre das Management des Krankenhausleistungsprogramms als eines ihrer wichtigsten Aktionsfelder annehmen und zielgerichtet ausgestalten. Die Publikation „Marktorientierte Gestaltung des Krankenhausleistungsprogramms“ tritt mit dem Anspruch an, das Entscheidungsfeld in seiner Gesamtheit zu erschließen. Sie legt erstmals eine vorläufige Theorie zur marktorientierten Gestaltung des Krankenhausleistungsprogramms vor. Damit schließt sie eine mehr als vierzig Jahre vorhandene Lücke in der Krankenhausbetriebslehre. Zudem zeigt sie den Praktikern, dass eine systematische Leistungsprogrammbereinigung zu wahrnehmbaren Kostensenkungen führen kann.

Nico Kasper
Marktorientierte Gestaltung desKrankenhausleistungsprogramms
Medizinstrategie in Theorie und Praxis
430 Seiten, 27 Abb. 48 Tabellen

eBook (PDF)
ISBN 978-3-11-065329-8
*€ [D] 99.95**
UVP
US$ 114.99 / GBP 91.00
eBook (EPUB)
ISBN 978-3-11-064930-7
*€ [D] 99.95**
UVP
US$ 114.99 / GBP 91.00
Gebunden
ISBN 978-3-11-064910-9
*€ [D] 99.95**
UVP
US$ 114.99 / GBP 91.00

Ein Algorithmus hat kein Taktgefühl

Wo künstliche Intelligenz sich irrt, warum uns das betrifft und was wir dagegen tun können

In ihrem Buch „Ein Algorithmus hat kein Taktgefühl" erklärt Prof. Dr. Katharina Zweig, was hinter den Begriffen aus der digitalen Welt steckt und wo künstliche Intelligenz lieber nicht zum Einsatz kommen sollte.

Die Themen Künstliche Intelligenz, Big Data und Algorithmen sind zurzeit in aller Munde. Die Informatikprofessorin aus Kaiserslautern hat sich mit den folgenden Fragen auseinandergesetzt: Muss man sich nun Sorgen machen, weil sie immer größere Teile unseres Lebens besetzen? Und wie sollte die Politik damit umgehen? Und versteht man wirklich immer alles richtig?

Für ihre Schilderungen nutzt die vielfach als Deutschlands bekannteste Algorithmus-Erklärerin bezeichnete Expertin praxisorientierte Beispiele aus dem Alltag, Politik und Wirtschaft. Damit trifft sie den Nerv der Zeit und positioniert sich mit ihrer Expertise in den aktuellen Diskussionen, wofür sie auch bereits mehrfach ausgezeichnet wurde.

Katharina Zweig
Ein Algorithmus hat kein Taktgefühl: Wo künstliche Intelligenz sich irrt, warum uns das betrifft und was wir dagegen tun können
Broschiert: 320 Seiten
Verlag: Heyne Verlag, Oktober 2019
Sprache: Deutsch
ISBN-10: 3453207300
ISBN-13: 978-3453207301

Neues Buchprojekt

Die Zukunft der Health-IT

Welche Anbieter überleben? – Wer sind die neuen Player?

Die Zukunft der Health-IT - wie wird sie aussehen? Experten sagen uns eine Revolution voraus! Künstliche Intelligenz (KI), permanentes Monitoring durch Wearables und Smartphones, Diagnostik durch massenhafte Datensammlung und Auswertung (Big Data) das sind nur einige Trends. Der Patient wird zum "Gesundheitskunden", Prävention statt "Reparaturbetrieb" und auf den Kunden abgestimmte personalisierte Medizin.

Wie diese Ziele umgesetzt werden können, hängt entscheidend von der Industrie ab, die entsprechende Produkte und Verfahren zur Verfügung stellen wird. Einen Überblick über die heutige Situation und die starke Spezialisierung einzelner Softwarelösungen bietet beispielsweise das Ausstellerverzeichnis auf einschlägigen IT-Messen (DMEA, Tagungen des Bundesverbandes KH-IT, Entscheiderfabrik oder andere Veranstaltungen). Man muss kein Hellseher sein, um zu ahnen, dass das Warenverzeichnis der Zukunft vermutlich anders aussehen wird.

Anbieter kommen zu Wort

Für die heutigen Anbieter besteht die Aufgabe darin, ihr Leistungsportfolio zu modifizieren oder neu zu entwickeln und den zukünftigen Anforderungen anzupassen, um auf dem Zukunftsmarkt bestehen zu können. Hierzu gehören Weitsicht, Visionen und "die richtige Nase". Einen langfristig wirtschaftlichen Erfolg werden nur die Unternehmen haben, die sich über diese Themen bereits heute Gedanken machen und die Weichen stellen.

Welchen Visionen haben Startups und IT-Sicherheitsanbieter?

Das Health-IT-Angebot der Zukunft wird durch die "überlebenden" Anbieter und einer Reihe neuer Player bestimmt

werden. Viele davon sind möglicherweise heutige Startups. Auch die Rolle der IT-Sicherheitsanbieter wird immer stärker an Bedeutung gewinnen. Sie werden das Fundament für eine funktionierende und störungsfreie IT bieten müssen. Erfolgreich werden nur die Anbieter sein, die die Besonderheiten des Health-IT Marktes berücksichtigen.

"Die Zukunft der Health-IT" wagt den Ausblick

"Die Zukunft der Health-IT" lässt Health-IT-Anbieter zu Wort kommen und ihre Vorstellungen und Visionen für zukünftige Entwicklungen und gegebenenfalls Neuausrichtungen erläutern. Eine Recherche im Vorfeld ergab, dass es eine starke Verunsicherung auf Kundenseite (Gesundheitseinrichtungen) hinsichtlich der Investitionssicherheit gibt. Schließlich hängt mit dem Einsatz der Systeme auch die Organisation und Gestaltung der Arbeitsabläufe der Zukunft ab.

Erscheinung

"Die Zukunft der Health-IT" erscheint im Frühjahr 2020 (geplant zur DMEA) im Antares Computer Verlag.

Für Rückfragen:

Hartmuth Wehrs
antares@medizin-edv.de
Kim Wehrs
k.wehrs@medizin-edv.de

Es war in der formlosen Atmosphäre viel Neues rund um Medizin, Gesundheit und Life Science zu entdecken bzw. zu bewundern – bespickt mit zahlreichen Showcases.

Bildquelle: XPOMET

Rückblick auf Jahreskonferenz XPOMET Medicinale

Menschen die Angst vor neuen Technologien nehmen – mit neuen Formaten

In seinem zweiten Ausführungsjahr öffnete die XPOMET Medicinale ihre Pforten vom 10. bis 12. Oktober 2019 in der Arena Berlin der Landeshauptstadt. Auf der großzügig angelegten Ausstellungsfläche von 6500 m² fanden 125 innovative Aussteller und 140 inspirierende Referenten Platz für ihre 2900 Besucher. Eindrücke von diesem außergewöhnlichen internationalen Event schildert *Dr. Aykut M. Uslu*, Berater für Projektierung in der Medizintechnik und Medizin-IT.

Was verbirgt sich eigentlich hinter XPOMET?

Mit XPOMET Medicinale hält ein neuer und neuartiger Medizinkongress in der Szene Einzug. Den Veranstaltern zufolge ist XPOMET eine globale Plattform für Innovationen in der Medizin und Pflege, das XPOMET Festival eine Hommage an Technologie und Fortschritt. Mutige Unternehmer, Forscher und Entrepreneure finden dort ihren Platz, ebenso wie kritische Querdenker und Visionäre.

Wenn es darum geht, die Zeichen der Zeit zu erkennen, haben die Erschaffer der XPOMET ins Schwarze getroffen. Bekanntlich rollen gewaltige Innovationslawinen mit hoher Geschwindigkeit auf uns zu. Die nächste Evolutionsstufe in der Medizin möglichst schadlos zu überstehen, erfordert dringend auch Plattformen wie diese.

Hochkarätige Wissenschaftler setzten neue Akzente

Nach dem Motto „Voneinander lernen" diskutierten zahlreiche hochkarätige Wissenschaftler aus Europa, USA, Indien, China und weiteren Regionen auf vier Bühnen bei Vorträgen miteinander und auch mit dem Publikum. Die bemerkenswertesten Beiträge waren:

- Medizin fürs All und ihr technologisch-methodischer Beitrag für die Versorgung für uns auf der Erde, von Prof. Dr. Pascale Ehrenfreund, Vorstandsvorsitzende des Deutschen Zentrums für Luft- und Raumfahrt (DLR).
- Smart Hospitals (Prof. Dr. Jochen Werner) und virtueller OP (Chirurgie-Koryphäen Prof. Dr. Shafi Ahmed und Dr. Rafael Grossmann)
- Verändern neue Geschäftsmodelle und neue Prozesse für die Leistungserbringung die Datenübermittlungs-Technologie 5G, Open Source, Big Data, Blockchain und Quantencomputing unsere Gesundheitsversorgung von Grund auf?
- Den Entwicklungsweg vom Teleskop zum Mikroskop und hin zu Big Data als Basis für Innovation zeigte der Visionär John Nosta auf – mit der Aufforderung, Patienten als Kollaborationspartner statt als Objekt für Leistungen zu sehen.

Weitere erklärende und einfordernde Beiträge zu den Rahmenbedingungen aus Politik und Wirtschaft sowie insbesondere zur Präzisionsmedizin, rundeten das wissenschaftliche Angebot ab.

Keynote Talk mit Dr. Auma Obama

Die in Kenia geborene Halbschwester des 44. US-Präsidenten, Barack Obama, hat in Deutschland (Heidelberg / Bayreuth) studiert und promoviert. Sie ist inzwischen weltweit als starke Stimme Afrikas unterwegs. Ob bei ihrem Appell an die Zuhörer, die Entwicklungshilfe einzustellen und den Afrikanern auf Augenhöhe zu begegnen oder bei der bildhaften Schilderung mancher ihrer Projekte, zeigte sie sich weltmännisch. Kein Wunder, denn Dr. Obama ist Mitglied im Weltzukunftsrat

Die in Kenia geborene Halbschwester des 44. US-Präsidenten Barak Obama, Auma: „Schluss mit „Entwicklungshilfe" – den Afrikanern auf Augenhöhe begegnen. *Bildquelle: XPOMET*

(World Future Council), Mitglied des Organisationsrats der Kilimandscharo-Initiative, die junge Menschen unterstützt, gewaltfrei zu leben und sich in ihren Gemeinden zu engagieren. Darüber hinaus ist sie die Gründerin und Vorsitzende der Sauti Kuu Stiftung, die Kindern in aller Welt Perspektiven geben will und ihnen hilft, ihre Potentiale zu erkennen und zu stärken.

Healthcare Hackathon

Ein weiteres Highlight der XPOMET bildete der #healthhackathon19 – ein Hackathon parallel zur gesamten Veranstaltung, bei dem internationale Startups im Wettstreit um die beste innovative Lösung gegeneinander antreten. Neun interdisziplinäre Teams mit 60 Teilnehmern erarbeiteten dabei digitale Lösungskonzepte in den Bereichen Medical Technology, Hospital Management & Care sowie Health Insurance. Mit dem Engagement von ETH Zürich, PwC, IBM, Bayer, InsurTech Hub München und weiteren Organisationen, ging es hier unter anderem darum, Diabetes-bedingte Augenödeme mit dem Smartphone zu identifizieren oder mittels Bewegungsanalyse die Einhaltung von Incentivierungsprogrammen von Krankenkassen zu überprüfen. Dank der Unterstützung von Google Cloud, Aicura Medical, Bayer IT und The Impact Farm konnten die Teilnehmer auf eine gut geeignete Infrastruktur zurückgreifen.

Gewinner waren die Teams „Hack4Life" (mobile screen retinopathy) aus der Schweiz, Alfaleus (age-related macular degeneration identification) aus Indien und Uncommon (digital personal trainer) aus Berlin.

Special Guest Viktoria Modesta, Singer-Songwriter und wohl bekanntestes Prothesen-Model der Welt im Interview mit Nina de Lianin. *Bildquelle: XPOMET*

Glamouröses Prothesen-Model: Viktoria Modesta

Viktoria Modesta, Singer-Songwriterin und wohl bekanntestes Prothesen-Model der Welt, trat auf der XPOMET als Special Guest auf. Im Interview mit Nina de Lianin berichtete die selbstbewusste Lettin unter anderen von ihrem Werdegang und davon, wie es ist, mit einem sichtbaren Implantat durch das Leben zu gehen. „Ich war damals in einer Situation, in der meine kreative Seite und meine körperlichen Fähigkeiten nicht übereinstimmten. Das wollte ich ändern. Als ich mich zur Amputation entschied, hatte ich den Wunsch, die Kontrolle über meinen Körper zurück zu erlangen". Nach der Beinamputation wurde die junge Frau mit Tanzvideos im Internet berühmt. Sie trat sogar auch mal im berühmten Pariser Kabarett Crazy Horse auf. Zeitungen titelten damals perplex mit „Erotik mit Prothese: Einbeinige tanzt im Crazy Horse". Bezaubert hat sie auch die Zuschauer bei der Abschlusszeremonie der Paralympics 2012, als sie als Schneekönigin auftrat - mit einer diamantbesetzten Prothese.

Save The Date

Die nächste XPOMET findet vom 15.–17. Oktober 2020 in der Arena Berlin statt.

Interview mit Prof. Goyen, Röntgendiagnostiker und Chief Medical Officer Europe bei GE Healthcare

Prof. Dr. med. Mathias Goyen ist Röntgendiagnostiker und derzeit verantwortlich als Chief Medical Officer Europe bei GE Healthcare für die Leitung der medizinischen, klinischen und Evidenzstrategien.

Die Entwicklung der künstlichen Intelligenz (KI) in der Radiologie hat in letzter Zeit einen enormen Hype ausgelöst. Müssen die Radiologen und das radiologische Personal die KI fürchten?

Prof. Mathias Goyen: Es gibt einige Stimmen, die insbesondere für die Radiologie zukünftige Szenarien voraussagen, dass KI den menschlichen Radiologen ersetzt. KI kann uns helfen, mehr zu sehen und genauer und schneller zu diagnostizieren aber KI per se wird den Radiologen nicht ersetzen. Ich sage aber genauso, dass Radiologen, die die Kraft der KI nutzen, diejenigen ersetzen, die dies nicht tun. Radiologen sitzen in Tumorboards, therapieren Krankheiten (z. B. durch lokale Ablationstherapien und Interventionelle Radiologie), erarbeiten aus der Bildgebung in Kombination mit der Krankengeschichte des Patienten Befunde und führen Patientengespräche. Das sind alles Aktivitäten, die nicht so einfach automatisiert werden können. Mein Rat an alle wäre: Wir sollten KI weniger oder gar nicht fürchten, sondern KI als Chance erkennen, als Werkzeug, das den Ärzten und MTRAs und allen im Krankenhaus die Arbeit erleichtert.

Bekanntermaßen hat die KI auch in die Medizintechnik Einzug gehalten. An welchen Stellen der diagnostischen Großgeräte wie CT, MRT und Angio findet die KI Einsatz? Wo sehen Sie darüber hinaus noch Möglichkeiten?

Prof. Mathias Goyen: Heute müssen Gesundheitseinrichtungen den Spagat zwischen höchstmöglicher Rentabilität und optimaler Patientenversorgung meistern. Dabei unterstützen wir sie durch den Einsatz von KI in den einzelnen Abteilungen. GE Healthcare verwendet Algorithmen für seine Modalitäten, um die Aufnahmen vor, während und nach der Untersuchung zu optimieren. So sorgt SmartScan beispielsweise für eine automatische Anpassung von Schichten während einer Übersichtsaufnahme im CT. Ein weiteres Beispiel ist eine Pneumothorax-Anwendung, die mit vier klinischen Einrichtungen, darunter die University of California, San Francisco, und das Boston Children's Hospital, entwickelt wurde. Das Tool ermöglicht es Radiologen, einen Vergleich von altersgerechten normalen Aufnahmen zusammen mit Patientenscans zu sehen. Ergänzend dazu weist die KI automatisch auf potenziell bedrohliche Ergebnisse hin. Auf diese Weise ermöglicht die Kombination von KI mit klinischer Expertise Gesundheitseinrichtungen eine effiziente Auswertung der enormen Datenmengen aus dem Klinikalltag. Für uns bei GE Healthdare sind KI-gesteuerte Krankenhäuser mit sogenannten Kommandozentralen der nächste logische Schritt.

Welche Aspekte der XPOMET Medicinale haben Sie beeindruckt, welche nicht? Was wünschen Sie sich zum Abschluss des XPOMET Medicinale Kongresses?

Prof. Mathias Goyen: Die XPOMET Medicinale ist insbesondere durch ihren Start-up-Charakter ein interessantes neues Konzept. Anders als normalerweise üblich ging es hier weniger um Präsentationen, sondern vielmehr um Diskussion und Austausch. Ich habe selber eine Session moderiert und war auf zwei Panels vertreten. Die internationale Faculty war sehr inspirierend – ich habe in Berlin spannende Referenten und Speaker erleben können, die ich bisher nur aus TED-Talks kannte. Natürlich gibt es wie überall Potenzial zur Optimierung, insgesamt hat der Kongress uns aber überzeugt.

Dr. Aykut M. Uslu,
Berater Medizintechnik und Medizin-IT,
www.uslumedizininformatik.de

E-Health im Doppelpack: Veranstaltung „TI für Krankenhäuser“ und Health-IT Talk Berlin in der Bundesdruckerei

Rund 150 Teilnehmer aus dem Klinikumfeld und der Industrie versammelten sich am 11. November 2019 in den Räumen der Bundesdruckerei in Berlin. Vertreten durch die Tochtergesellschaft D-TRUST GmbH zählt das Unternehmen zu den wichtigsten Vertrauensdienstanbietern in Deutschland. Das Produktportfolio im Bereich E-Health umfasst u. a. Institutionsausweise, Heilberufsausweise, Fernsignaturen, Zertifikatsdienste sowie viele andere Lösungen rund um das Thema Identitätensicherung.

Telematikinfrastruktur für Krankenhäuser

Die Herausforderungen, die Chancen und der Nutzen der Telematikinfrastruktur für den stationären Sektor standen im Mittelpunkt der Veranstaltung „TI für Krankenhäuser“, zu der die Bundesdruckerei einlud. Sowohl Teilnehmer als auch Referenten stimmten überein, dass das Nutzenpotenzial für Patienten sowie das Gesundheitssystem enorm sind. Dennoch erwarten die Leistungserbringer diverse Herausforderungen, die bewältigt werden müssen.

Die Vorträge und die vielen Fragen der Zuhörerschaft zeigten: Das Thema erfährt momentan eine hohe Dynamik und großes Interesse.

Eröffnet wurde der Nachmittag vom Gastgeber, Dr. Kim Nguyen, Geschäftsführer D-TRUST GmbH, der die aktuellen Lösungen der D-TRUST vorgestellt, aber auch einen Blick in zukünftige Entwicklungen gewagt hatte. Kern der Aussage: Digitale Identitäten benötigen Sicherheit und Vertrauen, die nur durch einen qualifizieren Vertrauensdiensteanbieter gewährleistet werden können.

Welche technischen Voraussetzungen müssen Krankenhäuser erfüllen? Wie kann ein Institutionsausweis beantragt werden? Wie viele Institutionsausweise sollten bestellt werden und wie werden diese finanziert? René Schubert, Geschäftsführer der DKTIG, hatte viele Antworten auf genau diese Fragen. Dennoch blieben einige Punkt - z. B. hinsichtlich der Konnektor-Thematik - offen.

Im Anschluss folgten zwei Anwenderberichte: Christopher Ludwig, IT-Leiter des Gesundheitsnetzwerks Waldfriede, stellte den Status quo seines Hauses bei der Einführung der Telematikinfrastruktur vor und bot einen Ausblick in die weitere Vorgehensweise. Im Anschluss wurden die Herausforderungen bei der Einführung der TI für die Charité Berlin betrachtet – vertreten durch Silke Eckardt sowie Sören Mews. Erkenntnis: Die Telematikinfrastruktur sollte nicht als ein reines IT-Projekt betrachtet werden, sondern vielmehr als ein interdisziplinär agierendes Programm.

Abgerundet wurde die Vortragsreihe mit dem Vortrag von Dirk Schladweiler von der Bundesärztekammer (BÄK), der über die bevorstehende Verfügbarkeit der elektronischen Heilberufsweise informierte und die Möglichkeiten der digitalen Signatur im Gesundheitswesen.

Zum Abschluss der Veranstaltung „TI für Krankenhäuser“ nahmen die Teilnehmer an Führungen zu den Themen Banknoten- und Personalausweisproduktion sowie das Lösungsportfolio der Bundesdruckerei im Showpavillon teil.

Health-IT Talk

Die zweite Veranstaltung an diesem Tag, der Health-IT Talk, wurde von Dr. Adrian Schuster vom Berufsverband Medizinischer Informatiker e.V. (BVMI) am Abend eröffnet. Nach der Begrüßung wurde das Wort zum zweiten Mal an diesem Tage an Dr. Kim Nguyen, den Geschäftsführer der D-TRUST GmbH, übergeben. Er erläuterte, warum und wie die europäische eIDAS-Richtlinie zur sicheren digitalen und grenzüberschreitenden Kommunikation in Europa verhilft sowie welche Auswirkungen diese Richtlinie für Deutschland hat.

Im anschließenden Bericht aus der Praxis stellte Karolin Jordan, Fachapothekerin für Klinische Pharmazie der Evangelischen Kliniken Essen, die eigene eRezept-Lösung und dessen Abrechnung im Ende-zu-Ende digitalisierten Prozess. Im Mittelpunkt dieses Prozesses steht die digitale Signatur – dabei im Besonderen die Fernsignatur – des Rezepts durch den Arzt und Apotheker sowie die digitale Bereitstellung der Abrechnung mit den Krankenkassen. Im letzten Vortrag des Abends erläuterte Senior Consultant Ralf Dittmar von der D-TRUST GmbH die Bedeutung von Webseiten-, Personen- und Maschinenzertifikaten anhand von Kundenreferenzen.

Ein Get-Together hat diesen gelungenen Abend abgerundet: Die Teilnehmer nutzten die Gelegenheit, angeregt über das Gehörte zu diskutieren und sich untereinander zu vernetzen.

Podiumsdiskussion beim Healthcare Forum

Komplexität beherrschen – Innovationen in der Gesundheitsversorgung ermöglichen

Intersystems DACH Symposium 2019 – Healthcare Forum

Unter dem Motto „Wettbewerbsvorteile sichern – Digitale Innovationen beschleunigen“ fand vom 12.-14. November 2019 im „The Westin Grand Frankfurt“ das InterSystems DACH Symposium 2019 statt (#DACHSymposium2019). Eingeladen waren IT-Dienstleister und Anwenderunternehmen. Mit über 200 Wissenschaftlern, Analysten und Branchenexperten wurde eingehend erörtert, wie digitale Innovationen, datenbasierte Geschäftsmodelle, aber auch Künstliche Intelligenz und Machine Learning in modernen Organisationen in die Realität umgesetzt werden können. Zu den Kernprodukten für das Gesundheitswesen gehören die Datenplattform „IRIS for Health“, für die schnelle, unkomplizierte, interoperable und standardkonforme Entwicklung datengetriebener Lösungen und „HealthShare“, eine interoperable Lösung, die umfassende, longitudinale Patientenakten für Versorger, Patienten und Kostenträger ermöglicht. Des weiteren bietet InterSystems mit „TrakCare“, eine einheitliche Lösung aus medizinischer Patientenakte und –managementsystem.

Healthcare Forum

In seiner Keynote am zweiten Tag des dreitägigen Symposiums gab Don Woodlock, Vice President HealthShare, einen umfassenden Einblick in die komplexen Strukturen des Datenmanagements. Er erläuterte anschaulich, dass es durch das dezentrale Gesundheitssystem und die Selbstverwaltung mit den vielen verschiedenen Akteuren, sehr komplex sei, die Gesamtheit aller Daten zu erfassen. Und diese Datenmenge wachse schließlich täglich beträchtlich. Für ihn liegen die Herausforderungen der digitalen Transformation in drei Bereichen: dezentral vorliegenden Gesundheitsdaten, kognitiver Überfrachtung der Beteiligten aufgrund der schieren Informationsmenge und den tiefgreifenden Umbrüchen, die momentan stattfinden.

Als Past-President der Deutschen Diabetes Gesellschaft (DDG) stellte Professor Dr. med. Dirk Müller-Wieland, den Ansatz der Diabetes-Akte eDA der DDG vor. Er betonte, dass der Fokus auf der Strategie zur Gestaltung der Versorgung, Forschung und Prävention liege. Man müsse sich aktiv in den Prozess einbringen, aber hierfür zunächst einen Schritt zurückgehen und sich fragen, „wie wir uns als medizinische Fachgesellschaft die Versorgung der Zukunft vorstellen“, so Prof. Müller-Wieland weiter. Die Tatsache, dass pro Stunde drei Menschen an Diabetes sterben, zeige die Wichtigkeit einer nationalen Diabetes-Strategie. Das Ziel hierbei sei eine Normalisierung der Lebenszeit und -qualität, erklärte der Professor. Um die digitale Transformation zum Nutzen der Patienten zu gestalten, wurde das Konzept einer „elektronischen Diabetes-Akte DDG (eDA-DDG)“ entwickelt.

Andreas Grode von der gematik GmbH referierte über „vesta 2.0 – Interoperabilität auf Basis von Standards“ und

stellte fest, dass es „nicht allein um Wertschöpfung, sondern auch um den Dialog" gehe. Organisationen müssen sich auf Standards einigen. Hierfür wurde vesta ins Leben gerufen - das Interoperabilitätsverzeichnis des deutschen Gesundheitswesens. Dieses Verzeichnis besteht aus den Online-Plattformen vesta Standards und dem vesta Informationsportal. Grode betonte, dass es um zwei wichtige Dinge gehe: Anwendungen und Standards. Die Instanzen, die Entscheidungen treffen, müssen zusammenkommen. Wichtig sei die Öffnung der Selbstverwaltung, so Grode.

Dr. Danny Ammon vom Konsortium SMITH (Smart Medical Information Technology for Healthcare) referierte über die „Interoperabilität für Datenintegration: Wie Vernetzung von Krankenversorgung und medizinischer Forschung gelingt". Im Rahmen der Medizininformatik-Initiative (MII) wurden insgesamt 4 Konsortien (SMITH, MIRACUM, HiGHmed und DIFUTURE) in Universitätskliniken gegründet, die das BMBF fördert, um Daten aus Forschung und Patientenversorgung untereinander zugänglich zu machen und austauschen zu können.

Über ein weiteres Konsortium, das HiGHmed Konsortium, an dem auch die Medizinische Hochschule Hannover mitarbeitet, sprachen anschließend Hagen Kosock und Birger Haarbrandt. Das Ziel ist die Entwicklung einer offenen eHealth Plattform, um Daten aus Forschung und Versorgung einrichtungsübergreifend austauschbar und nutzbar zu machen. Hierzu werden internationale Standards und Profilierungen wie IHE XDS, openEHR und HL7 FHIR miteinander kombiniert. Beide Referenten betonten die Wichtigkeit einer Standardisierung der Daten bei der Erzeugung.

Alex MacLeod, Manager, HealthShare Commercial Initiatives, InterSystems, sprach über „Alexa & HealthShare" und wie digitale Assistenten, zum Beispiel Amazon Alexa, in Versorgungsszenarien eingebunden werden können. In den USA gibt es inzwischen die ersten Healthcare-Skills für Alexa. So können beispielsweise auf Basis der InterSystems-Plattform in der vernetzten Behandlung Endgeräte auch mit Sprachinterfaces wie Alexa ergänzt werden, um Gesundheitsdaten zu erfassen und mit einer einheitlichen Patientenakte zu kombinieren – und so ein umfassenderes Bild der Gesundheit des einzelnen zu bieten.

Bislang ist der Einsatz von Sprachinterfaces aber noch nicht sehr ausgereift und es dauert sicher noch, bis Alexa tatsächlich eine große Rolle im Gesundheitswesen spielt.

Markus Stein, Strategic Product Manager, RZV Rechenzentrum Volmarstein GmbH, referierte über „Semantische Interoperabilität in elektronischen Aktensystemen – Erfahrungen aus der Umsetzung in FallAkten (EFA)". Das Rechenzentrum habe über 20.000 produktive Alten und verfüge über einen enormen Erfahrungsschatz, so Stein. Vor dem Hintergrund der voraussichtlich ab 2021 zu nutzenden Patientenakten nach §291 SGB V stellt sich gerade beim Zugriff auf diese die Frage nach einer schnellen und einfachen Bereitstellung der relevanten Inhalte. Mit der Erfahrung aus mehreren, langjährigen Umsetzungen von Elektronischen FallAkten (EFA) konnten in der RZV GmbH Rückschlüsse auf die notwendige (Metadaten-) Indizierung von Akteninhalten gezogen werden. Dabei stellte vor allem die Typisierung von Dokumenten, z.B. mit Value Sets oder angelehnter Nomenklaturen, die größte Herausforderung dar.

Über die „Digitale Einbindung von Patienten in die Gesundheitsversorgung mit mobilen Anwendungen" sprach Dr. Oliver Heinze, phellowseven GmbH. Seine Firma stellt eine mobile Lösung für Patienten zur Verfügung, um eine Interaktion mit Gesundheitsversorgern zu ermöglichen. Mobile Gesundheits-Apps werden mit eHealth-Infrastrukturen verbunden.

Eine vermehrte Einbindung bedeute auch mehr Lebensqualität, so Dr. Heinze. Eine Umfrage hatte ergeben, dass 95% der Patienten einem digitalen Datenaustausch zustimmen, nur 5% lehnten das ab. Die DSGVO bestimmt hierbei die Spielregeln, so Dr. Heinze. Und die Patientendaten müssen besonders geschützt werden.

In einem Impulsvortrag „Modellbasiert zur Interoperabiliät" gab Dr. Frank Oemig, Senior eHealth Architect, Deutsche Telekom Healthcare and Security Solutions GmbH sowie CTO bei HL7 Deutschland e. V., Einblicke in die Voraussetzungen für „Healthcare Innovationen und Patientenakten". Er betonte, dass es sehr wichtig sei, dass jedes System mit den anderen Systemen „redet". Die meisten nationalen Datenaustauschspezifikationen (bspw. NFDM der gematik oder der ADT/GEKID-XML-Basisdatensatz) werden als XML-Schema herausgegeben, fälschlicherweise aber als Informationsmodell tituliert. Neuere Vorgaben basieren manchmal sogar auf Datensätzen, die lediglich eine hierarchisch geordnete Zusammenstellung darstellen. Der Datenaustausch benötigt semantische Interoperabilität zwischen allen Akteuren. Interoperabiliät bedeutet auch die Wiederverwendung von Spezifikationen, so Dr. Oemig.

Abschlussdiskussion

In einer Podiumsdiskussion am Ende des Veranstaltungstags, stellte Alexander Ihls, Strategic Business Development Manager Healthcare, InterSystems, die provokante Frage: „Sitzen wir nicht genug zusammen?". Findet also nicht genug Austausch zwischen den verschiedenen Akteuren im Gesundheitswesen statt? Für Ihls ist es enorm wichtig, dass man ein Entscheidungsgremium, ein Regulativ, mit hoheitlichen Aufgaben schaffe.

Abschließend überlegten die Podiumsteilnehmer, wie wohl die Diskussion in fünf Jahren aussehen könnte? Man möchte auf keinen Fall Einzellösungen sehen, ein E-Health-Rat solle mit Experten, aber ohne Lobbyisten besetzt, also ohne politische Machspiele aufgestellt sein, die elektronische Patientenakte wird Standard sein, es wird datengetriebene Innovationen geben, die Zusammenarbeit mit medizinischen Fachgesellschaften wird stattfinden und, last but not least, wird der Patient in den Fokus gerückt sein.

Unangefochten analog

Unschlagbar digital

–

Heute.
Morgen.
Und in Zukunft.

–

agfahealthcare.de

AGFA HealthCare

Ergebnis-Veranstaltung, Auszeichnungen Unternehmens-/Klinikführer und Nachhaltiger Krankenhauspartner 2019

ENTSCHEIDERFABRIK auf der MEDICA 2019

Die ENTSCHEIDERFABRIK konnte sich auf der diesjährigen MEDICA wieder erfolgreich präsentieren. So waren 13 Aussteller auf dem Gemeinschaftsstand in Halle 13, 60 Mitgliedervorträge wurden vor Ort gehalten, davon 18 im Kongress und auch dieses Jahr konnte wieder ein Wachstum bei den Entscheider-Karten für die MEDICA und den Deutsche Krankenhaustag für Klinikentscheider verzeichnet werden.

Veranstaltungen auf der MEDICA

Am ersten Messetag, 18.11., fand die Mitgliederversammlung der Hosp.Do.IT – Hospitalgemeinschaft für die Digitalisierung der Gesundheits- und Sozialwirtschaft statt. Themen waren unter anderem die Zielerreichung im Mitgliedsjahr 2018/19 und die strategischen Ziele und Arbeitsschwerpunkte für 2019/20. Ebenso stand am ersten Messetag die Sitzung des IuiG-Initiativ-Rats auf der Tagesordnung, der inzwischen von 32 auf 36 fördernde Verbände angestiegen ist.

Zweiter Messetag

Am zweiten Messetag, 19.11., präsentierten die Kliniken des diesjährigen Entscheider-Zyklus, wie sie von den "5 Digitalisierungsthemen der Gesundheitswirtschaft 2019" profitiert, mit der Industrie 18 ganz konkrete Digitalisierungsprojekte aufgesetzt und umgesetzt und welche Ergebnisse sie bislang erreicht haben.

Dr. Josef Düllings, Präsident des Verbandes der Krankenhausdirektoren Deutschlands (VKD), bestätigte in seiner Begrüßung die Nachhaltigkeit, aber auch Ausrichtung der

ENTSCHEIDERFABRIK mit seiner seit 2012 bestehenden Akademie für Unternehmensführung und digitale Transformation (AudG) und der Zertifizierung mit dem College of Health Information Management Executives (CHiME) zum Certified Healthcare CIO (bereits 15 Zertifikate in 2019) auf dem richtigen Weg zu sein und forderte nicht nur mehr Investitionen in die Digitalisierung oder auch Health Information Management (HIM), sondern eben auch in die Weiterbildung.

Abends wurden während der Veranstaltung "Meet IT der Club" auf dem Gemeinschaftsstand in Halle 13 die Auszeichnungen "VKD e.V. Urkunde Nachhaltiger Krankenhauspartner" und "Unternehmens-/Klinikführer 2019" vergeben.

Nachhaltiger Krankenhauspartner

Die Unternehmen Agfa HealthCare und DMI erhielten vom VKD e.V. zum wiederholten Mal die Urkunde „Nachhaltiger Krankenhauspartner hinsichtlich Informations- und Medizintechnik". Die Unternehmensvertreter hatten erfolgreich die nach drei Jahren durchzuführende Reauditierung abgeschlossen.

Unternehmens-/Klinikführer des Jahres

Der Preisträger 2019 ist Prof. Dr. Axel Ekkernkamp vom Unfallkrankenhaus Berlin. Dem Preisträger wird zugesprochen, dass er im abgelaufenen Entscheider-Zyklus sichergestellt hat, dass das „Business-IT Alignment" im gewählten Projekt nicht aus den Augen verloren wurde und er sich durch die erfolgreiche Wahrnehmung seiner Führungsfunktion Themenkompetenz erarbeitet hat.

Der Unternehmens-/Klinikführer des Jahres gibt dann im Entscheider-Zyklus 2020 auf folgenden Veranstaltungen seine konstruktive Kritik:

- Entscheider-Event: bei der Wahl der fünf Digitalisierungsthemen aus den zwölf Finalisten am zweiten Veranstaltungstag
- Ergebnis-Veranstaltung, d. h. Präsentation der Ergebnisse der Digitalisierungsprojekte auf dem Deutschen Krankenhaustag/MEDICA
- Entscheider-Event: bei der finalen Präsentation und Auszeichnung der Projektgruppen im Folgejahr

Start Up und Young Professional Session

Am dritten und somit letzten Messetag ging es um Unternehmen, die noch nicht länger als drei Jahre am Start sind und eine interessante Geschäftsidee für Kliniken und z.B. Heime verfolgen. Die Verleihung des "Start Up und Young Professional Preises" wird im Rahmen des Entscheider-Event im Februar vorgenommen.

Health IT Talk: Frühwarnsystem unterstützt Intensivmediziner

Ein angehender Herzchirurg am DHZB hat eine intelligente Software zur Früherkennung postoperativer Komplikationen entwickelt. Das medizinische „Frühwarn"-System war Thema des Health IT Talks Berlin Brandenburg Dezember 2019 im 13. Jahr mit über 50 Teilnehmern. „Big Data und Artificial Intelligence (AI) haben in der Medizin großes Potenzial, bislang wurden allerdings nur wenige praktische Anwendungen entwickelt und retrospektiv evaluiert", erklärte Dr. Alexander Meyer, Informatiker und Mediziner in Ausbildung zum Facharzt für Herzchirurgie am Deutschen Herzzentrum Berlin (DHZB). Die Arbeitslast der Mediziner ist erheblich. Dabei müssen Messwerte und Kurven richtig interpretiert und priorisiert werden. Die Ärzte treffen lebenswichtige Entscheidungen, oft allein und in Zeitnot. Kurz: Die Menge an Patientendaten ist zu umfangreich, als dass eine Person sie wirkungsvoll bearbeiten könnte.

Mustererkennung und Machine Learning

Diese Notlage inspirierte Alexander Meyer: Eine Software könnte dabei helfen, die Daten im Sinne eines Frühwarnsystems rasch und richtig zu interpretieren. Intelligente Systeme zeichnen sich bisher aus, dass Regeln und Daten, klassisch programmiert, zu Antworten führen. Bei AI ist es ganz anderes. Hier führen nämlich Daten und Antworten über Machine Learning zu neuen Regeln. Alexander Meyer meinte: „Wir handeln reaktiv anstatt präventiv. AI kann sehen, was wir nicht entdecken". Dies ist Kernfeld von Mustererkennung und Machine Learning.

Sein neu entwickeltes AI-System soll das ändern können. Es bewertet bei Intensivpatienten das Risiko für bestimmte Komplikationen und warnt Pflegekräfte wie Ärzte vor, noch bevor es zu „echten" Symptomen bei Patienten der Intensivstation kommt. Die Software kann Symptome identifizieren, noch lange bevor sie für Ärzte und Pflegekräfte ersichtlich werden. Potenziell lebensbedrohliche Zustände können somit vorausgesagt und rechtzeitig durch entsprechende therapeutische Maßnahmen vermieden werden.

„Vor allem geht es uns dabei um die intensivmedizinische Nachbehandlung von Patienten, die am Herzen operiert wurden", führte Alexander Meyer aus. „Hier gibt es eine Reihe bekannter postoperativer Komplikationen, die umso besser behandelt werden können, je früher sie erkannt werden." Das Team der Intensivstation am DHZB verfüge zwar über die bestmöglich technische Ausstattung, Erfahrung und Expertise, dennoch gäbe es Fälle, in denen Komplikationen erst spät diagnostiziert werden können, insbesondere in Phasen besonders hoher Arbeitsbelastung und angesichts einer Vielzahl unterschiedlicher Überwachungsdaten.

Modell-Transparenz und Entscheidungstransparenz

Das von Dr. Alexander Meyer und seinem Team entwickelte Monitoring-System setzt alle Messwerte in Echtzeit in Bezug zu einander und wertet sie hinsichtlich erster Anzeichen drohender Komplikationen aus. Es basiert auf der enormen „Erfahrung" der Messwerte von über 11.000 intensivmedizinischen Behandlungen am DHZB, mit denen die künstliche Intelligenz „gefüttert" wurde. Maxime dabei sind Modell-Transparenz sowie Entscheidungstransparenz. Dabei bleibt für den sinnvollen Einsatz Zusammenarbeit von Domain-Experten mit AI-Experten wichtig.

Das System läuft am Deutschen Herzzentrum Berlin im Testbetrieb, zunächst ausschließlich zu wissenschaftlichen Zwecken. Anhand der dabei gewonnen Daten erfassen und bewerten Dr. Meyer und sein Team die Vorhersagequalität der

Referent Dr. Alexander Meyer, Informatiker und Mediziner in Ausbildung zum Facharzt für Herzchirurgie am Deutschen Herzzentrum Berlin (DHZB)

Reiner Petersen, Leiter Informationstechnik im Deutschen Herzzentrum Berlin, moderierte den Health IT Talk Berlin Brandenburg.

künstlichen Intelligenz nun im Rahmen einer aufwändigen Studie so akkurat wie irgend möglich. „Stark vereinfacht gesagt zeigen unsere Daten, dass postoperative Komplikationen mit Hilfe der neuen Software tatsächlich früher und zuverlässiger vorausgesagt werden konnten, als es dem Menschen im klinischen Alltag möglich wäre – und dass das System immer besser wird, je mehr es lernt".

Alexander Meyer betonte: „Wir können und wollen dem Intensivmediziner die Entscheidungen nicht abnehmen", und unterstrich: „Aber wir wollen ihm dabei helfen, die richtige Entscheidung sehr früh zu treffen und dem Patienten damit vielleicht das Leben zu retten". Doch er bleibt realistisch: „Wir müssen den Einsatz von Artificial Intelligence ebenso validieren wie ein Arzneimittel."

www.dhzb.de

von Wolf-Dietrich Lorenz, Krankenhaus IT Journal

Dr. Alexander Meyer gehört zu den Studienleitern (PI) des durch das Bundesministerium für Forschung und Bildung geförderten Berliner Zentrums für Maschinelles Lernen (BZML), wesentliche Punkte seiner Entwicklung sind bereits zum Patent angemeldet.

Bereits 2017 wurde Dr. Alexander Meyer in das „Clinician Scientist Program" am Berlin Institute for Health (BIH) der Charité und des Max-Delbrück-Centrums für Molekulare Medizin aufgenommen.

Das Förderprogramm ermöglicht Ärztinnen und Ärzten eine strukturierte Facharztweiterbildung mit genug „geschützter Zeit" für klinische und grundlagenorientierte Forschung. Dabei geht es vor allem um Translation, also die Umsetzung von Ergebnissen der Grundlagenforschung in der klinischen Anwendung. Das Projekt fördert das „Digital Health Accelerator"-Programm des BIH. Ergebnisse der Studie von Dr. Alexander Meyer erschienen in „The Lancet Respiratory Medicine", dem Fachableger für Intensivmedizin von „The Lancet", einer der bedeutendsten internationalen medizinischen Fachzeitschriften.

www.bihealth.org/
www.bzml.de/

Health-IT-Talk Berlin-Brandenburg: BVMI, KH-IT, SIBB, TMF

Im monatlichen Health-IT-Talk Berlin-Brandenburg tauschen sich verbands- und fachrichtungsübergreifend Branchenkollegen zur Digitalisierung der Gesundheitswirtschaft aus (Berufsverband Medizininformatik BVMI, Bundesverband der Krankenhaus IT-Leiterinnen/Leiter e.V KH-IT, Verband der Software-, Informations- und Kommunikations-Industrie in Berlin und Brandenburg e.V. SIBB, TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V.). Durchschnittlich nehmen rund 50 Health-IT Kollegen die Möglichkeit zum Lernen, Diskutieren und Vernetzen wahr. Es ergibt sich ein „interkulturelles" Networking zwischen Anwendern, Herstellern, Beratern, Politikern, Forschern und Patienten. Über die Jahre hinweg hat sich für die Health-IT eine Signalwirkung für das Bundesgebiet und darüber hinaus entwickelt. Unterstützt durch Non-Profit-Organisationen ist die Reihe zudem frei von wirtschaftlichen Interessen und kostenfrei für die Teilnehmer.

Nächste Termine

13.01.2020
Pflege, AAL, IT nah am Patienten und Robotik
Referent: Dr. Karsten Schwarz, Medizinische Fakultät Martin-Luther-Universität Halle-Wittenberg

10.02.2020
Health-IT Talk (Februar 2020)

09.3.2020
Health-IT Talk (März 2020)

06.04.2020
Health-IT Talk (April 2020)

www.health-it-talk.de

Wie Software und Medizinprodukte das Gesundheitswesen bestimmen

Ein Blick in die Zukunft der Medizin

75/20/2 – diese kryptische Zahlenkombination steht für ein gleich dreifaches Jubiläum: NSF International, eine unabhängige, globale Gesundheitsorganisation, die die Entwicklung von Normen erleichtert, Produkte für die Bereiche Lebensmittel, Wasser, Gesundheitswissenschaften und Konsumgüter testet und zertifiziert, um gesundheitsschädliche Auswirkungen zu minimieren und die Umwelt zu schützen, feiert seinen 75. Geburtstag, PROSYSTEM sein 20-jähriges Bestehen und seit zwei Jahren ist letzteres ein Teil der NSF-Gruppe. Grund genug, diese Anlässe mit einem hochkarätig besetzten Expertenpanel zu feiern. Unter dem Titel „Zukunft der Medizinprodukte in Europa: Ausblick 2020-2025" ging es um die Auswirkungen der EU-Medizinprodukteverordnung auf den Markt und die Anbieter sowie den Einfluss Künstlicher Intelligenz (KI) auf den Prozess.

Oliver Christ, Executive Vice President NSF PROSYSTEM, stellt fest, dass namhafte Unternehmen aus anderen Branchen bereits KI einsetzen und mittlerweile auch auf das Gesundheitswesen schielen. Als Beispiele nannte er Google und Amazon. „Je mehr Algorithmen im Gesundheitswesen eingesetzt werden, desto drängender wird die Frage nach deren Qualität", so Christ. Er sieht kurz- bis mittelfristig die Einführung entsprechender Zertifizierungen, wie es die Regulierungsbehörde Food and Drug Administration (FDA) in den USA vormacht. „Unsere Kunden verstehen die Bedeutung und den Sicherheitsnutzen einer unabhängigen Prüfung und Zertifizierung ihrer Produkte durch einen akkreditierten Zertifizierer wie NSF International, damit sie sich frühzeitig auf diese Entwicklungen vorbereiten können."

Woher nimmt Christ die Gewissheit, dass Microsoft, Amazon, Apple und Alphabet ins Gesundheitswesen einsteigen? „Sie können schlicht nicht anders", sagt er. „2021 wird das weltweite Brutto-Inlandsprodukt 100 Billionen Dollar betragen, 10 Prozent davon entfallen auf den Bereich Healthcare. Da dem öffentlichen Sektor die Mittel für Investitionen in Innovationen fehlen, werden die genannten Großen mangels lukrativer Alternativen einsteigen. KI und Big Data sind die Basis für neue Geschäftsmodelle und zukünftiges Wachstum."

Volles Haus meldete NSF PROSYSTEM zur Feier seines Dreifachjubiläums in Hamburg.

Ein Blick ins Jahr 2025

Darüber hinaus ändern sich bis 2025 die Rahmenbedingungen. Das Wichtigste: Der passive Patient von heute wird ein informierter Verbraucher und aktiver Kunde im digitalen Gesundheitsmarkt. „Jeder Verbraucher kennt über den Health-Index seinen Gesundheitszustand und kann ihn beeinflussen und verbessern – etwa durch Ernährung, Regeneration, Spiritualität, Sport, Entwicklung der Immunität und ähnliches", ist Christ überzeugt. Die Lebenserwartung von in diesem Jahr Neugeborenen wird mehr als 99 Jahre betragen.

Begleitet wird das durch die Entwicklung von Fitnesstrackern und Wearables, mit denen wir unsere Gesundheit in Echtzeit überwachen und sekündlich neue Updates erhalten. Dank KI und maschinellem Lernen können Prognosen erstellt sowie Krankheiten und Unfälle vermieden werden, bevor sie auftreten. Big Data öffnet die Tür zu einer viel effektiveren Krankheitsprävention.

Wird der Patient mündiger, ändert sich auch die Rolle des Arztes. Er wird zum medizinischen Berater seiner Kunden und seine Dienstleistungen werden wettbewerbsfähig. Über TeleHealth-Plattformen sind sie immer und überall abrufbar. Der „digitale Gesundheitskonsument" lässt sich von verschiedenen Quellen beraten und trifft die Entscheidungen über seine Gesundheitsvorsorge selbst.

„Damit werden klinische Daten von Patienten zur Währung des digitalen Gesundheitszeitalters, mit denen gesundheitsbezogene Dienstleistungen gezahlt werden", ist Christ überzeugt. Und: Das Gesundheitswesen muss den Fokus auf die Prävention legen, da es so wie heute künftig nicht mehr zu finanzieren ist. Ergo: Wer über medizinische Daten verfügt

Oliver Christ hieß die Teilnehmer willkommen und warf einen Blick voraus in das Gesundheitswesen von 2025.

und sie auswerten kann, hat die Macht – was aber auch den dunklen Kräften neue Möglichkeiten bietet. „Hier gilt es, frühzeitig und aufmerksam Regeln zu bestimmen und Grenzen zu ziehen", so Christ.

Aber nicht nur die Rolle von Ärzten ändert sich, auch die der Hersteller von Medizinprodukten. Sie werden zum „Digital Health Provider". Dabei verläuft der Übergang von einem Hersteller zu einer verantwortlichen Organisation mit der Kopplung unterschiedlicher Systeme mehrerer Hersteller fließend. Aber: Haftungsrisiken ändern sich damit je nach Marktbedingungen auch während der Nutzung.

Software als Medizinprodukt

Das wirft für Kim Trautman, Executive Vice President Medical Device International Services bei NSF, Fragen nach dem Status von Software als Medizinprodukt auf – besonders wenn sie Bestandteil einer Kombinationslösung, etwa mit einem Gerät, ist.

„Der Begriff ‚Software als Medizinprodukt' wird definiert als Software, die für einen oder mehrere medizinische Zwecke verwendet werden soll und diese Zwecke erfüllt, ohne Teil eines Hardware-Medizinprodukts zu sein", erläutert Trautman. Unter diese Definition fallen auch InVitro-Diagnostika. Software als Medizinprodukt kann auf universellen, nicht-medizinischen Computerplattformen betrieben werden. „Software fällt allerdings nicht unter die Definition als Medizinprodukt, wenn ihr Zweck lediglich darin besteht, eine medizinische Hardware zu betreiben. Sie kann aber in Kombination, etwa als Modul, mit anderen Produkten, einschließlich Medizinprodukten, verwendet werden", so Trautman. Software als Medizinprodukt kann mit anderen medizinischen Geräten, einschließlich Hardware-Medizinprodukten und anderer Medizinprodukte-Software, sowie mit allgemeiner Software verbunden werden. Auch Mobile Apps, die der genannten Definition entsprechen, gelten als Software als Medizinprodukt.

„Software als Medizinprodukt ist häufig Teil eines klinischen Workflows, um Diagnosen, Behandlungen und das Patientenmanagement zu verbessern. Probleme mit dem Design oder der Implementierung in einen Workflow können jedoch dazu führen, dass Benutzer falsche Entscheidungen treffen und Verzögerungen oder gar Fehler bei der Entscheidungsfindung verursachen – dies kann zu negativen Folgen für den Patienten führen", gibt Trautman zu bedenken. Also zeigt sich auch hier: Wo Licht ist, ist auch Schatten.

Bei der Entwicklung einer sicheren Software als Medizinprodukt sind also die Identifizierung von Risiken und die Festlegung von Maßnahmen, die das Vertrauen in die Software schaffen, wesentliche Aspekte. Es ist allgemeiner Konsens in Fachkreisen, dass das Testen einer Software allein nicht ausreicht, um festzustellen, ob sie betriebssicher ist. Infolgedessen ist es notwendig, quasi Vertrauen in die Software „einzubauen", um ihre Sicherheit zu gewährleisten. Als Beispiel nennt Trautman IEC 62304: eine Norm für die Lebenszyklus-Entwicklung von Medizinprodukte-Software. Die Norm spezifiziert ein risikobasiertes Entscheidungsmodell, definiert einige Prüfanforderungen und hebt drei Hauptprinzipien hervor, die die für eine Medizinprodukte-Software relevante Sicherheit fördern: Risikomanagement, Qualitätsmanagement sowie eine methodische und systematische Systemtechnik nach den besten Praktiken der Industrie.

„Software-Risiken können wir nie gänzlich ausschließen", gesteht Trautman ein. „Deshalb sollten Hersteller von Medizinprodukte-Software Kundenprobleme kontinuierlich überwachen, um das Sicherheitsniveau zu halten. Dieser Überwachungsprozess sollte neben anderem auch die Möglichkeiten beinhalten, Kundenfeedback in Form von Anfragen, Beschwerden, Marktstudien, Fokusgruppen und Services zu erfassen."

Lernen aus Erfahrung also – und dann besser machen.

Während der Pausen gab es genügend Diskussionsstoff für die Teilnehmer.

Digitalisierung der Krankenhäuser - der richtige Weg: was lohnt und was nicht?

Der Führungskräfte-Kongress Meeting-am-Meer 2020

Der digitale Patient und digitale Services stehen künftig im Mittelpunkt. Aber was zeichnet ein digitales Krankenhaus aus? Experten, Wissenschaftler und Praktiker geben Klinikverantwortlichen konkrete Handlungsempfehlungen für die digitale Transformation und ihre Umsetzung beim Kongress „Digitalisierung der Krankenhäuser - der richtige Weg: was lohnt und was nicht?“ am 5. und 6. 3. 2020 im Grand Hotel Heiligendamm an der Ostsee. Veranstalter ist *Prof. Dr. Wolfgang Riedel*, Institut für Krankenhauswesen – IfK.

Heiligendamm

Krankenhäuser müssen mehr in Digitalisierung investieren. Handfeste Gründe sprechen dafür. Mit dem Ausbau der Digitalisierung lassen sich vielfältige Ziele erreichen. Zu den Kernpunkten zählen vereinfachte Arbeitsabläufe und individualisierte Medizin. Die digitale Zukunft für Kliniken in Deutschland bedeutet: Jedes Haus muss eine individuelle IT-Strategie für sein Zielkonzept erstellen. Dazu sind die vorhandene Umgebung und die Möglichkeiten zur Optimierung von Prozessen und medizinischer Datenhaltung zu berücksichtigen. Digitalisierung wird künftig zum Wettbewerbsfaktor im Gesundheitswesen.

Impulse von renommierten Experten

Sind die Kliniken für die Zukunft gerüstet? Wie müssen Kliniken investieren? Renommierte Experten geben umsetzbare Impulse. Als Keynote-Speaker wird Wolfgang Bosbach, MdB a.D., den Bogen schlagen mit „Deutschland und Europa in Zeiten von Globalisierung und Digitalisierung“. Prof. Dr. Utz Claassen, Topmanager / Syntellix AG, weist im Gesundheitswesen auf Veränderungen in der Medizintechnik u.a. durch Digitalisierung hin. „Die Rolle der Kliniken im digitalen Gesundheitswesen“ stellt Prof. Dr. Bertram Häussler, IGES, vor. Dr. Frank Wartenberg, IQVIA, referiert über „Digitale Trends im Gesundheitswesen“. Florian Benthin, Deloitte, fokussiert bei der Digitalisierung in Deutschland auf den aktuellen KIS-Markt. Prof. Dr. Thomas Jäschke, smartcircles AG, FOM Hochschule, benennt bei den Erfolgsfaktoren der Digitalen Transformation die Notwendigkeit eines strukturierten Vorgehensmodells. „Medizintechnik 2030“ ist Thema von Oliver P. Christ, Pro-System AG, mit aktuellen Trends und Herausforderungen. Digitalisierung am Beispiel vom Klinikum Itzehoe hinterfragt Bernhard Ziegler, Krankenhausdirektor beim Klinikum Itzehoe: „Selbstzweck oder praktischer Nutzen?“. Als weitere Take home-Points gibt Prof. Dr.-Ing. Wolfgang Riedel, IfK Institut für Krankenhauswesen, „Strategieansätze für Kliniken im Umgang mit der Digitalisierung (Auswirkungen, Nutzen)“ als Leitfaden für das Management den Teilnehmern für die Umsetzungen der Impulse aus dem Meeting-am-Meer 2020 auf den Weg.

Die richtige Strategie zur Digitalisierung

Diese Themen betreffen alle Partner im Gesundheitswesen. Dabei kann das Management seiner Rolle in der digitalen Transformation gerecht werden kann, wenn es sich an die Spitze setzt, sie aktiv vorantreibt und ein zukunftweisendes Mindset etabliert. IT-Management und Digitalabteilungen können als interne Innovatoren neue Potenziale für nachhaltige digitale Lösungen identifizieren Damit lässt sich nachhaltige Wertschöpfung bei digitalen Services rund um den Patienten ermöglichen. Veranstalter Prof. Riedel regt an: „Diskutieren Sie mit uns Hintergründe und Lösungsansätze für das digitale Krankenhaus der Zukunft. Finden Sie die richtige Strategie zur Digitalisierung Ihrer Klinik und zur Prozessunterstützung. Investieren Sie gezielt in die richtigen Bereiche!“

www.meeting-am-meer.de

Prof. Dr.-Ing. Wolfgang Riedel, IfK Institut für Krankenhauswesen: Strategieansätze für Kliniken im Umgang mit der Digitalisierung (Auswirkungen, Nutzen), ein Leitfaden für das Management

Medizingeräte im Visier von Hackern:

Security Check on Medical Devices von TÜV SÜD für mehr Sicherheit im Gesundheitswesen

Die Digitalisierung ändert den Krankenhausalltag spürbar. In digitalen Patientenakten werden hochsensible persönliche Daten zum Krankheitsverlauf erfasst, wie beispielsweise Laborwerte, Untersuchungsergebnisse, Röntgenbilder oder Medikationen. Untersuchungen werden mittels vernetzter Medizingeräte durchgeführt, und Ärzte haben via Tablet jederzeit Einblick in den Gesundheitsstand ihrer Patienten. Die Digitalisierung macht Krankenhäuser zwar leistungsfähiger und effizienter, aber gleichzeitig auch angreifbarer. Denn jedes vernetzte Gerät kann in einem weit verzweigten Kliniknetzwerk zu einem potenziellen Einfallstor für Hacker werden – sofern es nicht richtig abgesichert ist.

Verdeutlicht wird die Dringlichkeit der IT-Sicherheit von vernetzten Medizingeräten durch die Zunahme von Cyber-Angriffen in Form von Denial-of-Service-Attacken oder Botnet- Angriffen. Unter einem „Denial of Service Angriff" versteht man die absichtliche Überlastung eines Datennetzes, welche zu einer Nicht-Verfügbarkeit des Services führt. Das kann gravierende Folgen haben, wenn beispielsweise lebenserhaltende Systeme in Krankenhäusern betroffen sind. „Botnetze" wiederum sind Netzwerke, die aus ferngesteuerten Computern, IT-Ressourcen und Bots bestehen. Die Computer werden mit Malware infiziert, die es ermöglicht, sie fernzusteuern. Ungesicherte IT oder angeschlossene Medizingeräte eignen sich als ideale Eintrittspforte für Hacker, die sich so über das Netzwerk Zugriff auf weitere Geräte verschaffen. Um solche Szenarien zu verhindern, muss die Cybersicherheit von Medizingeräten heute oberste Priorität haben und als integraler Produktbestandteil betrachtet werden.

Security by Design minimiert das Risiko

Umfassende Cybersicherheit muss weiter gedacht werden, als die bisher üblichen punktuellen Sicherheitsupdates dies leisten können. Sie ist keine Momentaufnahme, sondern ein kontinuierlicher Prozess, der den kompletten Lebenszyklus von Produkten und Systemen betrifft. Auch für Medizingeräte gilt in Zukunft immer mehr: Im Idealfall ist die Cybersicherheit schon von Anfang an eingebaut, man spricht hier von Security by Design. Dabei kommen Dokumenten- und Prozessaudits ebenso zum Einsatz wie regelmäßige Systemprüfungen durch Schwachstellen-Scans und Penetration-Tests. Hier setzen die Security Check on Medical Device Services von TÜV SÜD an: Umfangreiche Tests bewerten automatisch und manuell den Sicherheitsstatus von vernetzten Medizingeräten. Dabei wird der Sicherheitsstatus der Geräte anhand von Industrienormen wie UL 2900-2-1, IEC/TR 60601-4-5 und generellen Security by Design Prinzipien bewertet. Kritische Punkte, die eine Sicherheitslücke darstellen können, werden dem Hersteller angezeigt. Der Prüfprozess bewertet die kritischsten Bereiche, die die Cybersicherheit von netzwerkfähigen Geräten heute beeinflussen. Analysiert werden u.a. die Geräte-Firmware, produktintegrierte Web-Oberflächen, die Gerätekommunikation, jegliche Schwachstellen, die Sichtbarkeit der verwendeten Hardware- und Softwarekomponenten sowie der offenen Schnittstellen.

Dynamische Bedrohungslage: Angriffen zuvorkommen

Die Bedrohungslandschaft entwickelt sich ständig weiter, und skrupellose Angriffe sind nur noch eine Frage der Zeit. Darum ist es zwingend erforderlich, das Angriffsrisiko auf vernetzte Medizingeräte zu minimieren. Basierend auf den Prioritäten von Kliniken und Arztpraxen werden die Ergebnisse des Security Check on Medical Device Services auf die jeweiligen Industriestandards abgebildet. Diese können dann verwendet werden, um die Anforderungen und Bedürfnisse der Betreiber besser zu erfüllen. Letztlich geht es darum, dass sich beide Seiten – sowohl Hersteller als auch Betreiber von vernetzten Medizingeräten – ihrer Verantwortung in Sachen Cybersicherheit bewusst werden und noch enger zusammenarbeiten. Nur so lässt sich ein möglichst hohes Sicherheitsniveau erreichen, um Patienten effektiv zu schützen.

Security-by-Design in der Medizintechnik

Diagnose: Sicherheitslücke

Drei von zehn Patienten haben bei einem Krankenhausaufenthalt Angst vor dem Ausfall der Computersysteme, so eine aktuelle Studie. Zu Recht: Immer häufiger werden Gesundheitseinrichtungen Opfer gezielter Angriffe aus dem Cyberspace, die den Betrieb lebensnotwendiger Infrastrukturen einschränken oder sogar tagelang lahmlegen. Eine der größten Angriffsflächen und damit beliebtesten Einfallstore für Hacker stellen dabei vernetzte Medizingeräte dar.

Veraltete Systeme: Eine tickende Zeitbombe

Da die IT-Sicherheit netzwerkfähiger Systeme in der Vergangenheit nur unzureichend Beachtung fand, diese aber dennoch millionenfach in die IT-Netzwerke von Krankenhäusern oder Arztpraxen integriert wurden, stellen sie heute ein enormes Sicherheitsrisiko dar. Bereits eine einzige Schwachstelle genügt Hackern, um sich unbemerkt Zugriff auf das gesamte Netzwerk der betroffenen Gesundheitseinrichtung mit allen angeschlossenen Anwendungen zu verschaffen.

Um das aktuell erforderliche Sicherheitsniveau zu erreichen, müssen alle Beteiligten gleichermaßen ihrer Verantwortung gerecht werden. Das stellt Betreiber, vor allem aber Hersteller netzwerkfähiger Medizingeräte vor enorme Herausforderungen.

Hersteller unter Druck

Aufgrund der hohen Marktdynamik benötigen neue Medizinprodukte kurze Einführungszeiten, müssen jedoch zugleich für die Marktzulassung verschiedenste Anforderungen erfüllen. Dabei rückt die Cybersicherheit immer stärker in den Fokus: Bei einer mangelhaften IT-Sicherheitsbewertung können Behörden den Herstellern entsprechender Geräte den Zugang zu den Märkten verwehren.

Hersteller sind folglich gezwungen, Cybersicherheit als integralen Bestandteil ihrer Produktentwicklung zu betrachten. Um Schwachstellen zu minimieren, muss der "Security-by-Design"-Ansatz gelten. Das ist allerdings leichter gesagt als getan: Obgleich sich die meisten Hersteller netzwerkfähiger Medizingeräte der Cybersicherheitsrisiken bewusst sind, führt in den meisten Fällen der Mangel an Know-how und qualifizierten Ressourcen während des gesamten Entwicklungsprozesses zu sicherheitsrelevanten Nachlässigkeiten.

Verbindliche Standards für die Cybersicherheit fehlen

Eine der größten Herausforderungen stellt das Fehlen verbindlicher Normen in Bezug auf die Cybersicherheit von Medizingeräte dar. Da beispielsweise strenge Codierungsvorgaben fehlen, weisen viele Medizingeräte in ihrer Software und den Host-Betriebssystemen Schwachstellen auf. TÜV SÜD engagiert sich im Rahmen der Charter of Trust, einer Allianz global führender Unternehmen für mehr Cybersicherheit, für einen klaren regulatorischen Rahmen mit strengen Kriterien, die die grundlegende IT-Sicherheit und den Schutz lebenswichtiger Anwendungen gewährleisten.

Security by Design: IT-Sicherheit von Anfang an

Hersteller von Medizinprodukten begleitet TÜV SÜD während des gesamten Produktentwicklungszyklus mit einer Reihe von Dienstleistungen. Diese reichen von der frühen Bewertung und Begleitung der Produktentwicklung über ein sogenanntes Early-Bird-Assessment bis zur Unterstützung beim globalen Marktzugang. Medizintechnik und Medizinprodukte werden dafür umfangreichen Prüfungen unterzogen: Neben der funktionalen Sicherheit werden alle relevanten Faktoren im Bereich Cybersicherheit genau unter die Lupe genommen. Dies erfolgt unter anderem über Dokumenten- und Prozessaudits, obligatorische und regelmäßige Systemprüfungen mit Schwachstellen-Scans sowie Penetrationstests für Hard- und Software.

Ein besonderes Augenmerk liegt dabei auf sämtlichen Kommunikationsanschlüssen und Schnittstellen, mit denen ein Gerät an das Netzwerk einer Gesundheitseinrichtung angeschlossen werden kann. Zudem dürfen ausschließlich Betriebssysteme zum Einsatz kommen, die grundlegende Sicherheit und Schutz für lebenswichtige Anwendungen bieten. Mögliche Sicherheitslücken können so bereits in einer frühen Phase der Produktentwicklung und vor der Marktzulassung behoben werden.

Neue Richtlinie verschärft Vorgaben

Die Medical Device Regulation (MDR) ist ab Mai 2020 zu erfüllen und soll die Qualität und Sicherheit von Medizinprodukten auf dem EU-Markt weiter verbessern. Hierfür wurden die geltenden Anforderungen präzisiert und verschärft. Hersteller und Benannte Stellen bereiten sich bereits seit Jahren auf die Veränderungen vor, doch es gibt noch viel zu tun. Die

klinische Bewertung und zugehörige Unterlagen müssen beispielsweise während des gesamten Lebenszyklus eines Produkts anhand von Praxisdaten regelmäßig aktualisiert werden. TÜV SÜD ist eines von bislang sechs Unternehmen, die als Benannte Stelle offiziell registriert sind. Insgesamt haben 40 Unternehmen eine Anerkennung beantragt. Hersteller von Medizinprodukten höherer Risikoklassen müssen Benannte Stellen in den Zulassungsprozess einbeziehen.

Internationale Expertise

TÜV SÜD ist eine der weltweit führenden Benannten Stellen für Konformitätsbewertungen von Medizinprodukten. Mit mehr als 800 Mitarbeitern im Bereich Medizinprodukte an mehr als 30 Standorten kann TÜV SÜD auf ein weltweites Netzwerk an Experten in unterschiedlichen Zielmärkten zurückgreifen. Hersteller profitieren sowohl von der fachlichen Kompetenz als auch von umfassenden internationalen Akkreditierungen wie NRTL und INMETRO sowie dem Medical Device Single Audit Program (MDSAP). Mit einem einzigen Qualitätsmanagement-Audit lassen sich so zugleich die regulatorischen Anforderungen in Australien, Brasilien, Japan, Kanada und den USA erfüllen.

Ausblick: Zertifizierung nach verbindlichen Standards

Nie war es wichtiger, Safety- und Security-Features in vernetzte Systeme zu integrieren als im Zeitalter des Internet of Things (IoT) mit seiner dynamischen Bedrohungslandschaft. Immer mehr medizinische Geräte bieten Schnittstellen für den Internetzugang und benötigen damit einen Nachweis für den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der Daten und des jeweiligen Systems.

Eine der größten Herausforderung besteht dabei in den uneinheitlichen und bislang nicht verbindlichen Standards bezüglich der IT-Sicherheitsvorgaben. Bereits im frühen Entwicklungsstadium überprüft und begleitet TÜV SÜD Medizingeräte mit umfassenden Tests und Bewertungen auf ihre IT-Sicherheit und unterstützt damit Hersteller und Anwender gleichermaßen. Dabei ist ein neues Testverfahren in Entwicklung, das mit der dynamischen Bedrohungslandschaft nachhaltig Schritt halten kann. Denn: Prüfungen und Zertifizierungen weisen nicht nur nach, dass die jeweiligen regulatorischen Anforderungen eingehalten werden. Sie gewährleisten vor allem die Qualität und Sicherheit von Produkten, bei denen es im Zweifelsfall um Menschenleben geht.

akquinet AG präsentiert sich mit Partnern auf der MEDICA

In Halle 13 am Stand F37 präsentierte sich die akquinet AG gemeinsam mit ihren Partnern und stellte ihre neue objektorientierte Speicherlösung für das Gesundheitswesen, aber auch einen Abwurfadapter vor ***(siehe dazu Artikel auf S.79 „IT-Sicherheit im Krankenhaus“).***

central ONE, eine Lösung für die medizinische Branche, fokussiert auf die Haltung von großen Datenmengen aus bildgebenden medizinischen Umgebungen, bietet neben der sicheren Datenhaltung spezifische Workflowkomponenten, ein Vendor-neutrales-Archiv (VNA) und einen DICOM-optimierten Multifunktionsviewer mit integriertem non-footprint-Verfahren.

Die Herausforderung

Die heutigen in den unterschiedlichen medizinischen Fachgebieten eingesetzten bildgebenden Systeme erzeugen anwendungsspezifische Formate, die wiederum häufig noch in isolierten Archiven gespeichert werden. Diese Datensilos bremsen eine effiziente Diagnostik aus, die Medienbrüche in den anschließenden digitalen Workflows führen zu einer wahren „Kostenexplosion“.

Die Lösung

centralONE med realisiert auf Basis der hyperperformanten, unbegrenzt skalierbaren und kostengünstigen Objektspeichertechnologie von Cloudian und einer Dicom-orientierten Software ein Vendor-Neutrales Archiv (VNA). Durch die Integration eines universellen Bildbetrachters (Multifunktionsviewers) und automatisierter Workflows wird das Formatchaos nahezu beseitigt und Bilddaten werden in Echtzeit und ortsunabhängig verfügbar gemacht.

Bei der Visualisierung wird sichergestellt, dass einmal ins Archiv gelangte Daten nicht mehr transferiert oder umgelagert werden. Non-footprint ist vollständig umgesetzt und macht den Einsatz der Lösung effizient und sicher.

Digitale Pathologie im Fokus

centralONE med verkürzt den Zeitraum von der Präparation der Proben bis zur Retournierung der Analyseergebnisse auf ein absolutes Minimum.

Die Pathologie ist eine der zeitraubenden Untersuchungsmethoden in der medizinischen Praxis. Während die Vorbereitung von Gewebeproben und Körperflüssigkeiten standardisiert und etabliert ist, dauert die Bereitstellung und Interpretation der Proben aufgrund des chronischen Mangels an Pathologen und zeitraubender manueller Prozesse häufig Tage und Wochen.

In die Lösung integriert sind unter anderem die Scannertechnologien von 3DHistec, Hamamatsu und Leica aber auch die VNA und Wokflowkomponenten von Vitrea (Canon)..

Die akquinet AG ist ein international tätiges, kontinuierlich wachsendes IT-Beratungsunternehmen mit Hauptsitz in Hamburg. Aktuell werden 845 Spezialisten mit umfassenden Kenntnissen in zukunftsorientierten Technologien beschäftigt. Das Unternehmen hat sich auf die Einführung von ERP-Systemen (SAP und Microsoft) und die Individualentwicklung von Softwarelösungen spezialisiert. Speziell im Gesundheitswesen und der Sozialwirtschaft verfügt AKQUINET über langjährige Branchenexpertise und zertifizierte Lösungen. In vier hochleistungsfähigen Rechenzentren in Hamburg, Norderstedt und Itzehoe betreibt AKQUINET für Unternehmen aller Größen IT-Systeme im Outsourcing. Das Twin Datacenter erfüllt die Standards TÜV IT TSI 4.1 und EN50600.

Cloudian® ist ein Datei- und Objektspeicheranbieter mit Sitz im Silicon Valley, der auf S3-API-Speichersysteme spezialisiert ist. Cloudian, dessen Wurzeln im Bereich der Entwicklung von Nachrichtenübermittlungssystemen für große Unternehmen liegen, stellte 2011 seine objektbasierte Plattform HyperStore® vor.

Die Cloudian-Produkte werden von Partnern, darunter Amazon, Lenovo, Cisco, Hewlett Packard Enterprise und QCT sowie Wiederverkäufer, weltweit angeboten.

HYLAND ist ein internationales Softwareunternehmen mit Sitz in Westlake, Ohio. Die beiden Themenschwerpunkte sind branchenübergreifende DMS/ECM-Lösungen und Lösungen im Bildmanagement für das Gesundheitswesen. Mit weltweit über 3.600 Mitarbeitern und Präsenz auf allen Kontinenten ist Hyland ein global Player.

Die Lösungen im Gesundheitswesen von HYLAND Healthcare (das ACUO VNA, der non-footprint-Viewer NILread und die diagnostischen Workflows) werden weltweit von Top-Einrichtungen im Gesundheitswesen eingesetzt, darunter die gesamten Streitkräfte der Vereinigten Staaten von Amerika.

Mehr Informationen:
www.youtube.com/watch?v=NDNgIwvQABE
akquinet.com/centralone-med.html

Optimierung des Rechnungseingangs für den Klinikverbund Südwest

Schluss mit Papierrechnungen: Digitales Rechnungsmanagement

Jährlich gehen beim Klinikverbund Südwest über 100.000 papiergebundene Rechnungen ein. Die mit der Bearbeitung anfallenden Kosten sind hoch und steigen kontinuierlich an. "Die Anzahl der Rechnungen steigt ständig", so Hans-Ulrich Graf, Leiter des Geschäftsbereichs IT. „Der Rechnungseingang erfolgt zentral an einem Standort, die anschließenden Folgeprozesse bestehen aus vielen Einzelschritten: Öffnen der Rechnungen, Versehen mit Eingangsstempeln, Verteilung an den zuständigen Sachbereich, eine erste Rechnungserfassung und Vorkontierung, usw. – eine Neustrukturierung und eine damit einhergehende Digitalisierung, eines der zentralsten Prozesse im Verbund, hatte daher zum obersten Ziel, den gesamten Rechnungsworkflow noch effizienter und transparenter zu gestalten."

Neben deutlichen Kostensenkungen in der FiBu bzw. dem Rechnungswesen sowie einer deutlichen Steigerung der Bearbeitungsqualität soll durch den neuen digitalen Prozess die Grundlage für die steigenden Anforderungen im Hinblick auf die ab November 2020 verpflichtende elektronische Rechnungsstellung gelegt werden. „Zukünftig soll es im Klinikverbund keinen analogen Bestellworkflow mehr geben", führt Graf weiter aus. „Alle Prozesse rund um das Rechnungs- und Bestellwesen sollen in eine digitale Gesamtlösung überführt werden: Weg vom Papier – hin zu digital."„Die bereits seit vielen Jahren erfolgreiche Zusammenarbeit im Bereich der digitalen Krankenakte, veranlasste uns, auch das Projekt „Digitale Eingangsrechnung" mit der Heydt Gruppe durchzuführen. Für die Rechnungseingangslösung der Heydt Gruppe spricht die Integration der von Heydt digitalisierten Eingangsrechnungen in unser bestehendes FISystem sowie die Einbindung in bereits bestehende digitale Infrastrukturen."

Der Prozess heute

Am Verarbeitungsstandort der Heydt Gruppe wurden für die Rechnungen des Klinikverbunds Südwest zwei Postfächer eingerichtet: ein digitales Postfach für Rechnungen, die via Email kommen und ein analoges, für papiergebundene Rechnungen. Die datenschutzkonformen Transportservices der Heydt Gruppe leeren das analoge Postfach und bringen die Belege an den Verarbeitungsstandort. „Hier ist die räumliche Nähe zum Dienstleister von Vorteil", führt Graf aus.

Die papiergebunden Rechnungen werden geöffnet und gescannt. Gescannte und digitale (Email-)Rechnungen werden via Texterkennungssoftware (OCR) erfasst. „Dank der bei Heydt vorhandenen Infrastruktur zur automatischen Datenerkennung werden Rechnungskopfdaten oder einzelne Rechnungspositionen erkannt." Mit Hilfe der Positionsdaten kann jede Rechnung anhand der Bestellnummer mit den Bestellstammdaten aus dem ERP-System sachlich und rechnerisch automatisch geprüft werden. Anschließend erfolgt ein Abgleich zwischen Lieferscheinen und Bestellungen.

Das Ergebnis

„Die digitale Rechnungseingangslösung der Heydt Gruppe und insbesondere die damit verbundene Prozessautomatisierung in unserem Rechnungswesen trägt einen wichtigen Teil dazu bei, unsere Produktivität weiter zu steigern, die Datenqualität zu erhöhen und die rechtlichen Anforderungen zu erfüllen." Der neue transparente, noch effizientere Prozess lässt eine graphische, DIN EN ISO 9001-gerechte Darstellung in unserer Business Process Engine zu, so Graf. „Die Heydt Gruppe bietet uns eine automatische Rechnungserkennungslösung, die die digitalen Rechnungen schnell in unseren digitalen Workflow unseres ECM-Systems HYDMedia der AgfaHealthcare in einen zielgerichteten Zugriff leitet." Einsparpotential besteht nicht nur bei den Lagerkosten, sondern gerade bei Bearbeitungs- und Papierkosten. Vorteile eines digitalen Rechnungseingangs sieht Graf insbesondere in der allgegenwärtigen Verfügbarkeit auch auf mobilen Devices, im schnellen Wiederfinden der einzelnen Belege, in der dauerhaften Lesbarkeit für die Dauer der Aufbewahrungsfrist sowie im Schutz vor Verlust. „Die Heydt Gruppe – ein seit über einem Jahrzehnt zuverlässiger Partner – hat bei uns einmal mehr eine effiziente und zuverlässige Lösung implementiert."

Der Klinikverbund Südwest mit Sitz in Sindelfingen (Baden-Württemberg) ist ein Gesundheitskonzern kommunaler Trägerschaft, mit den Standorten Böblingen, Calw, Herrenberg, Leonberg, Nagold und Sindelfingen. Von rund 5.000 Mitarbeitern werden jährlich an allen sechs Standorten zusammen etwa 550.000 Patienten stationär und ambulant versorgt.

Klinikum Frankfurt Höchst versendet Arztbriefe über KV-SafeNet direkt aus dem KIS

ORBIS eArztbrief – deutschlandweit einmalig

Prof. Dr. Ulrich Hink, Chefarzt der Klinik für Innere Medizin 1 – Kardiologie im Klinikum Frankfurt Höchst, hat gerade eine Untersuchung abgeschlossen. Er sitzt am PC in seinem Büro, vidiert den Befund und erstellt den Arztbrief. Nach seinem Okay wird beides mit einem Mausklick im Krankenhaus-Informationssystem (KIS) gespeichert. Gleichzeitig geht der Brief automatisch an den Hausarzt, der den Patienten zugewiesen hat. Wenige Minuten später in einer Praxis in der Frankfurter City: Der Arzt erwartet seinen Patienten in einer Stunde zur Besprechung. Er möchte sich ein Bild von den Untersuchungsergebnissen machen und öffnet den Arztbrief, den er sofort mit einem Mausklick in seine elektronische Patientenakte übernimmt.

Dieses Szenario funktioniert in Frankfurt so deutschlandweit zum ersten Mal. „Es war schon länger unser Wunsch, uns elektronisch mit anderen Kliniken und Praxen auszutauschen. Die Idee war, direkt aus dem KIS ORBIS heraus Formulare in einer geeigneten Art zu generieren und zu versenden", sagt Dr. Thomas Engelhardt, stellvertretender Leiter der Abteilung I – EDV/Medizininformatik. Das ist nun in Zusammenarbeit mit Agfa HealthCare, dem GNEF- Gesundheitsnetz Frankfurt am Main eG, dem Gesundheitsnetzwerk Rhein-Main und der Kassenärztlichen Vereinigung Hessen (KVH) möglich geworden.

Der Anstoß kam von niedergelassenen Ärzten im GNEF. "Der eArztbrief in KV Connect wurde über zwei Jahre von unseren Mitgliedern, haus- und facharzt-übergreifend, getestet, bevor wir uns an den intersektoralen Austausch gewagt haben", so Dr. Carola Koch, Fachärztin für Allgemeinmedizin und Vorstandsvorsitzende des Gesundheitsnetzes Frankfurt. „Parallel wurden wir von Agfa HealthCare angesprochen, ob wir gemeinsam ein derartiges Portal erarbeiten wollten", so Dr. Engelhardt. Als treibende Kraft wirkte die KVH, die anderen Entwicklungen vorgreifen und ihren Ärzten eine eigene, sichere Lösung bieten wollte. Ziel war, dass der Arzt in seiner Praxis möglichst schnell und unkompliziert alle erforderlichen Daten aus dem Klinikum erhält, ohne dass beide Seiten viel tun müssen.

Digitalisierung als Treiber

Dieses Projekt startet im Vorfeld des Klinik-Umzugs in einen Neubau. Da dort weitgehend papierlos gearbeitet werden soll, überführen die Verantwortlichen alle noch papiergebunden Prozesse in digitale Workflows. „Der elektronische Arztbrief ist dabei ein wichtiger Baustein, mit dem wir das unsägliche Briefeschreiben und -versenden beziehungsweise Faxen ablösen und sicherstellen wollen, dass der niedergelassene Arzt zeitnah alle Informationen elektronisch bekommt", führt Michael Ellerbrock, Mitarbeiter der Abteilung I und verantwortlich für das Projekt auf Seiten des Klinikums, aus.

Um einen reibungslosen Datenfluss zu gewährleisten, galt es, einige Voraussetzungen zu erfüllen: Zum einen müssen die niedergelassenen Ärzte eine Push-Nachricht bekommen, wenn ein neuer eArztbrief vorliegt, den sie dann über eine gesicherte Infrastruktur abrufen können. Zum anderen muss sichergestellt werden, dass der Brief beim Speichern im eigenen System im korrekten Patientenkontext – hier durch die KV-Stammnummer des Patienten – gespeichert wird. „Als Plattform für dieses Prozedere bietet sich das KV-SafeNet geradezu an. Wir senden Informationen an einen Verteilungsserver, der sie mit eindeutiger Identifikationsnummer an die adressierte Praxis weiterleitet und die Speicherung unter den Versicherungsstammdaten des Patienten sicherstellt", beschreibt Dr. Engelhardt den Ablauf.

Sichere Kommunikationswege als Basis

Begünstigt wurde das Verfahren dadurch, dass sich vor zwei Jahren sämtliche Vertragsärzte in Hessen mittels Konnektor an diese Infrastruktur haben anbinden lassen. „So erreichen wir theoretisch jede Praxis im Bundesland. Alle unsere Zuweiser,

Michael Ellerbrock: „Über KV-SafeNet erreichen wir mit unserem eArztbrief theoretisch jeden niedergelassenen Arzt in Hessen."

schwerpunktmäßig aus Frankfurt, Wiesbaden und Darmstadt, arbeiten auf derselben Plattform und verfügen über Konnektoren, die die Übertragung ermöglichen", so Ellerbrock. Wie sieht nun die technische Umsetzung in Frankfurt aus? KV-SafeNet bietet das erforderliche hohe Sicherheitsniveau. Darauf fußt KV-Connect, ein Kommunikationsdienst, der den sicheren Datenaustausch zwischen verschiedenen Partnern ermöglicht. Ein weiteres Hilfsmittel ist die einheitliche Spezifikation der KV-Telematik zum eArztbrief, die die Integration sowohl in Praxis- als auch in Krankenhaus-Informationssysteme gewährleistet und dadurch Medienbrüche vermeidet. „Wir versenden unsere eArztbriefe als PDF/A-Dokumente mit strukturierten Daten. Das erst ermöglicht eine teilautomatisierte Zuordnung zum Patientendatensatz", erläutert Dr. Engelhardt.

2017 hat das Klinikum Frankfurt Höchst einen Vertrag zur Umsetzung des Projektes mit Agfa HealthCare geschlossen. Parallel zum Erarbeiten der benötigten Schnittstellen konnte Prof. Dr. Hink mit seiner Klinik als Pilotanwender gewonnen werden. Auch im Gesundheitsnetz Frankfurt konnten schnell Praxen mit unterschiedlichen Verwaltungssystemen gefunden werden. „Das war wichtig, um die Konnektivität mit möglichst vielen Anbietern zu etablieren", sagt der stellvertretende Abteilungsleiter. „Erste Tests waren erfolgreich – ebenso wie der Echtbetrieb seit Anfang dieses Jahres."

Als größte Hürde erwies sich, einen elektronischen Heilberufe-Ausweis mit entsprechenden Authentifikationen für KV-SafeNet als Klinikarzt ohne KV-Zulassung zu bekommen. Mit dem nötigen Pragmatismus haben aber alle Beteiligten zu einer Übergangslösung gefunden: Zuerst erfolgt die Authentifizierung über das Rollen- und Rechtekonzept in ORBIS.

Schnell, einfach, sicher

Momentan nehmen mit vier Praxen aus dem GNEF bewusst wenige am eArztbrief-Austausch teil. „Es sollten Praxen mit unterschiedlichen Arztinformationssystemen (AIS) ausgewählt werden, um die Praktikabilität des Anschlusses zu testen", erläutert Dr. Koch.

„Zuerst möchten wir das Verfahren im Alltag testen und stabilisieren. Es laufen aber bereits intensive Gespräche mit weiteren Niedergelassenen, um das Partnernetz schnellstmöglich zu erweitern", sagt Prof. Hink. Das Problem: Seine Top-Einweiser gehören noch nicht zu den Teilnehmern, was es schnell zu ändern gilt. Auch intern laufen Gespräche, um weitere Fachabteilungen für den eArztbrief zu gewinnen.

Was will Prof. Hink primär mit der einfachen Handhabung erreichen? „Mir entsteht kein zusätzlicher Aufwand", sagt er und beschreibt den Workflow: „Ich schließe den Arztbrief mit einem Klick auf ‚Vidieren' in ORBIS ab. In dieser Sekunde wird er bereits automatisch versendet – ohne weiteren Handgriff, ohne Login in ein anderes System. Das wird alles über das KIS gesteuert. Der Brief geht über den Konnektor in KV-SafeNet und wird dort an den entsprechenden Zuweiser verteilt."

Der Prozess ist mit dem E-Mail-Verfahren vergleichbar.

Prof. Dr. Ulrich Hink: „Der eArztbrief wird beiden Seiten sehr viel Zeit sparen. Zudem können wir die Patientenbehandlung beschleunigen."

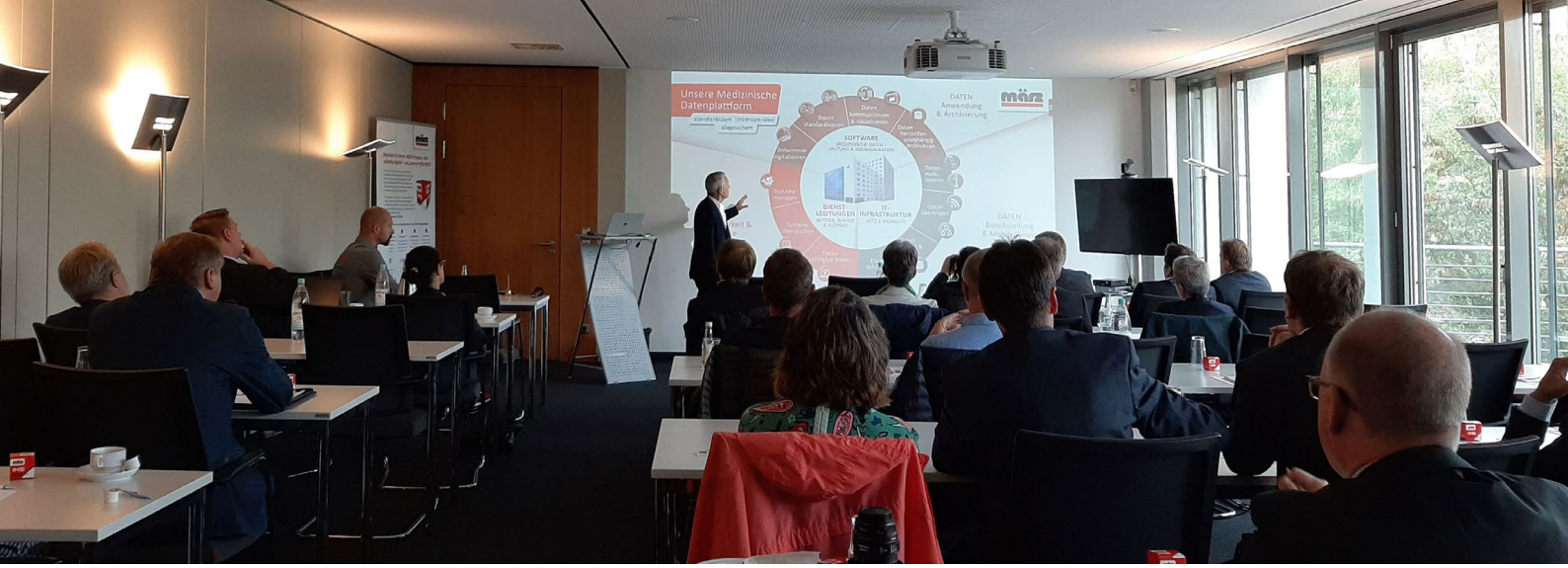
Die KV Hessen betreibt einen zentralen Server. Auf diesen übersendet das Klinikum den eArztbrief, der wie eine E-Mail verpackt ist, via Konnektor und über KV-SafeNet. Dort liegt das Dokument, bis der Empfänger es abruft. Mit einem Mausklick wird der Brief geöffnet und kann im Informationssystem der Praxis gespeichert werden. „Das ist für beide Seiten so viel einfacher als gewöhnlich", betont Prof. Hink. „Üblicherweise werden Arztbriefe gefaxt oder per Post versendet und in der Praxis dann eingescannt."

Nach uni- folgt bidirektional

Die Ambulanz der Kardiologie im Klinikum Frankfurt Höchst läuft seit Anfang Januar 2019 komplett digital. Der Chefarzt sieht enorme Chancen in der einfachen Kommunikation mit den niedergelassenen Kollegen: „Es wird beiden Seiten sehr viel Zeit sparen. Zudem erhält der Patient zügiger einen Termin zur Weiterbehandlung, weil der Zuweiser nicht mehr auf den Arztbrief warten muss. Und da die Informationen digital vorliegen, können sie auch ausgelesen werden."

Bei aller Zufriedenheit hat Prof. Dr. Ulrich Hink dann doch noch einen Wunsch: Das System sollte einen bidirektionalen Datenaustausch ermöglichen. „Hilfreich wäre eine Kommunikationsplattform, über die nicht nur wir den Zuweisern Daten schicken können, sondern auch umgekehrt. Hätten wir beispielsweise bereits im Vorfeld der Behandlung Voraufnahmen und -befunde, Laborwerte und ähnliche Informationen, würde uns das helfen." ORBIS jedenfalls ist bereits heute in der Lage, Dokumente abzurufen und einzupflegen.

Der Fokus liegt jedoch auf der Gegenwart. Zuerst gilt es, das Netzwerk an Einweisern zu erweitern und den eArztbrief klinikweit zu etablieren, denn darauf schaut nicht nur die KVH. „Das Interesse geht weit darüber hinaus. Funktioniert es bei uns, haben bereits andere Kassenärztliche Vereinigungen signalisiert, dass sie das für eine vielversprechende Alternative halten", sagt Dr. Thomas Engelhardt.



Roadshow: März präsentiert einfache und sichere Kommunikation mit der IHE BOX

Digitaler Datenaustausch zwischen Krankenhaus und MDK

Reinbek bei Hamburg, Essen, Stuttgart, München, Leipzig, Hanau und Karlsruhe. Das waren im zweiten Halbjahr 2019 die Stationen der Dialogtour „MDK – Kommunikation vollständig digitalisiert" des bundesweit aufgestellten IT-Dienstleisters März Network Services. Mehrere Hundert Teilnehmer folgten der Einladung, um sich über die März IHE BOX – und hier vorrangig den integrierten, vollständig digitalisierten MDK-Kommunikationsprozess – zu informieren und den Austausch zwischen Hersteller und Anwendern zu suchen. Die Roadshow fand gemeinsam mit dem Krankenhaus Reinbek und dem MDK Nord statt.

Die Herausforderung der Kliniken, zunehmend digital und papierlos ihre Prozesse mithilfe von IT-Lösungen abzubilden, läuft auf „Hochtouren". Die Kommunikation mit dem Medizinischen Dienst der Krankenversicherung (MDK) verläuft aber oftmals noch klassisch papierbasiert. Das verursacht auf beiden Seiten einen hohen Aufwand: Der MDK schickt seine Prüfanzeige zum Teil per Fax, woraufhin die Klinik ihre elektronischen Unterlagen ausdruckt und an den MDK sendet, wo sie wiederum eingescannt und beurteilt werden. Teilweise werden diese hier dann erneut ausgedruckt. Der Weg über eine CD-ROM ist zwar einfacher, aber nicht sicherer. Zudem führt das beim MDK zu einem speziellen Dilemma, wie Lutz Remshardt, Abteilungsleiter Service/IT beim MDK Nord, ausführt: „Wir bekommen die Unterlagen in einer großen Vielfalt von Medien, etwa auf Papier, CD mit und ohne Passwort, E-Mail oder Telefax, und zwar in verschiedenen Dateiformaten und ohne Indexierung."

Digitalisierung der gesamten Kommunikation

Das Krankenhaus Reinbek St. Adolf-Stift hat klinikweit einen hohen Digitalisierungsgrad erreicht. „Um die Potenziale vollständig auszuschöpfen, wollen wir die Kommunikation mit möglichst allen Beteiligten komplett digitalisieren", sagt Klinikmanagerin Laila Wahle – also auch die mit dem MDK. Hinzu kam, dass dieser das Krankenhaus nicht mehr als Begehungshaus, sondern neu als nach Aktenlage zu prüfen einstufte. „Wir mussten also die benötigten Aktenauszüge in Papierform zur Verfügung stellen, was zu erheblichen Personalmehrkosten führte", so Wahle.

Allerdings stieß sie beim MDK auf offene Ohren für ihr Anliegen, da dem Medizinischen Dienst selbst an einem standardisierten Datenaustausch gelegen ist. „Wir versenden bis

Andreas Kumbroch, Vorstand der Maerz AG

zu 1.500 Prüfanzeigen am Tag, in der Regel per Telefax. Allerdings sehen wir den Datenschutz und die Stabilität im Telefaxversand mit VoIP gefährdet", so Remshardt.

Als Kommunikationsplattform für die bidirektionale Kommunikation fungiert nun die März IHE BOX. IHE steht für Integrating the Healthcare Enterprise und ist ein etablierter Standard im Gesundheitswesen, der den Datenaustausch zwischen IT-Systemen im Gesundheitswesen auf Basis definierter Transaktionsprofile, lieferantenunabhängig ermöglicht. Die März IHE BOX unterstützt diesen Standard, ist entsprechend geprüft und weltweit als IHE-konforme Datenkommunikationsplattform gelistet. Damit kann sie beliebig viele Informationssysteme in den Datenaustausch integrieren.

Erfolgreiche Projektumsetzung mit positiven Erfahrungen

Gestartet haben die drei Partner das gemeinsame Projekt im August 2018. Nach einer dreimonatigen Konzeptionsphase erfolgte die Umsetzung. Seit dem 1. April 2019 kommunizieren Krankenhaus und MDK nun ausschließlich digital. „Beide Seiten konnten ihre Workflows optimieren, wir vor allem, um eine zeitnahe Bearbeitung von Prüffällen innerhalb gesetzlicher Fristen zu gewährleisten. Darüber hinaus konnten wir die lästigen und zeitraubenden Tätigkeiten wie Akten kopieren von unseren Fachkräften entlasten und die freigewordene Arbeitszeit in die Qualitätssicherung investieren.", nennt Wahle die wesentlichen Ziele des Projekts aus Krankenhaussicht. Der MDK möchte die Kommunikation generell auf ein elektronisches Verfahren und möglichst ein Format beschränken, um die Aufwände zu minimieren.

Die ersten Erfahrungen zeigen, dass das auch gelingt. „Wir schicken unsere Prüfanzeigen digital über die neue Plattform an das Krankenhaus Reinbek und bekommen von dort die geforderten Unterlagen in digitaler Form zurück – schnell, einfach, ohne Größenbeschränkung und in Echtzeit. Das reduziert die Bearbeitungszeit und stellt die Vollständigkeit der Dokumente sicher", freut sich Remshardt. „So können wir die Unterlagen direkt in das hauseigene Archivierungssystem übernehmen. Dabei wird automatisch eine Empfangsbestätigung generiert und versendet. Die März IHE BOX gewährleistet eine sichere, Ende-zu-Ende-verschlüsselte Datenübertragung und die Einhaltung aller Datenschutzanforderungen. Beide Seiten sparen sich viel Zeit und Aufwand, weil ein Großteil der Prozesse vollautomatisiert abläuft."

Einsparungen klar bezifferbar

Der neu etablierte Prozess über die März IHE BOX hat aber auch handfeste finanzielle Vorteile, wie Klinikmanagerin Laila Wahle in ihren Vorträgen auf der Dialogtour betonte: „Allein über das Abschmelzen von Rückstellungen nicht entschiedener Prüffälle durch schnellere Prozesse lässt sich ein Großteil der Investitionen für die Lösung refinanzieren." Gemeinsam mit ihrem Team hat sie jeden einzelnen Arbeitsschritt im Rahmen

Laila Wahle, Klinikmanagerin

des gesamten MDK-Prozesses – vom Eingang der Prüfanzeige bis zum Eingang des Gutachtens – minutiös erfasst. Das Ergebnis: Mit der neuen Lösung spart das Krankenhaus Reinbek bei 2.900 Fällen pro Jahr eine ansehnliche fünfstellige Summe und entlastet die Mitarbeiter von monotonen, wenig sinnstiftenden Tätigkeiten.

Die Diskussionen in den verschiedenen Workshops waren lebhaft und zeugten von einem großen Interesse der Teilnehmer an der März IHE BOX. Diese sparten auch nicht mit Anregungen, wie die MDK-Kommunikation mit der Lösung künftig weiter optimiert werden kann. Das durchweg positive Feedback macht auf jeden Fall Lust auf mehr. Darüber hinaus nutzten die Teilnehmer die Möglichkeit, sich mit Lutz Remshardt vom MDK Nord auszutauschen. Der nahm seinerseits die Gelegenheit wahr und informierte über die einheitliche Branchensoftware MDconnect sowie das anstehende MDK ePortal. Einhelliges Lob erntete die Tatsache, dass bei der Entwicklung der März IHE BOX zwei eigentliche „Gegenspieler", das Krankenhaus Reinbek und der MDK Nord, gemeinsam eine gewichtige Rolle gespielt haben. Daraus ist eine Lösung entstanden, die „in der Form einmalig am Markt ist", wie Andreas Kumbroch, Vorstand Software und Vertrieb der März AG, betonte.

Aufgrund des großen Interesses wird die Tour im kommenden Jahr fortgesetzt.

Lutz Remshardt, Abteilungsleiter MDK Nord

Das Behandlungszimmer der Zukunft dokumentiert mit Spracherkennung

Der deutsche Gesetzgeber hat sich die Digitalisierung der Gesundheitsversorgung auf die Fahne geschrieben und deren Umsetzung ist in den Krankenhäusern angekommen. Spracherkennung hilft dort nicht nur heute schon, Prozesse effizienter zu gestalten, sie ist auch eine wichtige Komponente im Behandlungszimmer der Zukunft.

In Deutschland hat die Digitalisierung im Gesundheitswesen deutlich an Fahrt gewonnen. Hierzu beigetragen haben die Initiativen des Bundesministeriums für Gesundheit (BMG), das die „Digitalisierung zur Chefsache" erklärt hat. Insbesondere mit dem aktuell verabschiedeten Digitale-Versorgung-Gesetz (DVG) wurde ein deutliches Signal gesetzt.

Digitalisierung im Gesundheitswesen beginnt mit der Digitalisierung von Prozessen. Dadurch gelingt es, das Personal in einer Klinik – angefangen von Ärzten, Pflegern bis hin zur Verwaltung – zu entlasten. Digitale Spracherkennung stellt dabei eine Option dar, die mittlerweile in gut der Hälfte aller Krankenhäuser in Deutschland eingesetzt wird.

Jede Minute mehr mit dem Patienten ist Gold wert

Eine amerikanische Studie belegt, dass Ärzte für jede Stunde direkten Patientenkontakt, zwei Stunden Verwaltungsaufgaben rund um die elektronische Patientenakte (ePA) erledigen müssen, oft nach Feierabend. Dadurch verkürzt sich die Zeit für ihre eigentliche Aufgabe – die Patientenversorgung.

Angesichts des hohen Dokumentationsaufwands gilt Spracherkennung als optimale Technologie, diese Aufgabe effizienter zu bewältigen – denn wir sprechen circa drei Mal schneller, als wir tippen. Diese direkte Verbesserung ist in Zeiten, in denen viele Ärzte und Pflegende mit Überlastung, Unzufriedenheit und Burn-out kämpfen, ein Gewinn an Lebensqualität. Allein im Jahr 2018 gaben 33 Prozent der deutschen Ärzte an, sich ausgebrannt zu fühlen.

Benjamin Hoch, Facharzt für Gynäkologie und Geburtshilfe am Universitätsklinikum Mannheim, bringt den Nutzen auf den Punkt: „Die Effizienzsteigerung durch die Spracherkennung generiert über den Tagesverlauf hinweg viele Minuten. Jede Minute, die man mehr auf den Patienten eingehen oder seine Fragen beantworten kann, ist Gold wert."

Dabei erzeugt die Digitalisierung nicht nur Mehrwert auf der Versorger-, sondern auch auf der Patientenseite. Beispiels-

weise kann der Einsatz von Spracherkennung bei einer Mammografie die Wartezeit auf Ergebnisse von mehreren Tagen auf unmittelbar nach der Untersuchung senken. Traditionell braucht ein Schreibbüro, bis der schriftliche Befund vorliegt und vom Arzt korrekturgelesen und freigegeben wurde, mehr als drei Tage. Erst dann kann der Arzt ihn mit der Patientin teilen. Durch Verwendung von Spracherkennung entfällt diese lange Wartezeit und erzeugt einen direkten Nutzen für die betroffene Frau, die viel schneller den Befund und damit Klarheit über ihren Gesundheitszustand erhält.

Mehr als die Hälfte der deutschen Krankenhäuser nutzt Spracherkennung

Die Digitalisierung ist in deutschen Krankenhäusern angekommen. Im Bemühen um zeitgemäße Arbeitsmittel hat sich dort auch Spracherkennung verbreitet, die mittlerweile von mehr als jedem zweiten Krankenhaus eingesetzt wird. Auch unter den niedergelassenen Ärzten in der D-A-CH-Region wird sie bereits von jedem siebten genutzt.

Anfangs wurde Spracherkennung vor allem in Fachabteilungen mit hohem Befundaufkommen wie der Radiologie verwendet. Doch übergreifende Strategien, Medienbrüche zu vermeiden, hat dazu geführt, dass sie inzwischen Bestandteil der Digitalisierungsstrategie ist und krankenhausweit zum Einsatz kommt, d. h., nicht nur im medizinischen Bereich sondern auch in Verwaltungs- und Rechtsabteilungen.

Ambient-Technologien – Die Zukunft des Arzt-Patienten Gesprächs

Wie wäre es, wenn sich die Dokumentation von selbst schriebe? Dieses Szenario ist keine Zukunft, sondern wird seit diesem Jahr in US-amerikanischen Krankenhäusern erprobt. Mithilfe der von künstlicher Intelligenz (KI) gesteuerten, sprachgestützten Ambient Sensing-Technologie wird ein Arzt-Patienten Gespräch audiovisuell aufgezeichnet, sofern der Patient dazu einwilligt und entsprechend dem bestehenden Datenschutz. Anschließend werden wichtige Inhalte wie Anamnese oder Medikation extrahiert und mit relevanten Kontextinformationen aus der ePA ergänzt und danach automatisch in dieser dokumentiert. Der Behandler kann zudem die ePA per Sprache navigieren und erhält direkten Zugriff in Echtzeit. Das erlaubt ihm, sich vollständig auf den Patienten zu konzentrieren, was die Zufriedenheit auf beiden Seiten steigert. Die dahinterstehende Technologie wird als „Ambient Clinical Intelligence“ (ACI) bezeichnet.

Im Oktober 2019 haben Nuance und Microsoft ihre Zusammenarbeit auf dem Gebiet von ACI bekannt gegeben. „Die Partnerschaft mit Microsoft hilft uns dabei, dringendste Herausforderungen im Gesundheitswesen gemeinsam schneller zu lösen", so Mark Benjamin, CEO, Nuance. „Die ACI-Technologien, die wir gemeinsam entwickeln, erhöhen die Produktivität und die berufliche Zufriedenheit, während sie es Ärzten ermöglichen, sich auf ihre wichtigste Aufgabe zu konzentrieren: die Betreuung der Patienten." Das bestätigt auch ein Anwender, Dr. James Lindner, CEO, Nebraska Medicine: „Wir sind begeistert von den Ergebnissen, die mit ACI bereits jetzt erzielt werden und es Medizinern ermöglichen, sich mehr auf ihre Patienten zu konzentrieren“.

Gleichzeitig kann diese Technologie um Anwendungen von Drittsystemen erweitert werden. Zum Beispiel mit ICD-10, dem internationalen System zur statistischen Klassifikation von Krankheiten, der medizinischen Kodierung oder klinischen Entscheidungssystemen, um den Behandler noch mehr zu entlasten.

Im deutschsprachigen Raum wartet man schon auf das Behandlungszimmer der Zukunft

Auch in Europa stößt ACI auf positive Resonanz. Eine Schweizer Universitätsklinik äußerte sich anerkennend: „Genau das, was die ACI-Technologie ermöglicht, wollen wir unseren Ärzten als Bestandteil des Arbeitsplatzes der Zukunft bieten.“ In Deutschland wird das Potenzial ebenfalls erkannt. Dr. Lennart Jahnke, Chief Digital Officer am Universitätsklinikum Mannheim berichtet: „Es ist erstaunlich, was bereits heute technisch realisierbar ist. Basierend auf KI werden wir zukünftig digitale Assistenten bekommen, die sprachaktiviert kommunizieren und die Ärztinnen und Ärzte in vielen Bereichen unterstützen werden.“

Jedoch müssen wir uns in Deutschland noch etwas gedulden. Die ePA wird 2021 eingeführt und ACI geht mit der Nutzung von Cloud und Software as a Service (SaaS) Modellen einher, die noch in den Startlöchern stehen. Aber auch hier gibt es Bewegung: Sicherheitsbedenken werden durch DSGVO und die von den Cloudanbietern zu erbringenden Zertifizierungsnachweise entkräftet und transparent dargelegt. Aber auch der Mangel an qualifiziertem IT-Personal wird Gesundheitsinstitutionen veranlassen mit SaaS- und Cloud-Lösungen von Drittanbietern zu arbeiten. Am Ende geht es immer um die Frage: wie kann Digitalisierung die Patientenversorgung spürbar verbessern und für den Bürger greifbar machen, wie z.B. durch Spracherkennung, welche dem Arzt mehr Zeit für seine Patienten gibt.

Martin Eberhart, General Manager DACH
Nuance Communications Healthcare Germany GmbH

Am Puls der medizinischen Zukunft

Das Klinikum Osnabrück vollzieht den digitalen Wandel. Zwei Bausteine dafür bilden die Lösungen E-ConsentPro mobile und E-DocumentPro von Thieme Compliance

„Wir müssen das Thema Digitalisierung aufnehmen und klarer positionieren", ruft die Führungsebene des Klinikums Osnabrück im Januar aus. Eine Vision, der kurz später Taten folgen sollten. In der IT-Abteilung, geführt von CIO Ingo Mette, formiert sich das neue Team „Digitalisierung & Prozessmanagement" unter der Leitung von Carsten Esser. Die Aufgabe der Experten: sich um hausweite Digitalisierungsprojekte zu kümmern, indem sie speziell die Fachprozesse in den Fokus rücken und analysieren, wie digitale Lösungen diese verbessern können. Im Rahmen der vollständigen Digitalisierung einer „Pilot-Klinik" mit zwei Pflegestationen wird aktuell etwa geprüft, inwiefern Teilprozesse im klinischen Alltag mit neuen Lösungen optimiert werden können.

Jens Kollmer, Leiter Application Management und Initiator beim Thema „Digitale Patientenaufklärung", sah mit dem Projektteam in diesem Bereich enormes Verbesserungspotenzial – und recherchierte nach Herstellern mit attraktiven Lösungen. „Da wir die papierbasierten Aufklärungsbögen von Thieme Compliance bereits im Einsatz hatten und gerne ‚aus einer Hand' arbeiten, wollten wir uns unbedingt die digitale Lösung zeigen lassen", erläutert er. „Man stellte uns das Programm E-ConsentPro mobile, das eine ortsunabhängige Patientenaufklärung erlaubt, vor. Technologie, Aufbau und Funktionen überzeugten uns und wir beschlossen, es zu testen."

Elfriede Bönisch, Leitung Patientenservice

Carsten Esser, Leitung Digitalisierung & Prozessmanagement

Optimismus statt Stress

So läuft die Nutzung: Der Patient füllt über die App „Anamnese mobil" die obligatorischen Fragen direkt auf einem Tablet aus. Mit einem Kreuz kann er signalisieren, dass er über ein bestimmtes Thema ausführlicher mit dem Arzt reden möchte. Der Arzt sieht über die App „Aufklärung mobil" den Status sowie die beantworteten und offenen Fragen des Patienten; spezielle Anmerkungen notiert oder zeichnet er in das Dokument ein. Dem Patienten kann er anschauliche Aufklärungsfilme, etwa zur Tumorentfernung oder Bypass-Operation, zeigen. Fühlt sich der Patient hinreichend informiert, unterschreiben Arzt und Patient elektronisch auf dem Tablet. Abschließend wird das Dokument digital archiviert und für den Patienten ausgedruckt – Patientenaufklärung unkompliziert und sicher.

„Wir betrauten einen der Assistenzärzte aus unserem Pilotbereich – der von Chefarzt Privatdozent Dr. Johannes Rey verantworteten inneren Medizinischen Klinik II. Als ‚Key User' testete Assistenzarzt Dr. Jens Rodeck in enger Abstimmung mit dessen Chef die Lösung über mehrere Wochen", schildert Kollmer. Schritt für Schritt erkunden die Mitarbeiter die neuen Möglichkeiten – und finden Gefallen an ihnen; insbesondere die übersichtliche Darstellung und die saubere digitale Aufbewahrung der Unterlagen („Früher ist schnell mal ein Bogen aus dem Fach geflogen") kommen gut an, sodass das Klinikum beschließt, das Produkt ab Herbst einzuführen und mittelfristig weiter auszurollen.

Thomas Kupper, Leitung Patientenmanagement

Gut aufgenommen

„Im Zuge der Digitalisierung haben wir außerdem die großen Aufnahmebereiche des Klinikums analysiert. Auch dort konnten wir Abläufe mit erheblichem Optimierungspotenzial identifizieren. Bis dato druckten wir bei jeder Aufnahme bis zu 12 Papierformulare doppelt aus. Diese Dokumente mussten unterzeichnet, der Akte zugeführt und an andere Stellen im Haus weitergeleitet werden – ein langwieriger, aufwendiger, bürokratischer Prozess. Die neue Lösung E-DocumentPro, die Thieme Compliance erst im April auf der DMEA präsentiert hatte, sollte uns in diesem Fall weiterhelfen", erzählt Esser. Das Prinzip dahinter: Thieme bindet die klinikindividuellen Dokumente wie Behandlungsverträge, Wahlleistungsvereinbarungen oder Datenschutzvereinbarungen in die App E-DocumentPro ein, sodass die Aufnahmekraft und der Patient die jeweils bei der Aufnahme benötigten, mit Checkboxen und Freitextfeldern versehenen Formulare gemeinsam auf dem Tablet ausfüllen können; Patient und Aufnahmekraft unterschreiben biometrisch, bevor das generierte PDF/A-Dokument revisionssicher archiviert wird.

Basis beider Lösungen ist die Software E-ConsentPro, die den Zugriff auf die Aufklärungsbögen und die hauseigenen Dokumente ermöglicht. Im Rahmen eines „Pilottages" durften die Mitarbeiter die Features inspizieren, ausprobieren und persönliche Wünsche äußern. Individuelle Inhalte stimmte man mit Thieme Compliance ab, etwa vordefinierte Bogenpakete für verschiedene Patientengruppen. In den Wochen bis zur geplanten Einführung habe man online, telefonisch und vor Ort intensiv zusammengearbeitet, um technische und anwendungsspezifische Detailfragen zu klären. „Wir haben unser Personal eng geschult, versucht, die Stimmung einzufangen und regelmäßiges Feedback einzuholen – uns dem Thema sensibel zu nähern, war uns sehr wichtig", betont Esser. „Vereinzelte Berührungsängste schwanden; jeder Mitarbeiter erkannte und schätzte schlussendlich die etlichen Erleichterungen. Im Juli gaben wir den offiziellen Startschuss für das Programm."

Elfriede Bönisch, Leitung des Patientenservice im Klinikum, ist eine der Mitarbeiterinnen, die die Patienten mittlerweile digital aufnehmen. Sie freut sich, technologisch unterstützt zu werden: „Das neue Verfahren vereinfacht unsere Arbeit kolossal. Wir sparen Papier und Toner, müssen Formulare nicht mehr mit Etiketten bekleben, auf denen die Patientendaten stehen, oder sie scannen", berichtet sie. Thomas Kupper, der das Patientenmanagement verantwortet, konkretisiert, man spare bis zu acht Minuten pro Aufnahme – das sei bei 33.000 stationären Patienten im Jahr ein gewaltiger Fortschritt. „Wir haben den gesamten Prozess der administrativen Patientenaufnahme bis ins kleinste Detail analysiert und visualisiert, mit dem Ziel, ihn mithilfe einer digitalen Lösung sowohl patienten- als auch mitarbeiterorientiert zu optimieren. E-DocumentPro erfüllt diese Anforderungen hervorragend", so Kupper und Esser.

Sowohl für die Mitarbeiter als auch für die Patienten sei die App laut Bönisch leicht zu handhaben: „Hat man die Schritte einmal gesehen, versteht man sie." Ihre Befürchtung, ältere Patienten scheuten sich vor dem modernen Hilfsmittel, hätten sich als falsch erwiesen: „Auch mit dem digitalen Stift kommen alle gut zurecht." Ist trotzdem jemand mit der Technik überfordert, könne er nach wie vor analog aufgenommen werden. Das Klinikum Osnabrück ist eines der ersten Krankenhäuser, die mit der neuen Lösung von Thieme Compliance die administrative Patientenaufnahme digitalisiert haben – ein Eckpfeiler auf dem Weg zur „elektronischen Patientenakte", die 2021 flächendeckend im Gesundheitswesen eingeführt wird.

Jens Kollmer, Leitung Application Management

Eine Gesamtlösung für Software und Services in der klinischen IT

Philips IntelliSpace Enterprise Edition

Die IT ist einer der wichtigsten Erfolgsfaktoren im hart umkämpften Gesundheitsmarkt. Sie trägt maßgeblich zur Optimierung der Prozesse in der Leistungserbringung und damit zur Steigerung der Versorgungsqualität und Effizienz bei. Die Kontinuität und Verfügbarkeit einer starken informationstechnischen Infrastruktur wird folglich über die Zukunftsfähigkeit von Krankenhäusern mitentscheiden. Umso wichtiger ist es deshalb, sich strategisch mit IT-Themen auseinanderzusetzen. Doch die Realität sieht anders aus. In einer aktuellen Studie gaben ein Drittel der Befragten an, dass die IT-Strategie nicht an der Strategie des Hauses ausgerichtet sei oder sogar ganz fehle. CIOs sind überwiegend operativ tätig und nutzen nur ein Viertel ihrer Zeit für strategische Analysen und Konzepte.[1] Mit IntelliSpace Enterprise Edition (ISEE) hat Philips nun ein Programm entwickelt, das von Routineaufgaben entlastet, indem es eine Vielzahl bislang nebeneinander bestehender Insellösungen in einer integrierten Systemservice-Landschaft zusammenführt. CIOs können dadurch Freiräume gewinnen, um die digitale Transformation ihres Krankenhauses weiter voranzutreiben.

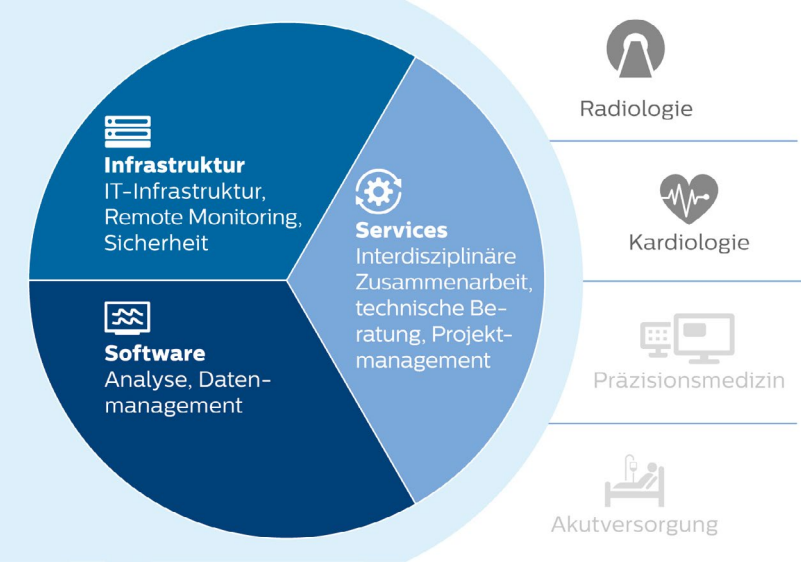
Konsolidieren heißt Komplexität reduzieren

„Mit IntelliSpace Enterprise Edition unterstützen wir unsere Kunden als verlässlicher Partner, sich in Sachen IT auf das Wesentliche zu fokussieren", erklärt Christian Neumann, Business Manager ISEE, Philips GmbH Market DACH (Deutschland, Österreich und Schweiz). „Die Plattform kombiniert innovative Softwarelösungen mit einem umfassenden Managed-Service-IT-Angebot. Die Krankenhäuser profitieren von klinischen Systemen mit hoher Leistungsfähigkeit, niedrigen Initialkosten und garantierter Verfügbarkeit." ISEE funktioniert nach dem Prinzip „Eins für alles": Es gibt einen einzigen Vertrag für sämtliche IT-Lösungen. Unter einer einheitlichen Support Nummer erhalten die Kunde Hilfe bei allen Belangen. Ein fester Ansprechpartner koordiniert sowohl die applikatorische als auch die technische Betreuung und initiiert notwendige Systemanpassungen.

Eine maßgeschneiderte Plattform, die mitwächst

IntelliSpace Enterprise Edition lässt sich entsprechend den spezifischen Anforderungen des Kunden individuell konfigurieren. Da Anforderungen sich im Laufe der Zeit ändern können, ist ISEE als skalierbare Plattform konzipiert, sodass Ressourcenengpässe gar nicht erst entstehen.

Auf der Grundlage umfangreicher Bedarfsanalysen und kontinuierlicher Beratung über die gesamte Laufzeit der Partnerschaft hilft Philips Krankenhäusern, eine optimale, bedarfsgerechte IT-Architektur zu erreichen und langfristig zu halten. Um die hochsensiblen Patientendaten vor Hackerangriffen zu schützen – fast zwei Drittel der deutschen Krankenhäuser wurden schon einmal Opfer von Cyberkriminalität[2] – bietet ISEE State of the Art-Datensicherheit inklusive Remote Monitoring, zentralem OS Patching, Antivirus-Management sowie zentralem Backup- und Recovery Management. Dank des Pay-per-Study-Modells entstehen keine hohen Anschaffungskosten. Der Kunde zahlt nur für die tatsächliche Nutzung des Systems.



Philips IntelliSpace Enterprise Edition unterstützt Krankenhäuser dabei, eine skalierbare, bedarfsgerechte IT-Architektur zu entwickeln und langfristig zu betreiben.

„Mit weniger mehr tun"

In den USA ist die Plattform bereits in mehreren klinischen Einrichtungen installiert und bewährt sich im klinischen Alltag. „Philips IntelliSpace Enterprise Edition ermöglicht es, mehr mit weniger zu tun. Unsere Experten verbringen weniger Zeit mit Papierkram oder Computerarbeit. Wir können uns mehr auf die Patientenversorgung und auf die Befundung konzentrieren. Und wir versorgen unsere Kardiologen und Radiologen mit qualitativ hochwertigen Daten", sagt Donna Russell, Leiterin radiologische und kardiologische Bildgebung, CarolinaEast Health System in New Bern, North Carolina.

Auf dem deutschen Markt ist ISEE in einer ersten Version verfügbar.

Philips GmbH Market DACH
Tel.: +49 40 2899-0
healthcare.deutschland@philips.com
www.philips.de/healthcare

[1] Deloitte: IT im Krankenhaus. Zwischen neuen Herausforderungen und Chancen. 2018
[2] Roland Berger Krankenhausstudie 2017

IT Sicherheit im Krankenhaus

Journal für Strategie und Praxis

IT-Sicherheit: Das „smarte“ Krankenhaus richtig absichern

Die Digitalisierung bietet der Gesundheitsbranche enorme Chancen. Damit sensible Daten sicher vor Missbrauch sind und es nicht zu Störungen der Abläufe kommt, sind im „smarten“ Krankenhaus aber auch neue IT-Sicherheitskonzepte und der Einsatz innovativer IT-Sicherheitslösungen erforderlich. Auch deshalb, weil sich Krankenhäuser jetzt auf das neue IT-Sicherheitsgesetz vorbereiten sollten, das verschärfte Regularien für KRITIS vorsieht.

Die Digitalisierung ist in der Gesundheitsbranche auf dem Vormarsch: Patienten können zum Beispiel Rechnungen für die Krankenkasse bequem in Apps hochladen oder Termine über die Webseiten von Ärzten vereinbaren. Vernetzte medizinische Geräte vereinfachen die Zusammenarbeit von Ärzten. Gesundheitsminister Jens Spahn möchte ab 2021 sogar eine digitale Patientenakte einführen, die Patientendaten gebündelt bereitstellt. Das Ziel: Doppeluntersuchungen vermeiden oder Unverträglichkeiten bei Arzneimitteln besser beachten. Das soll auch das Vertrauen der Patienten steigern.

Keine Seltenheit: Angriffe auf den Gesundheitssektor

Das „smarte Krankenhaus“ wird allerdings zunehmend attraktiver für kriminelle Hacker. Eine Studie der Roland-Berger-Stiftung ermittelte, dass 2017 bereits 64 Prozent aller Kliniken in Deutschland Opfer eines Cyberangriffs waren. Krankenhäuser sind gegen Angriffe jedoch häufig nicht ausreichend geschützt. Der Grund: Viele Kliniken stehen unter enormem Finanzdruck. Hinzu kommt, dass vor allem der zunehmende Einsatz sogenannter Webapplikationen neue Angriffsmöglichkeiten für Hacker bietet. Solche Anwendungen, die über den Browser zugänglich sind, machen die Zusammenarbeit in der Gesundheitsbranche erheblich flexibler und verbessern dadurch auch die Leistungen für den Patienten. Medizinische Unterlagen und Berichte lassen sich beispielsweise digital für jede berechtigte Person zugänglich machen – und zwar sowohl vom PC als auch von Tablet, Smartphone oder anderen vernetzten Geräten. Das Vertrauen der Patienten wird durch diese Anfälligkeit der Krankenhäuser jedoch erheblich geschwächt.

Das Problem: Webanwendungen sind für Hacker leicht zu knacken. Denn das Web, speziell das Protokoll HTTP und auch das etwas sicherere HTTPS, wurde nicht für die heute üblichen komplexen Anwendungen konzipiert. Schwachstellen lassen sich bei der Entwicklung kaum vermeiden. Vor allem sehr komplexe Anwendungen sind anfällig für Sicherheitslücken.

Cyberkriminelle nutzen dies gnadenlos aus. Datenbanken zählen dabei zu den beliebtesten Angriffszielen von Hackern. Denn sie halten riesige Mengen von persönlichen Daten in konzentrierter Form bereit. Bei der Speicherung in Cloud-Diensten kommt hinzu, dass nicht nur Benutzer und Administratoren Zugriff auf die Daten haben. Auch Cloud-Provider könnten sich Zugriff verschaffen, wenn Daten ungeschützt und unverschlüsselt abliegen. Finden Cyberkriminelle einen Zugang zu diesen Daten, lassen sich damit Patienten und Krankenhäuser erpressen.

Mangelnde IT-Sicherheit trotz gesetzlicher Auflagen

Dabei ist der Schutz von gesundheitsbezogenen Daten streng geregelt: Diese unterliegen der EU-weiten Datenschutz-Grundverordnung (EU-DSGVO). Zusätzlich gibt das „E-Health-Gesetz" einen konkreten Fahrplan für den Aufbau einer sicheren Telematik-Infrastruktur und die Einführung digitaler medizinischer Anwendungen vor. Im Falle von Datenverlusten oder Verstößen drohen erhebliche Sanktionen. Ergänzend gilt für größere Kliniken mit mindestens 30.000 vollstationären Fällen pro Jahr die „Verordnung zur Bestimmung kritischer Infrastrukturen (KRITIS)" des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Diese Kliniken müssen seit Juli 2019 ein Mindestniveau an Informationssicherheit nachweisen. Doch auch für kleinere Häuser empfehlen sich diese Vorgaben als Leitfaden für mehr Versorgungssicherheit. Insbesondere auch deshalb, weil sie schon bald unter die KRITIS-Richtlinien fallen könnten. Für das IT-Sicherheitsgesetz 2.0 ist geplant, den derzeitigen Schwellenwert von 30.000 abzusenken. Dann besteht in den betroffenen Kliniken akuter Handlungsbedarf.

Neben rechtlichen und wirtschaftlichen Konsequenzen kann ein erfolgreicher Angriff auch zu einem beträchtlichen Imageschaden und Vertrauensverlust bei den Patienten führen. Das ist aber nicht alles: Bricht im schlimmsten Fall die gesamte gesundheitliche Versorgung durch einen Cyberangriff zusammen, bedroht das unsere ganze Gesellschaft.

Um diese Szenarien zu verhindern, ist ein geeignetes IT-Sicherheitskonzept für Gesundheitseinrichtungen entscheidend. Zunächst müssen IT-Spezialisten prüfen, ob die Daten gut abgesichert sind und an welcher Stelle nachgebessert werden muss. Auf dieser Grundlage können Gesundheitseinrichtungen konkret handeln und individuell geeignete Sicherheitstechnologien anschaffen. Diese Technologien sollten von vertrauenswürdigen Herstellern kommen, die BSI-zertifizierte Lösungen anbieten können. Der IT-Sicherheitsspezialist setzt bei seinen Produkten auf neue Sicherheitsansätze, mit denen sich auch Angriffe stoppen lassen, gegen die herkömmliche Lösungen machtlos sind. Dies sind einige Beispiele:

Webanwendungen absichern: Um Webapplikationen zu schützen, brauchen Krankenhäuser eine „Web Application Firewall": Die Web Application Firewall verhindert, dass Webanwendungen zum Einfallstor für Schadsoftware werden, indem sie den Datenaustausch zwischen Endgeräten und Webservern analysiert. Sie prüft alle eingehenden Anfragen an den Webserver sowie dessen Antworten. Sobald bestimmte Inhalte als verdächtig eingestuft werden, verhindert die Web Application Firewall den Zugriff.

Daten in der Cloud schützen: IT-Sicherheitslösungen für die Cloud müssen in der Lage sein, die Daten unabhängig von ihrem Speicherort vor dem Zugriff Dritter zu schützen. Technisch umsetzen lässt sich das mit einem datenzentrischen Sicherheitsansatz: Dabei werden die Daten verschlüsselt, fragmentiert und regulatorisch konform gespeichert. Daten, die Europa nicht verlassen dürfen, werden konfigurierbar z.B. in einem europäischen Rechenzentrum abgelegt, obwohl sie virtualisiert in der Cloud vorliegen. Egal, wo ein Angreifer Zugriff erlangt: Er kann keinen großen Schaden mehr anrichten. Diese Art der Speicherung ist nicht nur besonders sicher, sie entspricht auch den strengen Datenschutz- und Sicherheitsvorgaben der EU-DSGVO.

Übertragungswege absichern: Zu einer IT-Sicherheitsstrategie im Gesundheitswesen gehört auch die Absicherung der Übertragungswege – sei es zwischen einem Gerät im Krankenhaus und dem Hausarzt eines Patienten oder dem Krankenhaus und einem Rechenzentrum. Die Herausforderung: Die Übertragung muss trotz hochsicherer Verschlüsselung effizient bleiben. Dazu gibt es spezielle Verschlüsselungsprodukte, die einen hohen Schutz bieten, ohne dass die Übertragungsleistung herabgesetzt wird.

Angriffe aus dem Internet abwehren: Da 70 Prozent der Malware über den Browser in das Netzwerk kommen, ist es ein wichtiger Schritt für Krankenhäuser, Angriffe aus dem Internet abzuwehren. Am gezieltesten ist das möglich mit einem virtualisierten Browser. Dieser ist von allen anderen Anwendungen und sensitiven Daten auf dem PC hermetisch getrennt. Eine Malware-Attacke läuft ins Leere, weil sie im Browser eingesperrt bleibt und keinen Zugriff auf das PC-Betriebssystem bekommt.

Mit diesen Maßnahmen erfüllen Gesundheitseinrichtungen nicht nur wichtige Regularien und Vorschriften – sie bilden auch die Grundlage für weitere digitale Entwicklungen. Denn nur mithilfe einer effizienten IT-Sicherheit können IT-basierte Prozesse eingesetzt werden, ohne dass dabei die Datensicherheit auf dem Spiel steht. Das wiederum wirkt sich auch positiv auf das Vertrauen der Patienten in das „smarte" Krankenhaus der Zukunft aus.

Dr. Falk Herrmann, CEO bei Rohde & Schwarz Cybersecurity *(www.rohde-schwarz.com/cybersecurity)*

Deepfakes heben Social-Engineering-Angriffe auf neue Gefahrenstufe

Social-Engineering-Angriffe stellen eine hohe Gefahr für die IT-Sicherheit dar, weil sie technische Abwehrmaßnahmen umgehen. Noch problematischer wird die Bedrohungslage durch KI- und ML-basierte Deepfakes, die stark im Kommen sind. Unternehmen müssen ein Bewusstsein für diese Gefahren entwickeln und Führungskräfte wie Mitarbeiter entsprechend sensibilisieren.

Auch eine ausgefeilte IT-Security-Strategie schützt nicht unbedingt vor Social-Engineering-Angriffen. Wenn Angreifer durch cleveres Social-Engineering oder -Hacking, also durch „soziale Manipulation" der Mitarbeiter, Zugang zu unternehmenskritischen Systemen und Daten wie Domain-Controllern oder Passwörtern erlangen, sind die besten technischen Sicherheitsvorkehrungen in der Regel nutzlos.

Mit Abstand am häufigsten treten im Social Engineering Betrugsversuche mit Phishing-Mails auf, beliebt bei Hackern ist vor allem der gezielte Angriff auf wenige Personen per E-Mail, also das sogenannte Spear-Phishing. Aber auch die Gefahr des Vishings, das heißt von Phishing-Angriffen via Telefon, sollte nicht unterschätzt werden. Nicht zuletzt gibt es immer wieder Fälle, in denen Angreifer physischen Zugang zu einem Werksgelände und Firmenbüros erlangen.

Solange es keine 100-prozentige technische Absicherung gegen solche Social-Engineering-Methoden gibt, wird keiner dieser Angriffe wirklich veralten. Leider sind sich viele Personen der Gefahr – selbst trotz zahlreicher Awareness-Kampagnen – nicht ausreichend bewusst. Noch komplexer wird die Sache allerdings hinsichtlich neu hinzukommender Methoden des Social-Engineerings. Und dabei sind vor allem Deepfakes stark zu beachten.

Als Deepfakes, abgeleitet aus den Begriffen Deep Learning und Fake, werden manipulierte Medieninhalte wie Bilder, Videos oder Audio-Files bezeichnet. Die dahinterstehenden Technologien wie Künstliche Intelligenz (KI) und Machine-Learning (ML)-Algorithmen haben sich in letzter Zeit rasant weiterentwickelt, sodass aktuell vielfach kaum mehr Original von Fälschung zu unterscheiden ist.

In größerem Umfang tauchten Deepfake-Videos erstmals 2017 auf; das Netz fluteten vor allem gefälschte Porno-Videos mit Hollywoodstars wie Scarlett Johansson und Emma Watson. Große Bekanntheit erlangten zudem die zahlreichen Deepfakes mit Nicolas Cage, in dem der Oscar-Preisträger nahezu in jedem Hollywoodstreifen zu sehen war, etwa als Indiana Jones oder als Forrest Gump. Und auch Politiker wurden von Deepfakes nicht verschont, etwa Angela Merkel, die in einer Rede plötzlich die Gesichtszüge von Donald Trump annimmt, oder Barack Obama, der in einem Fake-Video sagt: „President Trump is a total and complete dipshit."

Die Deepfake-Gefahr für Unternehmen

Deepfakes von Prominenten und Politikern sind bisher die bekanntesten Beispiele, aber auch die versuchte Schädigung von Unternehmen wird nicht lange auf sich warten lassen. Das mögliche Angriffsszenario reicht von der Übernahme von Identitäten bis zur Erpressung von Unternehmen.
Nach Einschätzung von NTT Security sind vor allem die folgenden drei Deepfake-basierten Angriffsvarianten zu beachten:

■ C-Level-Fraud

Beim C-Level-Fraud versuchen die Betrüger nicht mehr, einen Mitarbeiter einer Firma mit einer fingierten E-Mail davon zu überzeugen, zum Beispiel Geld zu überweisen, sondern durch einen Anruf, bei dem der Anrufende sich genauso wie der CFO oder CEO anhört.

■ Erpressung von Unternehmen oder Einzelpersonen

Mit der Deepfake-Technologie können Gesichter und Stimmen in Mediendateien übertragen werden, die Personen dabei zeigen, wie sie fingierte Aussagen treffen. Beispielsweise könnte ein Video mit einem CEO erstellt werden, der bekannt gibt, dass ein Unternehmen alle Kundendaten verloren hat oder dass das Unternehmen kurz vor der Insolvenz steht. Mit der Drohung, das Video an Presseagenturen zu schicken oder es in sozialen Netzwerken zu posten, könnte ein Angreifer dann eine Firma erpressen.

■ Manipulation von Authentisierungsverfahren

Die Deepfake-Technologie kann auch genutzt werden, um kamerabasierte Authentisierungsmechanismen zu umgehen, etwa die Legitimationsprüfung über Postident.

Prinzipiell können aber alle Attacken, bei denen sich Angreifer zum Beispiel am Telefon, per E-Mail oder Videobotschaft als eine andere Person ausgeben, durch die Deepfake-Technologie erweitert und wesentlich schwerer erkennbar werden. Dadurch ist es durchaus denkbar, dass Deepfakes auch für Angriffe auf Privatpersonen genutzt werden, etwa für den Enkeltrick-Betrug. Ein vermeintlicher Enkel könnte per Video Kontakt mit seinen Großeltern aufnehmen und diese um finanzielle Unterstützung bitten – etwa für das Studium oder eine Reise.

NTT Security sieht die Gefahr, dass Deepfakes künftig deutlich an Bedeutung gewinnen werden, da die dabei eingesetzten Machine-Learning-Methoden weiter optimiert werden und auch die Realisierung von Deepfakes keine zeit- und kostenaufwendige Herausforderung mehr darstellt. So können etwa Video-Deepfakes mit im Internet frei verfügbaren Tools wie der Software FakeApp und überschaubaren technischen Kosten erstellt werden. Benötigt werden lediglich eine Webcam für rund 80 Euro, ein Greenscreen für rund 90 Euro und eine Grafikkarte für rund 1.000 Euro. Auch ein Audio-Deepfake ist inzwischen einfach zu realisieren. In der Vergangenheit musste ein Modell noch anhand von Sprachdaten mit mindestens fünf Stunden Länge erstellt werden. Heute gibt es öffentlich verfügbare Tools wie Lyrebird, die das Synthetisieren von neuen Stimmen auf Basis eines vorhandenen Modells mit nur einer Minute an Audiomaterial ermöglichen.

Die Bedeutung von Security-Awareness-Trainings

Nach Einschätzung von NTT Security kennen die meisten Unternehmen die konkreten Deepfake-Bedrohungen noch nicht, da es sich um völlig neue Angriffsformen handelt. Der erste Schritt muss also sein, ein Bewusstsein im Unternehmen zu schaffen, dass solche Attacken möglich sind. Es bedeutet auch, sich von jahrzehntelang vertrauten Wahrheiten zu verabschieden. Bislang galt zum Beispiel am Telefon, dass sich am anderen Ende der Leitung auch diejenige Person befindet, der diese Stimme gehört. Nur wenn jemand weiß, dass dies unter Umständen nicht mehr zutrifft, kann er auch möglichen Angriffen aus dem Weg gehen.

Da die technischen Möglichkeiten zum Schutz von Unternehmen und Personen vor Social-Engineering-Angriffen im Allgemeinen und Deepfakes im Besonderen limitiert sind, kommt dem sicherheitsbewussten Verhalten jedes einzelnen Mitarbeiters eine entscheidende Rolle zu. Folglich sind adäquate Security-Awareness-Trainings unverzichtbar. Wichtig ist dabei, dass firmenspezifische Schulungen durchgeführt werden, in denen individuell auf mögliche Social-Engineering-Angriffe auf das jeweilige Unternehmen eingegangen wird. Die weit verbreiteten generischen Awareness-Trainings hingegen werden von den Mitarbeitern in der Regel als lästige Pflichtveranstaltung angesehen und erzielen folglich auch nicht den gewünschten Erfolg. Durch die Vorstellung konkreter – und nicht allgemeingültiger – sicherheitsrelevanter Fälle aus dem Unternehmen entsteht eine deutlich bessere Identifikationsmöglichkeit für alle Mitarbeiter.

Eventuell sollte ein Unternehmen auch ein Profiling aus Sicht eines potenziellen Angreifers in Betracht ziehen. Dabei wird analysiert, welche Informationen ein Angreifer über ein Unternehmen und die Mitarbeiter erlangen kann, beispielsweise über Suchmaschinen und in sozialen Netzwerken. Daraus kann dann ein Risikoprofil erstellt und ermittelt werden, welche Mitarbeiter am ehesten für einen Social-Engineering-Angriff ausgesucht werden. Auf dieser Basis können individuelle Awareness-Trainingsmaßnahmen konzipiert werden, die auf den jeweiligen Mitarbeiter zugeschnitten sind.

Die Durchführung von Security-Awareness-Trainings ist ein erster Schritt. Allerdings sollten Unternehmen auch die weitere Entwicklung technischer Abwehrmaßnahmen gegen Social-Engineering-Angriffe im Auge behalten. So wird gegenwärtig beispielsweise auch an Applikationen zur Erkennung von Deepfakes gearbeitet und NTT Security kooperiert in diesem Bereich bereits mit allen relevanten Herstellern.

David Wollmann ist Executive Consultant bei NTT Security *(Quelle: NTT Security)*

Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus

Mit dem „Branchenspezifischen Sicherheitsstandard für Krankenhäuser" (B3S), der im Oktober erst die Prüfung durch das Bundesamt für Sicherheit in der Informationstechnik bestanden hat, können die Kliniken jetzt die Anforderungen des IT-Sicherheitsgesetzes für sogenannte "Kritische Infrastrukturen" aus dem Kliniksektor umsetzen. Das Krankenhaus-IT Journal sprach mit Markus Holzbrecher-Morys, Deutsche Krankenhausgesellschaft e. V., Stellvertretender Geschäftsführer (IT, Datenaustausch und eHealth).

Der branchenspezifische Sicherheitsstandard ist eine wichtige Basis für die Sicherheit in Krankenhäusern. Wie kann er den KRITIS-Betreibern aus dem Kliniksektor helfen?

Markus Holzbrecher-Morys: Der Branchenspezifische Sicherheitsstandard (B3S) definiert Anforderungen und Maßnahmen, die der Verbesserung der Informationssicherheit in den Krankenhäusern dienen. Der B3S umfasst dabei sowohl technische als auch organisatorische Maßnahmen in allen Bereichen, in denen die Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität von Informationen für die Patientenversorgung gewährleistet werden muss. Von der Aufnahme bis zur Entlassung der Patienten müssen die Prozesse und Systeme betrachtet werden, die für die vollstationäre Versorgung benötigt werden. Dies betrifft die Informationstechnik, Kommunikations- und Versorgungstechnik bis hin zur Medizintechnik, konkret z.B. das Krankenhausinformationssystem oder auch Rufanlagen, Schließsysteme und Klimatechnik. IT-basierte Prozessunterstützungen können helfen, bei ohnehin knappen Ressourcen den weiter steigenden Anforderungen an die Organisation und Dokumentation des Behandlungsablaufs gerecht zu werden. Mit der zunehmenden Digitalisierung des Behandlungsgeschehens wächst jedoch gleichzeitig die Abhängigkeit von digitalen Informationen. Stehen diese nicht inhaltlich korrekt, nachprüfbar und rechtzeitig zur Verfügung, kann es zu Beeinträchtigungen im Behandlungsverlauf kommen. Betreiber kritischer Infrastrukturen sind nach BSI-Gesetz verpflichtet, geeignete Maßnahmen zur Vermeidung eben jener Beeinträchtigungen oder Ausfälle umzusetzen. Der B3S benennt in insgesamt 168 Einzelanforderungen diejenigen Maßnahmen, die nach intensiver Beratung in den hierfür zuständigen Gremien der DKG sowie dem Branchenarbeitskreis „Medizinische Versorgung" im UP KRITIS als geeignet und angemessen gelten können, um die Informationssicherheit in den Krankenhäusern zu gewährleisten. Das Bundesamt für Sicherheit in der Informationstechnik war bereits während der Erstellung des B3S eng in die Abstimmungen eingebunden und hat zwischenzeitlich die Eignung des B3S zur Umsetzung der Maßnahmen nach § 8a BSIG festgestellt. Damit besteht für Krankenhäuser, die als kritische Infrastruktur im Sinne des BSIG gelten, die Sicherheit, mit der Umsetzung des B3S auch den gesetzlichen Anforderungen zu genügen. Allerdings darf der B3S nicht als simple „Checkliste" missverstanden werden. Wenngleich einzelne Maßnahmen, z.B. zur Frage der Zulässigkeit und Absicherung privater Geräte im Krankenhausumfeld („BYOD"), sehr konkret formuliert sind, wird an anderer Stelle mit einem teils höheren Abstraktionsgrad eine Anforderung formuliert, deren Umsetzung im konkreten Fall durch unterschiedliche Maßnahmen realisiert werden kann. Die Heterogenität der eingesetzten Systeme, die unterschiedlichen organisatorischen, rechtlichen, regionalen und nicht zuletzt finanziellen und personellen Rahmenbedingungen der Krankenhäuser bedingen unterschiedliche Lösungsansätze, die einem gemeinsamen Ziel folgen. Bei der Formulierung der Maßnahmen wurde daher nach dem Muster verfahren: „So konkret wie möglich, so abstrakt wie nötig."

Welchen Herausforderungen müssen sich die Krankenhäuser konkret stellen? Welche Handlungsempfehlung können Sie geben?

Markus Holzbrecher-Morys: Schon bisher bestehen für Krankenhäuser im Bereich Datenschutz hohe Anforderungen. Infolge der weltweiten Zunahme von Cyberangriffen verschärft sich diese Situation. Zwar sind den Behörden bis heute keine gezielten Angriffe auf Krankenhäuser in Deutschland bekannt, als „Beifang" sind sie jedoch regelmäßig von Angriffen durch verbreitete Malware, wie Emotet, Trickbot etc. betroffen. Hier kommt es zunächst darauf an, durch schnell umsetzbare Sicherheitsvorkehrungen und Sensibilisierung der Mitarbeiter die vielzitierte „Resilienz", also Widerstandsfähigkeit, gegenüber diesen Bedrohungen zu erhöhen. Solche „Quick Wins" können kein umfangreiches Sicherheitskonzept ersetzen. Sie können jedoch dabei helfen, den immer perfideren Angriffswerkzeugen von Cyberkriminellen eine erste „organisatorische Firewall" entgegenzustellen. Perspektivisch sind die Einführung eines Informationssicherheitsmanagementsystems sowie die organisatorische und personelle Abbildung dieser Aufgaben im Krankenhaus (z.B. durch die Benennung eines Informationssicherheitsbeauftragten) unumgänglich

Markus Holzbrecher-Morys, Deutsche Krankenhausgesellschaft e. V., Stellvertretender Geschäftsführer (IT, Datenaustausch und eHealth).

IT Sicherheit im Krankenhaus im Layer 1 aus Sicht des OSI-Modells

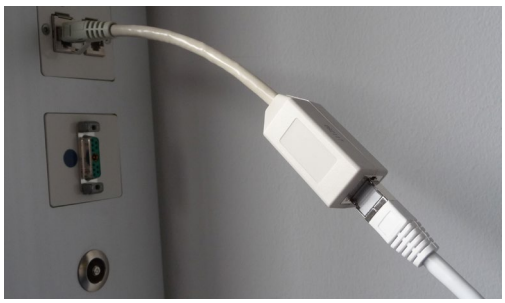
In den Krankenhäusern hat die IT Sicherheit die höchste Priorität. Die IT Sicherheit beginnt aber, wie man nicht unbedingt im ersten Moment vermutet, schon im Layer 1 des OSI-Schichtenmodells. Wer kennt nicht die Situation, dass am Patientenbett teures, elektronisches IT Equipment wie Tablet oder IP Telefon auf beweglichen Tischen zur Verfügung steht.

Diese Nachttische sind in der Regel durch ein RJ45 Kabel mit der entsprechenden Datendose in der Medienleiste verbunden, um Tablet und IP Telefon mit Power over Ethernet und Daten zu versorgen.

Viele Patienten sind aufgrund ihrer Krankheit nicht immer in der Lage, ihre Bewegungen entsprechend gut zu kontrollieren.

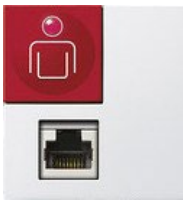
Sie bewegen den Nachttisch in unterschiedliche Richtungen, so dass Zug auf dem Datenkabel entsteht und die Datendose beschädigt werden kann.

Das hat zur Folge, dass der Datentransfer unterbrochen ist und weder Tablet noch IP Telefon funktionieren.



Um diesem Defekt vorzubeugen wurde der RJ45 Abwurfadapter entwickelt. Eine kosteneffiziente Lösung, um dieser Problematik vorzubeugen.

Sobald Zug auf dem Datenkabel oder direkt auf der Datendose entsteht, löst sich die Verbindung und das RJ45 Kabel sowie die Datendose werden nicht beschädigt.



Auch die Schwesternrufanlagen in Kliniken werden immer häufiger mit diesem IT Sicherheitssystem ausgestattet.

In diesem Einsatzszenario wird der RJ45 Abwurfadapter analog zu den Patienten Nachtischen eingesetzt, um das „Ausreißen" des Datenkabels oder der Datendose zu verhindern.

Durch den RJ45 Abwurfadapter der RED EAGLE IT Distribution löst sich die Verbindung zwischen Datenkabel und RJ45 Stecker, sobald der „Zug" zu stark wird. Trotzdem ist bei Nichtbelastung die Verbindung stabil und stört weder den Datentransfer noch die Funktion.

Zugentlastung ist das Geheimnis der IT Sicherheit im Layer1 des OSI-Schichtenmodells.

Kleiner Adapter, große Wirkung, hohe Sicherheit, extreme Kosteneffizienz

Technische Daten:

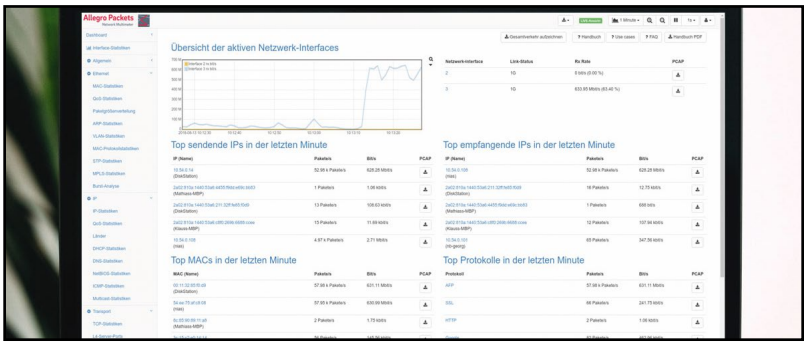
Item	Value
Transmission Performance	Meets all the channel requirements specified for ISO 11801 Class EA
Electrical Insulation Resistance	500 MΩ @100 V d.c
Dielectric Performance	1000V d.c for I minute
Insertions	750 Cycles Minimum
Pull force of Jack	20N +15/-10N
Jack Assembly Material	Fully Screened Zinc Alloy
Contacts	Phosphor Bronze Alloy with 50 micro-inch Gold plating
Cable	Category 6_A F/UTP with LSOH outer sheath.
Cover Material (Plug and Jack)	High impact flame retardant plastic
Plug Assembly	Polycarbonate body with the contacts being plated with 50 micro-inches of hard Gold

Für weitere Produktinformationen, Datenblätter, Preisinformationen, Referenzen können sie sich an RED EAGLE wenden:

RED EAGLE IT Distribution GmbH, Hans-Pinsel-Straße 9a, 85540 Haar bei München,
Telefon: +49 89 122 28 39 30

it-sa 2019-Rückblick: Neue Netzwerkanalyse-Lösungen begeistern Anwender

Die „Home of IT Security“ 2019 schließt mit Rekordergebnis ab. Eine positive Bilanz zieht auch die Allegro Packets GmbH, die dort ihre intelligenten Troubleshooting-Lösungen für Systemadministratoren präsentierte. Dieses Jahr hatte der Spezialist für Netzwerkanalyse das neue Allegro 500 mit im Gepäck sowie die neu entwickelte Integration von Webshark als Analyse-Feature.



Mobiles Netzwerk-Troubleshooting mit dem Allegro Network Multimeter

Die von Allegro Packets entwickelten Allegro Network Multimeter sind Geräte, die Fehler und Probleme im Netzwerk mit wenigen Klicks aufspüren können. Sie analysieren alle Metadaten von Layer 2 bis Layer 7 in Echtzeit. Verschiedene Produktvarianten (1 bis 100 GBit/s) bieten je nach Anspruch das entsprechend zugeschnittene Gerät, vom ultra-portablen Allegro 200 bis hin zum 4 U Allegro 5500 für große Rechenzentren und ISPs.

Allegro 500 und Webshark begeistern Besucher

Besonders begeistert waren die Standbesucher auf der it-sa von den verbesserten Möglichkeiten im ultra-mobilen Bereich. Mit dem Allegro 500 hat Allegro Packets eine Appliance auf den Markt gebracht, die mit etwa einem Kilogramm Gewicht kaum größer ist als ein kompaktes Taschenbuch. Dadurch ist es sehr gut geeignet für die mobile Fehlersuche in weitläufigen Krankenhäusern und Kliniken. Dort wird in jedem Bereich ein störungsfreies Netzwerk erwartet und benötigt, sei es in Behandlungsräumen, Patientenzimmern, OP-Bereichen, Verwaltungsgebäuden oder Kantinen. Netzwerk-Fehler oder -Ausfälle können die notwendige Patientenversorgung erheblich stören.

Allegro 500 im Krankenhaus

Ein spezieller Anwendungsfall für das Allegro 500 ist das Netzwerk-Monitoring im Krankenzimmer oder Wartebereich. Natürlich können Patienten auch funktionierende Multimedia-Systeme erwarten, aber bei bereitgestellten WLAN-Accesspoints muss es dem Administrator im Problemfall möglich sein, den Netzwerkverkehr zu untersuchen. Dadurch kann er Geräte identifizieren, die zu viel Bandbreite nutzen oder auch verdächtigte Aktivitäten durchführen, wie z.B. Port-Scans. Dies zu erkennen und ggf. zu verhindern, erfordert eine Messung direkt an der Netzwerkschnittstelle des Geräts, um unverfälscht den tatsächlichen Netzwerkverkehr zu sehen. Administratoren können so schnell erkennen, welche Netzwerkdienste die Geräte nutzen oder selbst bereitstellen. Für solche Einsätze eignet sich das neue Allegro 500 besonders durch die mobile Bauform und die unkomplizierte Installation. Ein zusätzliches Tablet genügt und der Admin kann alle notwendigen Messungen vor Ort erledigen.

Allen Geräten von Allegro Packets ist gemein, dass Netzverantwortliche mit deren Hilfe den gesamten Netzwerkverkehr ohne Wartezeit in Echtzeit untersuchen können, sowohl den aktuellen als auch den zurückliegenden Verkehr. Über das browserbasierte Webinterface werden auf dem Dashboard die wichtigsten Netzwerkparameter dargestellt, z.B. die größten Verbindungen, die wichtigsten Protokolle oder die TCP-Retransmissions.

Noch effizienter mit Webshark

Um einzelne Bereiche der Verkehrsdaten noch effizienter zu untersuchen, kann der Administrator die Daten mit dem neu integrierten Webshark-Feature direkt im Browser einer Paketanalyse unterziehen. Mussten vorab eingekreiste Problemstellen zunächst gecaptured und anschließend in Wireshark eingespielt werden, stehen ab jetzt viele Paketanalyse-Funktionen in Echtzeit zur Verfügung.

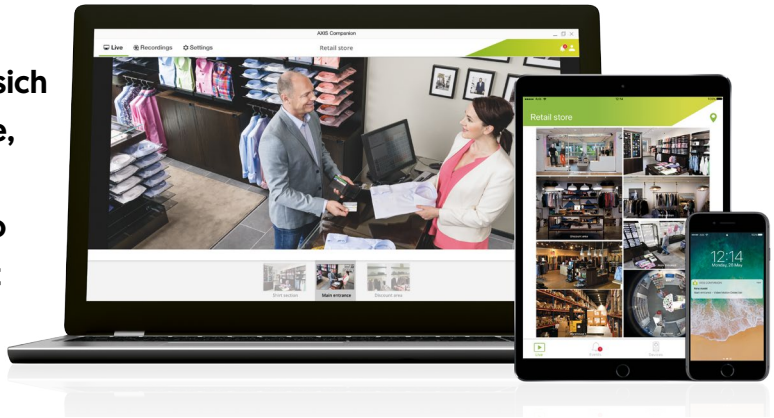
Der Administrator kann mit den auf der it-sa präsentierten Produkt- und Funktionserweiterungen sein Netzwerk noch effizienter analysieren.

Über Allegro Packets

Der Spezialist für Netzwerkanalyse Allegro Packets bietet innovative Fehlersuch- und Analysefunktionen für Netzwerkprobleme mit dem Allegro Network Multimeter an. Die Allegro-Geräte erfüllen durch ihre innovativen Features alle Anforderungen moderner Informations-Infrastrukturen. Zu den Kunden gehören Netzwerkverantwortliche von Unternehmen, Rechenzentren, IT-Dienstleistern, Systemhäusern und ISPs. Entwickelt wird das Allegro Network Multimeter zu 100 Prozent in Deutschland.

Innovationen für eine intelligentere und sichere Welt

Auf der it-sa 2019 in Nürnberg, Europas größter Messe für IT-Sicherheit, drehte sich bei Axis alles rund um aktuelle Produkte, Anwendungen und Lösungen aus den Bereichen Netzwerk-Video sowie Audio und dem entsprechenden Management von Sicherheitskonzepten.



Ob zur Verhinderung eines Diebstahls, zur Lösung eines Vorfalls oder dem effizienten Schutz eines Areals vom größeren Firmengelände bis zum Ein-Mann-Betrieb – viele Unternehmen scheuen oftmals den Einsatz eines professionellen Sicherheitssystems. „Zu teuer. Zu komplex" lauten wiederholt die Vorurteile. Doch mit der Komplettlösung AXIS Companion und der Video Management Software AXIS Camera Station gibt es spezielle Lösungen, die besonders einfach in der Handhabung und auf die Bedürfnisse der jeweiligen Zielgruppen abgestimmt sind.

AXIS Companion bietet einfachen, sichere und zuverlässige Verwaltung von Sicherheitssystemen

Als Einstiegsmodell in die professionelle Überwachung eignet sich AXIS Companion. Die Komplettlösung besteht aus Überwachungskameras, Videoaufzeichnungslösungen sowie einer kostenfreien Video Management Software inklusiver mobiler Applikation. Besonders die schnelle und einfache Systemkonfiguration sowie intuitive Bedienung zeichnet die Komplettlösung aus. Dabei können bis zu 16 AXIS Companion Kameras integriert werden. Außerdem ermöglicht die AXIS Secure Remote Access Technologie den Benutzern den Fernzugriff auf Live-Video oder aufgezeichnete Videos ohne Netzwerk- oder Router-Konfiguration. Egal ob Ladengeschäft, Hotel, Büro oder andere kleine Unternehmen – AXIS Companion ist eine qualitative Sicherheitslösung, die Unternehmen, Mitarbeiter und Anlagen gleichermaßen schützt und ein hervorragendes Preis-Leistungs-Verhältnis bietet.

Zu den wichtigsten Eigenschaften der AXIS Companion 4 gehören:

- Benachrichtigungen in Echtzeit
- Multi-User-Funtkion für mehr Flexibilität
- Systemverwaltung per Fernzugriff

AXIS Camera Station für mehr Effizienz

Eine effiziente Verwaltung bietet sich durch die AXIS Camera Station, um die Sicherung von Beweismittel zum Schutz von Räumlichkeiten zu ermöglichen oder zur Erleichterung des Geschäftsalltags beizutragen. Die vielseitige, flexible Video Management Software ist ideal für Industriebetriebe, Behörden und Bildungseinrichtungen sowie andere Unternehmen geeignet, die ein anwenderfreundliches Videoverwaltungssystem suchen. Eine intuitive Steuerung der Kameras über die Software bietet optimale Sicherheit.

Mit der AXIS Camera Station kann der Nutzer aus der Ferne nützliche Funktionen der Axis Netzwerk-Video-Türstationen zur audiovisuellen Identifizierung und der Eingangskontrolle ergänzen. Ferner können durch die Integration von Axis Netzwerk-Lautsprechern Personen per Fernzugriff angesprochen und unerwünschte Aktivitäten abgewendet werden. Wenn es der Kunde wünscht, unterstützt die AXIS Camera Station schließlich auch die Integration von Drittanbieter IP-Kameras.

Über Axis Communications

Axis ermöglicht eine smarte und sichere Welt durch die Entwicklung von Netzwerklösungen. Diese bieten Erkenntnisse, um die Sicherheit und Geschäftsmethoden zu verbessern. Als Technologieführer im Bereich Netzwerk-Video bietet Axis Produkte und Dienstleistungen für Videoüberwachung und -analyse sowie Zutrittskontrolle und Audiosysteme. Das 1984 gegründete schwedische Unternehmen beschäftigt mehr als 3.000 engagierte Mitarbeiter in über 50 Ländern. Gemeinsam mit seinen Partnern auf der ganzen Welt bietet das Unternehmen kundenspezifische Lösungen an.

www.axis.com.

AlgoSec auf der it-sa 2019

Für AlgoSec war die it-sa 2019 ein voller Erfolg, denn wir waren an den Ständen von drei Partnern vertreten, wo reger Austausch mit Kunden und Interessierten stattfand. Dabei haben wir mit Freuden festgestellt, dass sich die Messe auch in diesem Jahr wieder vergrößert hat und noch mehr Leute für die IT-Sicherheit begeistert. Auch in diesem Jahr stießen wir mit unseren Produkten, unter Anderem zur Automatisierung der IT Sicherheit von internen Abläufen, auf breites Interesse des it-sa-2019-Publikums.

von Robert Blank, DACH Lead – Regional Sales Manager bei AlgoSec

Die Beschleunigung von Prozessen und das Vereinfachen der Verwaltung in der IT-Sicherheit sind in aller Munde. Das hängt einerseits mit der Vielfalt an Produkten zusammen, andererseits mit neuen Trend-Themen, wie Cloud und Compliance. Unternehmen müssen mittlerweile nicht nur einen Unternehmensperimeter überblicken, sondern eine Mischung unterschiedlicher Sicherheitslösungen, wie Firewalls verschiedener Hersteller, unter Kontrolle haben und hybride IT-Umgebungen verwalten. Außerdem wollen viele deutsche Firmen und Einrichtungen zwar in die Cloud, aber das Rechenzentrum aus mannigfaltigen Gründen nicht völlig aufgeben. So entsteht das Modell der hybriden Cloud-Struktur.

Im Zeichen der Automatisierung

Der Schwerpunkt lag für uns in diesem Jahr darauf, den Menschen zu erklären, wie sie die vielen verschiedenen Schutzmaßnahmen ihres Unternehmens, eine umfassende Compliance zu aktuellen Verordnungen – wie bsp. der DSGVO – und die Durchsetzung von Firewall-Richtlinien im gesamten Netzwerk, unter einen Hut bringen können. Das Jahr 2019 steht klar im Zeichen der Automatisierung. Gerade öffentliche Einrichtungen, wie Krankenhäuser profitieren von diesem Konzept, weil sie sensible Daten verwalten müssen, die keinesfalls in die falschen Hände geraten dürfen. Darüber hinaus unterliegen diese Einrichtungen den strengen Bestimmungen der deutschen KRITIS.

Ihnen allen kommt eine Vereinfachung der IT-Sicherheit sehr entgegen. Unsere zentrale Konsole gewährt einen Überblick des gesamten Netzwerks und sorgt dafür, dass Firewall-Regeln automatisiert auf allen Systemen eingeführt werden. Das nimmt den Verantwortlichen aufwendige, monotone Arbeit ab und spart wertvolle Zeit und Ressourcen.

Garantierte Compliance – Vertrauensvolle Patienten

Gerade im Bereich des Datenschutzes haben wir auf der it-sa 2019 einen schönen Höhepunkt unseres diesjährigen Schaffens präsentieren können. Unsere Sicherheitslösung unterstützt den neuen BSI-200-Standard und liefert vorgefertigte Reports für Audits und interne Abteilungen. Das hilft allen Unternehmen und Einrichtungen, deutsches Recht zu erfüllen, und darüber hinaus besonders viel Vertrauen zu den Kunden aufzubauen, weil sie die Empfehlungen der deutschen Sicherheitsbehörden umsetzen. Vor allem Krankenhäusern, die Gesundheitsdaten handhaben müssen und tausende von Patienten betreuen, sollten die beste IT-Sicherheit so einfach wie möglich bieten können, um ihren wichtigsten Rohstoff zu bewahren: Das Vertrauen der Menschen in die Sicherheit der Einrichtungen.

Robert Blank, DACH Lead – Regional Sales Manager bei AlgoSec

IT-Sicherheit für Krankenhäuser gehört auf den Prüfstand

Vor drei Jahren traf eine Ransomware das Lukas Krankenhaus in Neuss, schaltete dort die IT-Systeme ab und verschlüsselte sie. Der Angriff konnte ohne Lösegeld vereitelt werden, doch die Gefahr bleibt. Ende des Jahres 2018 geriet ein Krankenhauses in Bayern ins Visier. Erneut legte ein Cyber-Angriff die IT-Systeme lahm. Die Reparatur dauerte zwar aufgrund guter und schneller Fehlerbehebung nur eine Woche, dennoch ist das nur Schadensbegrenzung: Krankenhäuser, die wochenlang keine Patienten versorgen können oder auf analogen Betrieb umstellen, befinden sich in einer extremen und inakzeptablen Situation. Im Jahr 2019 schließlich wurde die DRK-Trägergesellschaft Süd-West des Kirchener Krankenhaus in der Nähe Siegens von Ransomware getroffen. Zwischenzeitlich waren alle 11 Einrichtungen an den 13 Standorten unter Beschuss.

Dirk Arendt, IT-Sicherheitsexperte und Leiter Public Sector & Government Relations bei Check Point Software Technologies GmbH

Gefahrenherd IoT

Anfang des Jahres wiesen unsere Sicherheitsforscher auf Lücken in Ultraschallgeräten hin. Sie enthielten Schwachstellen, die auf fehlende Patch-Management-Möglichkeiten, mangelnde Verschlüsselung bei der Datenübertragung und gespeicherte, staatliche Anmeldeinformationen zurückgehen. Das ist sehr gefährlich, denn die Geräte sind mit dem Krankenhausnetzwerk verbunden. Erfolgreiche Angriffe können zum Verlust personenbezogener Daten führen oder zur gefährlichen Manipulation der Behandlungen: Hacker könnten die medizinischen Informationen eines Patienten über Medikamente oder Dosierungen ändern und MRI-, Ultraschall- und Röntgen-Geräte übernehmen. Krankenhäuser müssen daher auf die zahlreichen Einstiegspunkte achten, die in ihrem Netzwerk vorhanden sind.

Daten trennen & Netzwerke segmentieren

Eine Trennung der Patientendaten vom Rest des IT-Netzwerks empfiehlt sich. Die IT-Mitarbeitern im Gesundheitswesen erhalten dadurch eine klare Sicht auf den Netzwerkverkehr, um ungewöhnliche Bewegungen zu entdecken, die auf einen Verstoß oder eine Beeinträchtigung hinweisen können. Mithilfe der Netzwerk-Segmentierung verhindern die Einrichtungen zudem, dass sich Malware oder Hacker ungehindert ausbreiten können und isolieren so die Bedrohung. Die Segmentierung ist eine bewährte Methode, die dabei hilft, neue und digitale Innovationen und Sicherheitslösungen einfacher zu implementieren. Gleichzeitig entsteht eine weitere Sicherheitsebene für den Netzwerk- und Datenschutz – ohne die Leistung oder Zuverlässigkeit zu beeinträchtigen.

Fazit: Moderne Sicherheitstechnologien als Präventionsmaßnahme

Fremde und illegitime Zugriffe auf Netzwerke lassen sich durch technische Lösungen einschränken, wie: Firewalls, Application Control, URL-Filtering, Intrusion-Prevention-Systeme, Anti-Viren-, Anti-Bot- und Sandboxing-Technologien. Wenn die Schutzmaßnahmen zusätzlich über eine zentrale Plattform kommunizieren und Daten austauschen – außerdem von dort schnell und aufeinander abgestimmt gesteuert werden – erkennt die Sicherheitslösung rechtzeitig eine große Anzahl virtueller Attacken und wehrt sie ab. Präventiv sollte gegen Bedrohungen vorgegangen werden, nicht reaktiv. Sonst ist der Angriff bereits geschehen und was bleibt ist die Schadensbegrenzung. Ziel aber muss die Schadensvermeidung sein.

Dirk Arendt, IT-Sicherheitsexperte und Leiter Public Sector & Government Relations bei Check Point Software Technologies GmbH

Wie verhindert man Cyberangriffe in Krankenhäusern?

Cyberkriminelle haben es immer mehr auf Krankenhäuser abgesehen. Deren Fülle an persönlichen Daten ist eine wahre Goldgrube und die Zahl der erfolgreichen Angriffe wächst ständig. Veraltete IT-Systeme und eine zu geringe Investition in die Cybersecurity setzen Krankenhäuser der Gefahr aus, dass Abläufe gestört werden und Patientendaten bedroht sind. Im Zuge der auch dort fortschreitenden Digitalisierung von Patienten-Aufzeichnungen und dem Weiterleiten von Patientendaten steigt die Anzahl der möglichen Angriffsziele.

Cyberattacken stellen für alle Organisationen eine große Bedrohung dar, für Krankenhäuser allerdings kann es sogar noch lähmender sein. Eine erfolgreiche Attacke kann einem medizinischen Mitarbeiter die Patientendaten unzugänglich machen, medizinische Geräte können nicht genutzt werden oder Patientendaten werden sogar gestohlen. Letztendlich ist die Sicherheit der Patienten gefährdet und Krankenhäuser werden mit Klagen, Kunstfehler-Vorwürfen und Geldbußen konfrontiert.

Jüngste Forschungen zeigen, dass fast alle IT-Zuständigen in der Healthcare Branche den Cyberkriminellen hinsichtlich Security-Prozesse und -Technologien hinterherhinken. Die Industrie erwartet Datenschutzverletzungen, die sie bis Ende 2019 3,6 Milliarden Euro kosten wird. Das ist durchaus ein wichtiges Thema! Wenige in der Industrie waren nicht betroffen vom WannaCry Virus, der den UK National Health Service in 2017 angriff. Die Attacke verursachte großen Schaden und die Wiederherstellung und Bereinigung kostete rund 79 Millionen Euro.

Wie können Krankenhäuser Cyberangriffe verhindern?

Jeder IT-Security-Experte weiß, dass es keine Frage ist, OB man angegriffen wird, sondern lediglich WANN. Cyberkriminelle lernen dazu und Angriffe werden immer anspruchsvoller und häufiger. Traditionelle Security Lösungen wie Firewall und Antiviren-Lösungen reichen nicht mehr aus. Um den Cyberkriminellen eine Nase voraus zu sein, müssen Krankenhäuser einen mehrschichtigen, präventiven Ansatz für den persönlichen Datenschutz und die Cybersecurity anwenden.

Die Lösung: Schutz persönlicher Daten auf dem Device und Cybersecurity-Schutz von BlackFog

Viele Hersteller von Netzwerksicherheitsprodukten können Ihnen sagen, wann ein Schaden oder ein Angriff stattgefunden hat. BlackFog stoppt den Angriff genau dort, wo er passiert. Im Fokus sind Datendiebstahl, das Erstellen von Profilen anhand Ihrer Daten und das Sammeln von Daten. BlackFog schützt Sie vor den modernsten Angriffsmustern. Es schließt die Lücke zwischen Security Solutions, die -wie Firewalls- einen Zugriff verhindern, und AV/Malware Lösungen, die den Schaden bereinigen, NACHDEM er schon längst entstanden ist.

Durch den mehrschichtigen Ansatz erkennt BlackFog in Echtzeit, wenn ein Angreifer unberechtigt versucht, Daten von einem Gerät oder einem Netzwerk abzugreifen, und lässt es erst gar nicht so weit kommen.

Warum ist BlackFog anders?

- **BlackFog** ist die einzige Software, die auf dem Device vor Datendiebstahl schützt. KEINE Daten werden an die Cloud geschickt.
- **BlackFog** ist die einzige Firma, die in der Lage ist den AUSGEHENDEN Datenfluss zu blocken. Was auf dem Device ist, BLEIBT auf dem Device
- **BlackFog** schützt 12 verschiedene Schichten gegen Ransomware, Spyware, Malware, Phishing, unberechtigtes Datensammeln und Erstellen von Profilen.
- **BlackFog** ist die EINZIGE Lösung, die Cybersecurity, Privacy und Compliance liefert.

Schlussfolgerung

Krankenhäuser werden das Ziel für Cyberkriminelle bleiben und Angreifer werden ausnahmslos in das Netzwerk eindringen. Somit sind proaktive Lösungen, die auf Cyberattacken abzielen, kritisch zu sehen. Cybersecurity Tools, die Angriffe in Echtzeit erkennen und sie abwehren BEVOR irgendwelche Daten kopiert und entnommen werden können ist der neue Normalzustand. Um dem Datenschutzgesetz zu entsprechen und vor Fehlverhalten und späteren Klagen zu schützen, ist dieser mehrschichtige, präventive Ansatz der Cybersecurity essentiell.

Die Red Eagle IT Distribution beantwortet Ihnen gern weitere Fragen!
Kontakt: Red Eagle IT Distribution **www.redeagle-it.de**
Telefon **+49 (0)89 1 22 28 39 30**

Autonomes Krankenhaus – für das Netzwerk ideal

Visite per Tablet, papierloses Arbeiten oder Patienten-Self-Service – die Digitalisierung in der Gesundheitswirtschaft zieht kräftig an. Mit ihr nehmen aber auch die Attacken von Cyberkriminellen zu. So hatte das Gesundheitswesen nach einer aktuellen Studie[1] überwiegend Malware vom Typ Trojaner zu bekämpfen, die im dritten Quartal 2019 um 82 Prozent gegenüber dem Vorquartal angestiegen ist. Weiter heißt es: „Aufgrund der alt(ernd)en Infrastruktur, niedrigen IT-Budgets und einer Fülle von persönlich identifizierbaren Informationen (PII) haben sich vor allem Gesundheitseinrichtungen zu attraktiven Zielen von Cyber-Kriminellen entwickelt."

Um dieser Entwicklung entgegenzutreten, ist es für Krankenhäuser essenziell, bereits auf der Netzwerkebene anzusetzen. Wenn hier die richtigen Stellschrauben bewegt werden, dann ist ein erster, wichtiger Schritt getan. Denn die in der Studie angesprochene Infrastruktur besteht nicht selten aus Netzwerken alter Prägung. Diese sollten – und das kostenschonend sukzessive – in ein autonomes, mit künstlicher Intelligenz (KI) versehenes Netzwerk transformiert werden. Dieses übernimmt selbstständig Aufgaben, sowohl der Administration als auch der IT-Sicherheit. Die KI sorgt außerdem dafür, dass das Netz dazu lernt, seine Fähigkeiten kontinuierlich ausbaut.

Die dafür notwendigen technologischen Werkzeuge sind eine Fabric-basierte Netzwerkarchitektur, eine regelzentrierte Netzwerkadministration und ein modernes Netzwerkmanagement. Alles unter einer Oberfläche und optimiert mit eingängigen Analysetechniken. Ein großes Plus an Sicherheit entsteht in diesem Konzept dadurch, dass Schutz und Redundanzmechanismen integriert sind, die die Integrität und Zuverlässigkeit fortlaufend verbessern. Elemente des autonomen Netzwerks sind Access Point, Ethernet-Switch, Router und Software.

In solch einem Netzwerk lässt sich dessen Datenverkehr beispielsweise sehr schnell und komfortabel segmentieren. Eine sogenannte Hyper-Segmentierung isoliert die speziellen Datenströme auf Ebene 2 und/oder Ebene 3 und macht die Daten außerhalb des betreffenden Netzwerksegmentes unsichtbar. Sollte es einem Hacker gelingen, in einen Datenstrom einzudringen, dann bleibt er auf dieses Netzwerksegment und damit diesen Datenstrom beschränkt, da die anderen Segmente aus diesem Netzwerksegment heraus nicht sichtbar sind.

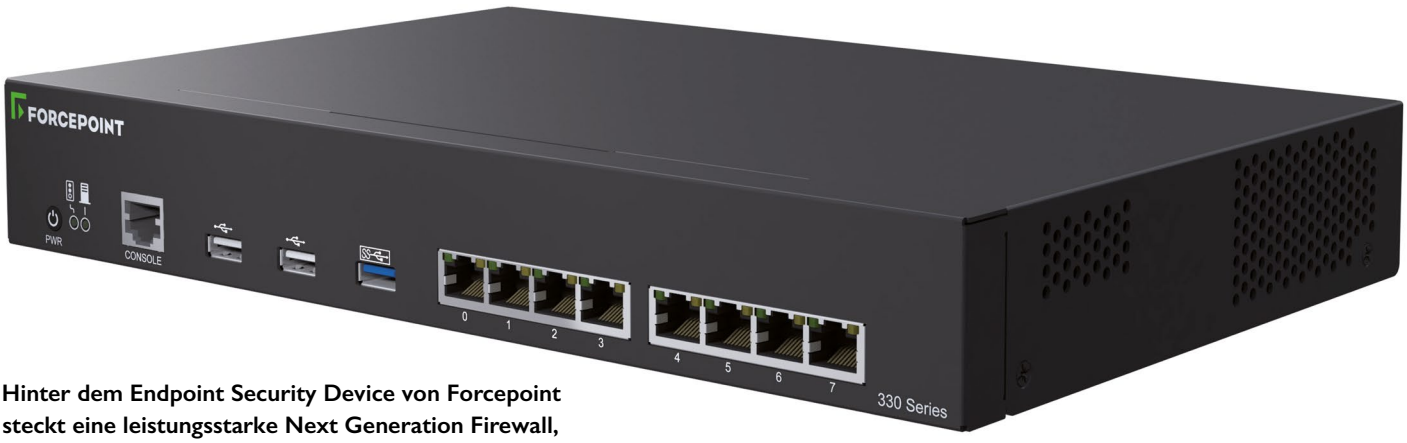
Ähnliches gilt für die Integration von medizinischer Hardware. Vom Röntgengerät über das Tablet des Chefarztes bis hin zu Pumpensystemen sind heute unzählige Devices mit dem Netz verbunden. Durch die Kombination eines Regelwerks mit der Fabric-Technologie können sowohl Nutzer als auch Geräte identifiziert und automatisch mit den Netzwerkdiensten verbunden werden, auf die sie Zugriff haben dürfen. Dies ist unabhängig davon, wo und wann sie sich innerhalb des Netzwerkes verbinden. Damit entfällt die sonst notwendige vorherige Konfiguration aller für diese Nutzer eventuell nutzbaren Anschluss-Ports an den Switchen beziehungsweise Access Points. Dies funktioniert reibungslos und sicher.

Fazit: Autonomie auf Netzwerkebene hilft im Gesundheitswesen enorm, sorgt automatisch für mehr Sicherheit, entlastet die IT-Administration und minimiert Fehler und Risiken.

Andreas Helling

Legacy-Systeme im Krankenhaus schützen

Medizingeräte sind häufig länger in Betrieb, als es für den Antivirus-Agenten Sicherheitsupdates gibt. An dem Tag an dem dieser Support endet und keine aktuellen Updates mehr bereitgestellt werden, sind die Geräte nicht mehr ausreichend geschützt. Ein neues Endpoint Security Device von Forcepoint, das vor die Geräte geschaltet wird, verspricht nun als „virtuelles Schild" umfassenden Schutz.



Hinter dem Endpoint Security Device von Forcepoint steckt eine leistungsstarke Next Generation Firewall, die Traffic-Normalisierung beherrscht.

Im September 2019 wurde nach Recherchen des Bayerischen Rundfunks und der US-Investigativplattform ProPublica bekannt, dass millionenfach hochsensible Patientendaten ungeschützt im Netz abgelegt wurden. Sind die vernetzten Geräte nicht ausreichend geschützt, haben Kriminelle leichtes Spiel, über den Remote Access Port auf das jeweilige Gerät zu gelangen und so in ein Klinik-IT-Netzwerk einzudringen. Auch ein deutscher, brachenführenden Hersteller von Medizinprodukten stand vor der Herausforderung, seinen Tausenden von Bildgeräten weltweit den aktuellsten Schutz bereitzustellen.

Nachholbedarf bei IT-gestützen Medizingeräten

Medizingeräte werden meistens bis ans Ende ihrer maximalen Lebensdauer in Betrieb gehalten. Das ist wirtschaftlich. Das branchenübergreifende Problem dabei ist allerdings, dass alte Legacy-Systeme zunehmend vernetzt sind beziehungsweise ans Internet angebunden werden. Je länger ein Gerät in Betrieb ist, desto größer wird jedoch das Risiko, dass dieses angegriffen wird. Ein Beispiel: Zum Schutz der angeschlossenen medizinischen Bildgebungsgeräte, die das oben erwähnte Unternehmen verkauft, stellte es eine Antiviren-Endpunkt-Sicherheitssoftware von Drittanbietern zur Verfügung, die auf Windows-Betriebssystemen läuft. Am 31.12.2018 endete allerdings die Unterstützung von Windows XP. Dieses Betriebssystem ist aber auch heute noch sehr weit verbreitet. Immer weniger Hesteller liefern noch ein Update hierfür aus. Für Windows XP gibt es jedoch eine sehr hohe Anzahl an Malware, die angewendet werden kann, um verborgene Schwachstellen auszunutzen. Kliniken machen hierbei oft den Fehler, sich in Sicherheit zu wiegen, weil ihre Next Generation Firewall noch über aktuelle Updates verfügt. Das Problem dabei sind allerdings die sogenannten Advanced Evasions. Getarnt oder etwas manipuliert wird Malware, dann nicht mehr erkannt. Es gibt kein Match mehr mit der bestehenden Blacklist. Dasselbe Szenario steht uns zum kommenden Jahreswechsel mit Windows

7 bevor, denn auch für dieses Betriebssystem endet der Support bei einigen großen Herstellen von Antivirus Software.

Hat ein Krankenhaus also eine Vielzahl von Windows-XP- und Windows-7-gestützten Geräten im Einsatz, für die es keine neuen Security Patches mehr gibt und somit auch die Blacklists nicht mehr aktualisiert werden, ist es für Hacker ein leichtes, innerhalb von Sekunden auf medizinische Geräte zuzugreifen. Das Aktualisieren oder Ändern von Software auf den Geräten selbst ist schwierig, zeitaufwändig und öffnet wiederum die Tür für das Risiko von Manipulationen und Ausfällen. So musste auch der bekannte Medizintechnikhersteller seinen Kunden einen alternativen Schutz vor Angriffen bieten.

Die Lösung: ein Endpoint Security Device von Forcepoint

Die Lösung besteht darin, vor die Bildgebungs- bzw. Medizingeräte mit einem alten Betriebssystem, ein Forcepoint Endpoint Security Device zu schalten, hinter dem sich eine leistungsstarke Next Generation Firewall (NGFW) verbirgt, die Traffic-Normalisierung beherrscht. Mit solch einem Device lässt sich die Zugriffskontrolle auf die vernetzten Geräte regeln und genau scannen, ob unter den zugreifenden Nutzern auch Schädlinge sind. Dabei wird nicht nur bekannter Schadcode, der auf einer Blacklist als solcher definiert ist, erkannt. Vielmehr reagiert das Endpoint Security Device durch integrierte Advanced Evasion Techniques wie Traffic-Normalisierung auch bei getarnten Dateien. So lassen sich auch Varianten eines Schädlings als solche erkennen und abblocken. Um die Geräte herum wird ein virtuelles Schild aufgebaut.

Intrusion Prevention Systeme als virtuelles Schild

Das Endpoint Security Device von Forcepoint kann als Teil eines Intrusion-Prevention-Systems (IPS) eingesetzt werden. Die Schutzwirkung eines IPS legt sich wie eine virtuelle Glocke über ein zu schützendes Medizingerät. Man spricht auch vom „virtual shielding". Dieser Vorgang ist genau dann hilfreich und wichtig, wenn es noch nicht gepatchtes „Equipment" zu schützen gilt. Betriebsverantwortliche müssen schließlich sicherstellen, dass ihre Geräte bis zum Patchzyklus über ausreichenden IT-Schutz verfügen.

Die wenigsten Next Generation Firewalls und Intrusion Prevention Systeme sind allerdings aufgrund ihrer rein Pattern-basierten Arbeitsweise in der Lage, Attacken verlässlich abzuwehren. Die Anzahl der Möglichkeiten, einen Schadcode zu verschleiern, ist schlicht zu groß. Das schafft nur ein System, das in der Lage ist, vor dem Datenbankabgleich eine Traffic-Normalisierung durchzuführen, wodurch der eigentliche Schadcode sichtbar wird und der Datenabgleich erfolgreich sein kann. Im Forcepoint IPS findet die gesamte Malware-Kontrolle statt. Und: Im Gegensatz zum reinen Intrusion Detection System (IDS) wird Schadecode hierbei nicht nur erkannt, sondern gleichzeitig auch abgewehrt.

Fazit

In einer digitalisierten Gesundheitsbranche sollte die Cybersicherheit oberste Priorität haben. Die Realität ist allerdings nach wie vor: Sie wird von vielen Kliniken, Krankenhäusern und auch Medizintechnikherstellern vernachlässigt. Doch nur wenn die Cybersicherheit gewährleistet ist, sind sensible Daten gut aufgehoben und Medizingeräte können ordnungsgemäß eingestzt werden. Institutionen und Unternehmen brauchen deshalb ein Endpoint Security Device, um ihrer obersten Priorität, dem Schutz des Patienten, Sorge tragen zu können. Das angeführte Medizintechnikunternehmen mit mehr als 120 Jahren Erfahrung in den Bereichen medizinische Bildgebung, Labordiagnostik und neuartige Therapien, hat dies bereits erkannt.

Frank Limberger Data and Insider Threat Security

E-Mail-basierte Angriffe auf Krankenhäuser haben Hochkonjunktur

Auf der IT-Sicherheitsmesse it-sa 2019 im Oktober sieht Arne Schönbohm, Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI), IT-Sicherheit als Grundpfeiler der Digitalisierung. Wenige Tage nach dem Event veröffentlicht die Behörde ihren aktuellen Lagebericht der IT-Sicherheit und warnt vor „intensiven Ransomware-Kampagnen", welche seit Anfang des Jahres 2019 für schwerwiegende Ausfälle in ganz Europa sorgten. Als größte Bedrohung macht das BSI dabei Schadprogramme aus, die vor allem per E-Mail gestreut werden.

Von Lothar Geuenich, Sales Director Central Europe bei Mimecast

Gerade im Gesundheitswesen ist die Gefahr weiterhin hoch. Einige erinnern sich noch an das Medienecho im Jahre 2016, als ein Krankenhaus in Neuss nach einer erfolgreichen Attacke mit Verschlüsselungstrojanern Patienten abweisen musste. Im letzten Jahr sorgte zudem das Klinikum Fürstenfeldbruck für Schlagzeilen: Mit nur einer verseuchten E-Mail wurden hunderte Computer lahmgelegt. Experten sind der Meinung, dass beides keine Einzelfälle sind, da die Betroffenen sich häufig nicht zu Attacken äußern.

Die Gefahr wächst, da die eingesetzten Schädlinge immer potenter werden. Das BSI nennt zum Beispiel die Bedrohung von „Outlook-Harvesting" und erläutert dies am Beispiel der Schadsoftware Emotet. Die Malware ist bereits seit 2010 bekannt, wird aber durch organisierte Cyberkriminelle immer wieder erweitert. Jetzt ist sie in der Lage, den Mailverlauf der Opfer zu analysieren und sich gezielt weiterzuverbreiten – wie im Fall von Fürstenfeldbruck. Nach einer Infektion verteilt sich der Schadcode rasend schnell und streut sich über die E-Mail-Kontakte des Opfers. Krankenhäuser sind daher besonders bedroht.

Immer mehr Prozesse im Gesundheitswesen sind digitalisiert. Viele sensible Informationen werden über virtuelle Kanäle ausgetauscht. Allerdings muss medizinisches Fachpersonal neben ihrer normalen Tätigkeit und dem Umgang mit IT zudem noch Sicherheitsherausforderungen stemmen. Intelligente Malware ist nur ein Teil der Bedrohung. Sie kann zwar teilweise durch Sicherheitstechnologie abgewehrt werden, allerdings sind Security-Tools alleine nicht mehr ausreichend. Eine andere Methode sind beispielsweise Phishing-E-Mails oder Links zu Scam-Homepages. Vor beidem warnt das BSI ebenfalls explizit, denn diese tragen erstmal keine schädlichen Payload in sich und lassen sich durch klassische Schutzsoftware nicht erkennen.

Typische Angriffe ohne Schadsoftware imitieren Nachrichten von Kollegen, Partnern oder Patienten. Immer wieder werden als Folge sensible Informationen an Kriminelle weitergegeben oder Banktransfers unwiderruflich auf falsche Konten getätigt. Ohne entsprechende Sensibilisierung sind gefakete Mails nur schwer zu durchschauen. Dabei sind die Nutzer in der Regel die letzte Verteidigungslinie, um eine Attacke zu vereiteln.

Ein Schlüsselfaktor zur Abwehr dieser neuen Welle von E-Mail-Attacken ist die Resilienz einer Organisation: Es geht um die Widerstandsfähigkeit in allen Bereichen. Dies betrifft Schadsoftware wie Ransomware, aber eben auch Phishing-Attacken und Social Engineering. In der Praxis sollten Einrichtungen zum einen passende Sicherheitstools implementieren, die sämtlichen E-Mail-Verkehr absichern. Gleichzeitig braucht es aber damit verbundene Trainingsmechanismen, die sich an die Bedürfnisse der Nutzer anpassen und regelmäßig die Awareness in diesem Bereich verbessern. Außerdem braucht es für den Fall der Fälle eine Backup-Strategie samt Notfallplan, damit selbst bei einer Infektion der laufende Betrieb nicht gefährdet wird.

Lothar Geuenich, Sales Director Central Europe bei Mimecast

Datenklassifizierung und Auditierung im Gesundheitswesen

Für Netwrix stellte die it-sa 2019 wie auch letztes Jahr einen vollen Erfolg dar. Am gutbesuchten Messestand konnten wir interessierten Besuchern die Wichtigkeit intelligenter Lösungen für Auditing und Datenklassifikation näherbringen und gleichzeitig aufzeigen, welche Risiken ungeordnete und unklassifizierte Daten für die Unternehmenssicherheit darstellen.

Ein Beitrag von Jürgen Venhorst, Country Manager DACH bei Netwrix

Unser Highlight für die diesjährige it-sa war mit Sicherheit der Cloud Data Security Report (CDSR). Besonders für das Gesundheitswesen konnten wir mit seiner Hilfe wertvolle Erkenntnisse liefern, die Organisationen aus diesem Bereich dabei helfen, eventuelle Schwachstellen in ihrer IT-Sicherheit auszumachen. Obwohl oder eben weil sie zur kritischen Infrastruktur gehören, sind Datenlecks und Sicherheitslücken ein immer noch allzu häufiges Problem. Beispielsweise berichten 26 Prozent der im Zuge des Reports befragten Gesundheitsorganisationen, seit Mitte 2018 mindestens einen Sicherheitsvorfall gehabt zu haben.

Mit Data Classification und Auditing zu mehr Sicherheit

Eine intelligente Auditierungslösung kann hier sowohl eine hohe Übereinstimmung mit gesetzlichen und firmeninternen Vorgaben gewährleisten, als auch IT- und Sicherheitsabteilungen in Unternehmen entlasten, indem sie auf Knopfdruck verständliche und verlässliche Audits liefert. IT-Verantwortliche können mit ihrer Hilfe sehen, an welchen Stellen Risiken in der IT-Sicherheit existieren und werden gleichzeitig entlastet, indem die Auditierung automatisiert stattfindet.

Im gleichen Maße wichtig ist eine gut funktionierende Lösung zur Datenklassifizierung. Diese durchsucht beispielsweise die im Krankenhausnetzwerk gespeicherten Daten nach unklassifizierten Informationen wie Krankenakten, Aufnahmen sowie Berichten und ordnet diese nach vorher festgelegten Regeln ein. So können Daten nach bestimmten Begriffen durchsucht und ihrer Kritikalität nach geordnet werden.

Compliance gewährleisten

Seit über einem Jahr ist die DSGVO gültig und noch immer stellt die Verordnung viele Unternehmen vor große Herausforderungen. Um die Compliance hierzu und zu anderen Vorgaben garantieren zu können, haben wir den großen Bedarf an Audit-Lösungen erkannt – nicht nur in unseren Gesprächen auf der itsa. Besonders der Gesundheitsbereich gilt als eine der am stärksten reglementierten Branchen, da die Daten, mit denen hier gearbeitet wird, zu den persönlichsten Daten überhaupt gehören.

Da Krankenhäuser genauso wie Stromerzeuger und die Wasserversorgung zur Kritischen Infrastruktur (KRITIS) gehören, besteht für sie im Falle eines erfolgreichen Cyber-Angriffs eine Mitteilungspflicht an das BSI. Auch hier kann eine Auditing-Lösung wie sie Netwrix anbietet helfen, indem sie Audits automatisiert zusammenstellt, die dann an das BSI geschickt werden können.

Jürgen Venhorst, Country Manager DACH bei Netwrix

uniscon auf der it-sa 2019

„Wir von uniscon blicken auf eine erfolgreiche it-sa zurück und freuen uns über den regen Austausch, der am Stand stattgefunden hat. Zum wiederholten Male als Aussteller in Nürnberg vertreten, haben wir wahrgenommen, dass sich die Fachmesse für IT-Security von Jahr zu Jahr weitervergrößert. Das zeigt uns, dass die Awareness und Sensibilität für Datensicherheit und Datenschutz über sämtliche Branchen hinweg eine immer größere Rolle spielt. Dennoch – oder gerade deswegen – gibt es nach wie vor großen Bedarf an hochsicheren Lösungen, besonders wenn es um die Übertragung, Speicherung und Verarbeitung sensibler Daten geht, beispielsweise aus dem Gesundheitsbereich. Als führender Anbieter von Trusted-Cloud-Lösungen in Europa ist es unser Anliegen, die Vorteile einer Public Cloud mit der Sicherheit eines unternehmensinternen Rechenzentrums zu kombinieren, sodass der Austausch und die Verarbeitung von Informationen einfacher, schneller und vor allem sicher verlaufen.

Von Dr. Hubert Jäger, CTO und Gründer der uniscon GmbH

Sealed Platform für sensible Daten

So lag der diesjährige Messeschwerpunkt bei uniscon auf der sealed platform. Einer Cloud-Plattform, die dank patentierter Sealed Cloud Technologie auch höchsten Sicherheitsstandards gerecht wird: Durch rein technische Mittel sind Daten und Anwendungen vor jeglichem unbefugten Zugriff geschützt – manipulationssicher und präventiv. Selbst der privilegierte Zugriff im Rechenzentrum ist technisch ausgeschlossen. Infrastrukturen wie die Sealed Cloud von uniscon, die auch den Cloud-Betreiber und Administratoren vom Zugriff auf gesicherte Informationen ausschließen, erfüllen dadurch die Kriterien, die für Betreiber Kritischer Infrastrukturen (KRITIS) gelten. Denn Einrichtungen aus dem Gesundheitssektor, die hierzu zählen, sind verpflichtet, den Anforderungen von IT-Sicherheits- und BSI-Gesetz nachzukommen. Das heißt, ihre IT-Infrastruktur muss nicht nur den bewährten und anerkannten Sicherheitsregeln entsprechen, sondern zudem nach dem Stand der Technik gerüstet sein und mindestens dasselbe Sicherheitsniveau einhalten wie fortschrittliche, bereits in der Praxis erprobte Verfahren. Es besteht zudem eine regelmäßige Nachweispflicht, dass Systeme entsprechend geschützt sind; Zertifikate können diesen Nachweis entscheidend erleichtern.

Hochsicherer Austausch von Gesundheitsdaten

Für reges Interesse sorgte am uniscon-Stand zudem idgard, ein hochsicherer Webdienst für den schnellen und unkomplizierten Datenaustausch. Denn wenn Kliniken und Arztpraxen sensible Patientendaten auf digitalem Wege austauschen, spielt der Sicherheitsaspekt eine bedeutende Rolle. Hierbei sind zwingend die Anforderungen der EU-Datenschutzgrundverordnung (DSGVO) zu erfüllen. Außerdem sollte zuverlässig sichergestellt sein, dass lediglich autorisierte Personen Zugriff auf die vertraulichen Informationen haben. uniscon hat hierfür einen Cloud-Dienst entwickelt, der EU-DSGVO-compliant und in der höchsten Schutzklasse für Cloud-Dienste (TCDP-Schutzklasse III) zertifiziert ist. Aufgrund der Sealed Cloud Technologie ist dabei natürlich ebenso gewährleistet, dass der Cloud-Betreiber keinerlei Zugriff auf die gespeicherten oder übertragenen Daten hat.

Vor dem Hintergrund der geplanten digitalen Patientenakte, die den Austausch von sensiblen Gesundheitsdaten zwischen Ärzten, Patienten und Versicherungen vereinfachen soll, ist das rege Interesse an hochsicheren, datenschutzkonformen Lösungen gut nachzuvollziehen. Wir haben uns über die hohen Besucherzahlen auf dem Stand gefreut."

Dr. Hubert Jäger, CTO und Gründer uniscon GmbH

Security aus der Cloud für die Cloud

Im Fokus der it-sa 2019 stand für uns die Absicherung Cloud-basierter Infrastrukturen durch moderne Sicherheitslösungen. Da Mitarbeiter und Anwendungen den klassischen Sicherheits-Perimeter um das unternehmenseigene Rechenzentrum verlassen, sind für die Datenströme in die Cloud neuartige Sicherheitsangebote erforderlich. IT-Verantwortliche bekamen neue Lösungsansätze präsentiert, um die gewonnene Agilität mit sicherem und leistungsstarkem Zugriff auf die Cloud zu kombinieren.

Von Thomas Koch, Area Manager Large Enterprise Germany bei Zscaler

Diese Cloud-basierten Security-Lösungen gehen mit dem Vorteil eines hohen Automatisierungsgrads und höherer Sicherheit einher und wirken dadurch dem IT-Fachkräftemangel und Kostendruck im Gesundheitswesen entgegen. Die Verwaltung von Security-Hardware und Patch-Management gehören der Vergangenheit an, da der Cloud-Security-Anbieter die erforderlichen Sicherheits-Updates automatisch in der Cloud vornimmt, und dabei bis zu 120 000 Updates pro Tag bereitstellt.

Auf der Sicherheitsmesse wurde auch der Zero-Trust-Ansatz als Gebot der Stunde gehandelt, zu dem erste Cloud-basierte Lösungen vorgestellt wurden. Ein solches Modell löst den traditionellen Netzwerkzugriff ab und führt ein Zugangsmodell auf Anwendungsebene ein. Der Angriffsvektor auf sensible Patientendaten wird reduziert, da der Anwender oder Partner erst Zugang auf seine benötigte App in der Gesundheitsorganisation erhält, wenn er sich erfolgreich authentifiziert hat – und damit nicht mehr in das gesamte Netzwerk zugelassen werden muss.

Zscaler Private Access stellt einen solchen Cloud-basierten Lösungsansatz dar, bei dem der Verbindungsaufbau von der Anwendung ausgeht. Dazu wird über eine in der Cloud zur Verfügung gestellte Vermittlungsinstanz ein Tunnel der Anwendung mit einem weiteren verknüpft, der vom Anwender ausgeht. Hierbei handelt es sich um eine echte Mikrosegmentierung, die unabhängig vom Standort stattfindet. Da die Anwendung auf diese Weise nicht mehr dem Internet ausgesetzt wird, ist sie dort nicht sichtbar und somit nicht angreifbar.

Darüber hinaus stellten wir auf der Messe mit Zscaler B2B einen neuartigen Service vor, der Organisationen die Bereitstellung des sicheren Zugriffs auf Anwendungen für Kunden, Lieferanten und Drittanbieter ermöglicht. Dienstleister können durch eine automatisierte, sichere Anbindung in den Betrieb eingebunden werden und entlasten die IT-Administration. Die Lösung besteht aus einer Kombination von Zscaler Private Access (ZPA) und Multiple IDP (MIDP) und basiert auf einer Zero Trust Network Access (ZTNA)-Architektur, wobei der Zugriff vom Service aus initiiert wird. So wird externen

Thomas Koch, Area Manager Large Enterprise Germany bei Zscaler

Partnern von Krankenhäusern der Zugriff auf Anwendungen Richtlinien-basiert ermöglicht, nachdem sie sich bei ihrer eigenen IDP-Lösung authentifiziert haben. Nach der Autorisierung sind nur die Anwendungen einsehbar, auf die Zugriffsrechte bestehen. Kündigt ein Mitarbeiter eines Lieferanten, werden seine Zugriffsrechte sofort entzogen, sodass es keine digitalen Spuren außerhalb des Unternehmens gibt, über die unberechtigter Zugang möglich ist.

Die Benutzer werden über einen sicheren Tunnel mit den Anwendungen verbunden, der die vollständige Privatsphäre und Integrität aller Daten und Benutzer gewährleistet. Geschäftskunden wählen sich anwenderfreundlich über einen Cloud-Broker bei ihren Anwendungen ein, über vollständig verschlüsselte Verbindungen, die von innen nach außen aufgebaut werden.


Effektiver Schutz für sensible Krankenhaus-Daten:

sayTEC auf der it-sa 2019:

Der Münchener Datensicherheits-Spezialist sayTEC AG hat auf der diesjährigen IT-Security Fachmesse it-sa Nürnberg, Schwachstellen von Krankenhäusern und medizinischen Einrichtungen behandelt. Und das hat einen ganz konkreten Grund – denn die Bedrohung wächst: Krankenhäuser stehen zunehmend unter Beschuss von Cyber-Kriminellen. So waren etwa im Sommer 2019 mehr als zehn Einrichtungen in Deutschland betroffen. Krankenhäuser und Altenpflegeeinrichtungen unter der Trägerschaft des Deutschen Roten Kreuzes (DRK) **sahen sich mit einer Malware-Attacke konfrontiert, die in Folge die IT großflächig lähmte: Der Zugriff auf die gesamte Infrastruktur war nicht möglich, in vielen Fällen mussten beispielsweise Befunde händisch mit Papier und Bleistift notiert werden – an einem funktionierenden Betrieb war nicht zu denken.**

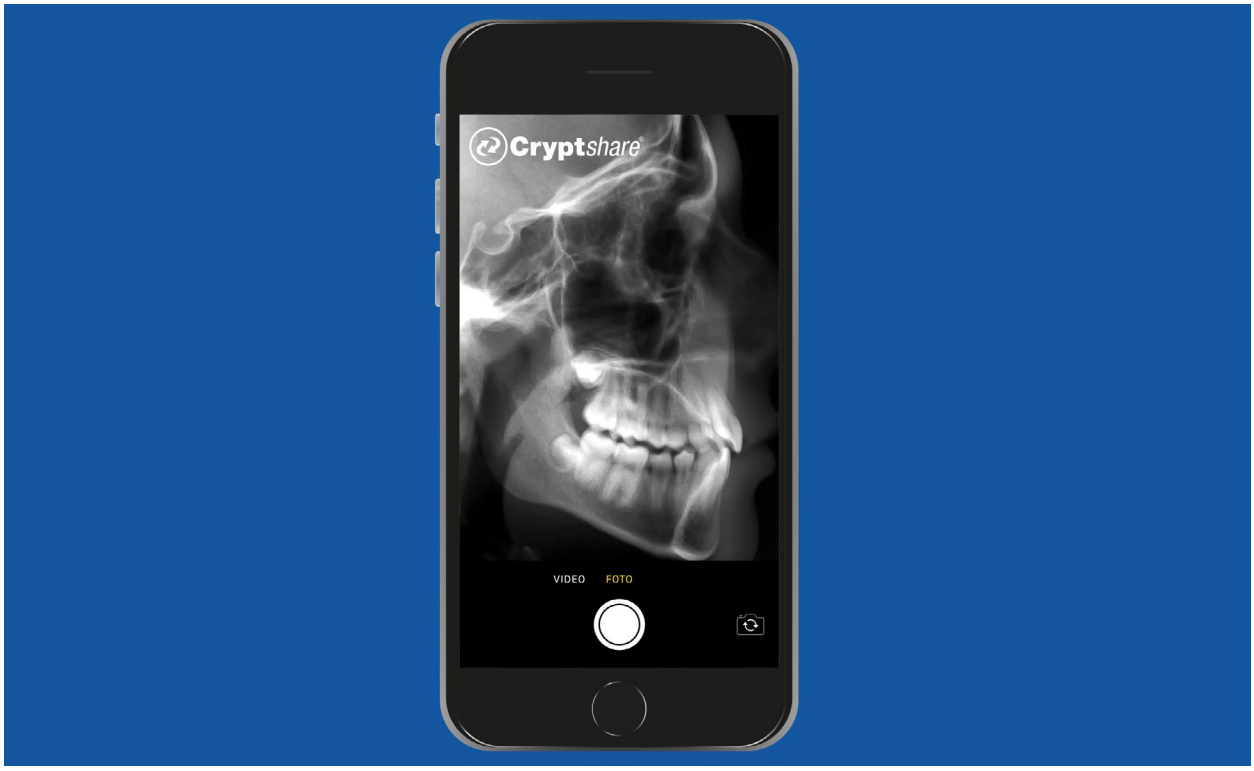
Neben der Einschränkung der Produktivität, ist vor allem auch der theoretisch mögliche Verlust von sensiblen Patientendaten äußerst heikel und kann vor dem Hintergrund der EU-DSGVO durch empfindliche Bußgelder zu drastischen finanziellen Konsequenzen führen. Fatalerweise stehen Krankenhäuser für Hacker auf dem Präsentierteller. Denn große Mengen an personenbezogenen Daten werden in vielen Fällen aufgrund schrumpfender Budgets, mit veralteten Systemen und Technologien gesichert. Eine echte Herausforderung für Healthcare-Einrichtungen.

Mit neuen Technologien und maßgeschneiderten Lösungen „Made in Germany" kann die sayTEC AG helfen. In den Bereichen Datensicherung und hochsichere Datenkommunikation sind die Produkte vor allem darauf ausgerichtet, Daten jederzeit geschützt verfügbar zu halten und einen hochsicheren Zugriff für berechtigte Personen – und nur diesen – zu gewährleisten.

Auf der it-sa 2019 präsentierte sayTEC in diesem Segment die neue patentierte Netzwerk-Zugangstechnologie VPSC (Virtual Protected Secure Communication). Der Zugriff auf das Netzwerk erfolgt praktisch über eine nicht sichtbare Tunneltechnologie und bietet einen äußerst wirkungsvollen Schutz vor Cyber-Attacken. Die VPSC-Technologie eignet sich insbesondere als Alternative zu klassischen, angreifbaren VPN-Verbindungen.

Mit sayFUSE präsentierte sayTEC eine einzigartige Lösung für Backup, Archivierung und Wiederherstellung. Bis zu 18 TB kann die Appliance in einer Stunde auslagerbar sichern. Das Besondere dabei ist die Möglichkeit, eine All-in-One-Lösung zu nutzen, die individuell nach Bedarf bestückt und konfiguriert werden kann. In der Grundkonfiguration bietet das Gerät in einem 19 Zoll Gehäuse auf nur 4 Höheneinheiten eine komplette IT-Infrastruktur inkl. Serverumfeld, Sorage- und Backup-Einheit. Die Lösung ist dabei auf absolute Zuverlässigkeit und Verfügbarkeit ausgelegt, indem die Backups im Mehrgenerationsprinzip auf Festplatten gesichert werden und die Wiederherstellung im Störfall durch einfaches plug & play in Hochgeschwindigkeit erfolgt.

*Weitere Informationen: **www.saytec.eu** oder bei unserem Distributionspartner Red Eagle IT GmbH **www.redeagle-it.de** Die Red Eagle IT hat sich auf das Thema Security spezialisiert und kann Sie als Value Added Distributor durch Fachkenntnis bestens unterstützen.*



Wie Einrichtungen im Gesundheitswesen die Ansteckungsgefahr durch Ransomware senken können

Warum Prophylaxe immer wichtiger wird

Der Befund ist eindeutig: Erpressung ist ein lohnendes Geschäftsmodell für Cyber-Kriminelle, Tendenz steigend. Einrichtungen im Gesundheitswesen müssen immer mit einer Infektion rechnen, hundertprozentigen Schutz gibt es nicht. Vorfälle wie die erneuten Angriffe mit der Schad-Software Emotet im Sommer belegen, dass E-Mails nach wie vor das Haupteinfallstor für Malware aller Art sind. Das ist Teil des Problems und kann Teil der Lösung sein – wenn die Gesundheitsbranche die Art ihrer Kommunikation ändert.

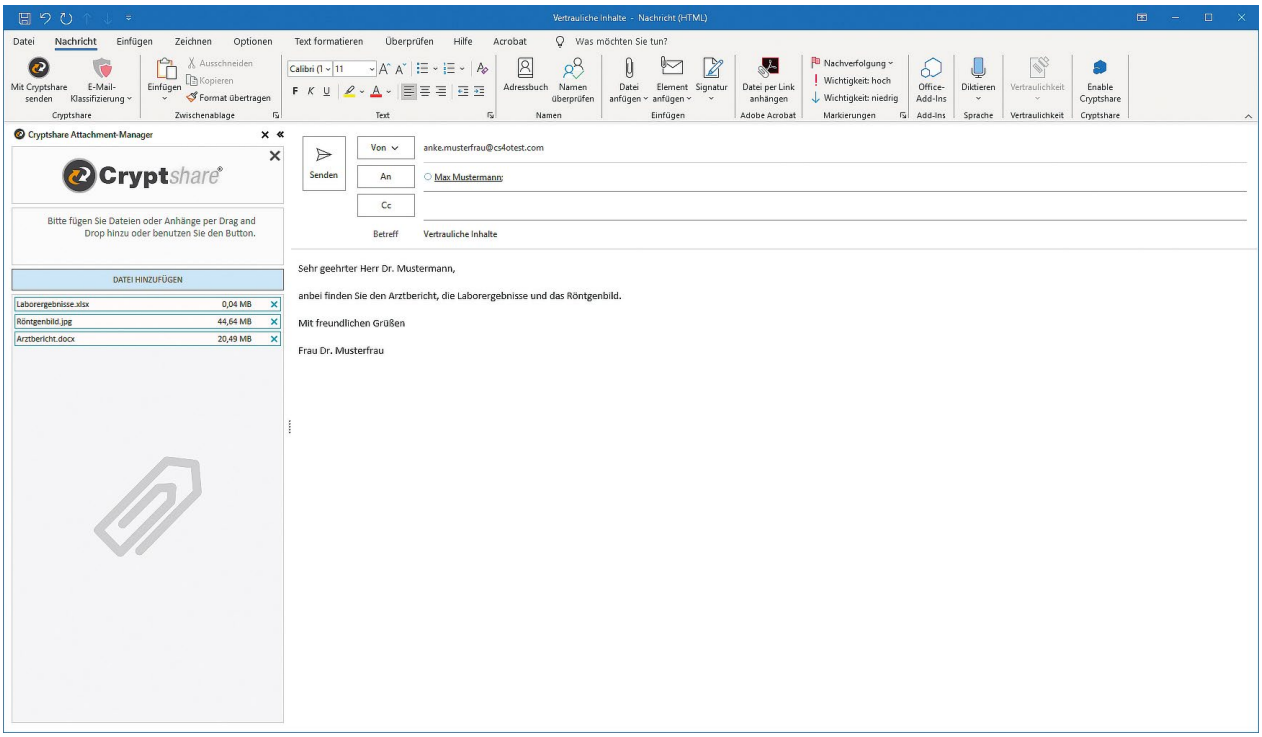
Drastischer als durch die Vorfälle, die in den vergangenen Jahren bekannt wurden, hätte uns die Verwundbarkeit der digitalen Infrastruktur wohl kaum vor Augen geführt werden können.

Dabei fällt auf, dass immer wieder Systeme in „kritischen Infrastrukturen (KRITIS)“ infiziert wurden, zu denen viele größere Kliniken gehören. Die Vorfälle zeigen auch, dass die Sensibilisierung von Mitarbeitern in Form regelmäßiger Schulungen unabdingbar ist, aber nicht isoliert betrachtet werden sollte. Das IT-Grundschutz-Kompendium nennt übrigens explizit beide Maßnahmen, Sensibilisierung und Schulungen.

Befund: Cyber-Kriminalität lohnt sich

Wer kann, sollte seine Systeme umgehend „impfen“ – das Patchen von Sicherheitslücken gilt zu Recht als probate Schutzmaßnahme. Der Einsatz passender Sicherheitslösungen (die 2018 endgültig in Kraft getretene DS-GVO spricht von „angemessenem Schutz“) sowie regelmäßige Backups sollten ohnehin selbstverständlich sein.

Doch auch in der Gesundheitsbranche tun sich die Betroffenen oft schwer, die Forderungen nach sofortigem Aktualisieren von Betriebssystemen und Software-Programmen umzusetzen.



Medizinische Einrichtungen müssen daher erstens ein effizientes Risikomanagement betreiben und zweitens Maßnahmen ergreifen, um zu verhindern, dass sensible personenbezogene Daten in die falschen Hände gelangen.

Vorsorgeuntersuchung: Auch in der IT wichtig

Wie in der Medizin sollten auch in der IT regelmäßige „Vorsorgeuntersuchungen" durchgeführt werden. Um eine fundierte Diagnose stellen zu können, müssen die in vielen Gesundheitseinrichtungen gängigen Kommunikationsprozesse betrachtet werden.

Die Therapie – und das ist die gute Nachricht – besteht aus einfachen und schnell umsetzbaren Maßnahmen, deren kombinierte „Wirkstoffe" den Angreifern das Leben schwerer machen. Hier greift die Umstellung der internen Workflows ebenso wie der Einsatz entsprechender Software-Lösungen, die dafür sorgen, dass vorab definierte Dateitypen erst gar nicht per E-Mail angenommen werden können.

Eine spezielle Authentifizierung sowie das verschlüsselte Übertragen der Inhalte machen das Mitlesen von E-Mail-Korrespondenz unmöglich. Und erst wenn auch die Betreffzeilen (anders als bei S/MIME und PGP) verschlüsselt sind, können Angreifer nicht erkennen, wer mit wem worüber spricht und daraus Rückschlüsse ziehen. Schon diese Informationen können für einen Social-Engineering-Angriff ausreichen.

Mit der richtigen Kombination aus Authentifizierung und Verschlüsselung ist es bspw. möglich, Laborergebnisse, Arztberichte und 3D-Scans sicher auszutauschen. Anhand von Röntgenbildern und CT-Scans lassen sich ganz einfach von entfernt praktizierenden Kollegen Zweitmeinungen zu Diagnosen einholen. Auch kann man Patienten Kopien ihrer Aufnahmen zukommen lassen, ohne sie auf CD brennen und per Post versenden zu müssen. Und mit entsprechenden Automatisierungsmöglichkeiten lässt sich der Versand an einzelne Empfänger oder große Verteilerlisten zeit- oder ereignisgesteuert gestalten, beispielsweise von Gehaltsabrechnungen.

Therapie: Kombination von Wirkstoffen

Diese Art der Vorsorge in Verbindung mit einem Umdenken bei bestehenden Kommunikationsprozessen ist auf lange Sicht auch deutlich günstiger als teure „Not-OPs". Denn wenn die Betroffenen Notfallmaßnahmen ergreifen und Spezialisten hinzuziehen, nachdem der Ernstfall bereits eingetreten ist, ist das mit deutlich höheren Kosten verbunden.

Die Prophylaxe, die aus gutem Grund immer stärker in den Mittelpunkt der Gesundheitspolitik rückt, sollte also in der IT noch stärker umgesetzt werden. In beiden Bereichen gilt: Kann die Entstehung einer Erkrankung verhindert werden, ist die anschließende Behandlung erst gar nicht nötig. Am Beispiel der E-Mails zeigt sich, dass das nicht mit großem Aufwand und hohen Kosten verbunden sein muss.

www.cryptshare.com/healthcare

***Matthias Kess* ist technischer Leiter bei der Cryptshare AG. Erste Berührungspunkte mit Healthcare-Themen hatte er bereits in den 1990er Jahren während seines Wirtschaftsinformatikstudiums bei einem deutschen Medizintechnikhersteller.**

Privilegierte Zugangsverwaltungslösung durch virtuelle sterile Desktops

Systancia, französisches Unternehmen im Bereich Cybersicherheit, Virtualisierung und Identitätsmanagement, stellte auf der it-sa 2019 Cleanroom 4 vor, die PAM-Lösung (Privileged Access Management), die Virtualisierung und Cybersicherheit kombiniert. Dieses Update von Systancias Kernlösung zur Sicherung der Desktops von IT-Administratoren bietet mehrere Serviceebenen. Es erfüllt alle Anforderungen privilegierter Benutzer, indem es die Funktionen zur Überwachung, Authentifizierung und Verwaltung von Desktops nutzt.

Modernisierung der Sicherheitsstandards zur Abwehr von Angriffen

Die Aufgaben von IT-Administratoren sind für alle Unternehmen und für die Sicherheit ihrer Daten von strategischer Bedeutung. Doch viele von ihnen haben keine Lösungen, um sich vor den ständig zunehmenden und raffinierten Angriffen von Hackern zu schützen, die wichtige Informationen stehlen oder Produktionssysteme angreifen wollen.

Systancias Lösung transformiert die Verwaltungsdesktops, indem eine sterile und verfügbare Umgebung bereitgestellt wird und die Bedürfnisse der Administratoren erfüllt werden:

- **Mobilität:** Ein Administrator muss seine Administrationsanwendungen überallhin mitnehmen können, ohne die Kontrolle und Sicherheit zu verlieren.
- **Haltbarkeit:** Ein IT-Manager muss die Sicherheit des Zugriffs auf alle aktuellen und zukünftigen Anwendungen der Systemadministration gewährleisten können.
- **Dedizierter Desktop:** Ein Administrations-Desktop soll nur für die Administration und nicht für andere Aufgaben verwendet werden.

Mehrere Service Levels erfüllen die Anforderungen:

Cleanroom Session (ehemals IPdiva Safe) ist für Unternehmen konzipiert, deren Hauptaufgabe der Schutz ihrer Informationssysteme ist. Die Lösung erfüllt ihre Anforderungen dank Berechtigungsmanagement, Passwortwechsel und Videoaufzeichnung.

Cleanroom-Deskop (ehemals IPdiva Cleanroom) richtet sich an Unternehmen und Organisationen, die ihre Verwaltungsarbeitsplätze in taktische Werkzeuge umwandeln müssen. Diese Lösung ermöglicht es ihren Administratoren, alle ihre Administrationsanwendungen auf sichere Weise mit den gleichen Funktionalitäten wie im Büro mitzunehmen. Es bietet ihnen auch Funktionen für das Management von Administrations-Desktops und erweiterte Authentifizierungsverwaltungsmechanismen für Administrationsanwendungen, um IT-Netzwerksicherheitsverantwortlichen ein zusätzliches Sicherheitsniveau zu bieten. Die Option **"Extranet-Access"** ermöglicht auch die Sicherheit des Remote-Administratorzugriffs. Managed Services Operators, Homeworkers oder Mobile Administrators ist es wichtig, einen sicheren Zugriff auf ihre virtuellen Administrations-Desktops zu haben, unabhängig vom jeweiligen Aufenthaltsort. Durch **Cloud-Angebote**, die von Systancia gehostet werden, können Unternehmen die am besten auf ihre Bedürfnisse und Infrastruktur zugeschnittenen Lösungen nutzen, von den neuesten Updates profitieren und sich so voll und ganz der Sicherung von Administrationsarbeitsplätzen widmen.

Systancia bietet die folgenden Dienstleistungen an:

Cleanroom-Starterservice, der den Zugang zu PAM für weniger gut ausgestattete Unternehmen ermöglicht. **Cleanroom Session** und **Cleanroom Desk** sind als vom Unternehmen verwaltete Softwareprodukte oder über Cloud Services erhältlich, die direkt von Systancia in einer privaten Cloud verwaltet werden (Cleanroom Session Private und Cleanroom Desk Private).

Systancia Cleanroom Desk erfüllt die höchsten ANSSI-Anforderungen:

Cleanroom Desk beinhaltet Mechanismen, die es Administratoren ermöglichen, ihre Administrations-Desktops sofort nach dem Trennen der Verbindung zu regenerieren, um das Risiko der Virenverbreitung zu begrenzen. Seine fortschrittlichen automatischen Authentifizierungsmechanismen für Anwendungen und verwaltete Ressourcen stellen sicher, dass keine Anwendung ungesichert bleibt.

Dank seines innovativen Ansatzes ist **Cleanroom Desk** die einzige PAM-Anwendung, die höchste Standards der ANSSI (Nationale Agentur für Sicherheit der Informationssysteme) erfüllt. Gewarnt wird vor Lösungen, die als "Bastion" bezeichnet werden, da sie die Verhinderung eines Angriffs über den Administrationsdesktop nicht berücksichtigen. Es wird daher empfohlen, Office Desktops von Administrations-Desktops zu trennen.

www.systancia.com/de

Application Whitelisting als wirksame Endpoint Protection

Application Whitelisting ist weitaus sicherer, als jede andere Antivirus Technologie, hat aber den Ruf, einen höheren Administrationsaufwand zu erzeugen. Wir haben fünf Krankenhäuser befragt, die SecuLution Application Whitelisting einsetzen.

Cyberangriffe auf Gesundheitseinrichtungen – auch in Deutschland – haben in den letzten Jahren zugenommen. Ein wirksamer Schutz ist die Absicherung der Endpunkte, also der Computer, Server oder Workstations, mittels Application Whitelisting. Das verhindert das Ausführen von ungewollter Software, wie Viren, Trojaner oder Spiele.

Application Whitelisting ist ein technischer Ansatz, bei dem ein elektronischer Fingerabdruck jeglicher Software auf einer Freigabeliste vorhanden sein muss, damit die Software ausgeführt werden kann. Application Whitelisting stellt damit das Gegenteil des Virenscanners dar: Der Virenscanner erlaubt alles und verbietet als "schadhaft" bekannte Software. Application Whitelisting verbietet alles und erlaubt als "gut" bekannte Software. Die technische Herausforderung bei Virenscannern ist, dass auf der Blacklist (der Liste der verbotenen, "bösen" Software) jegliche Schadsoftware vorhanden sein muss. Kennt die Blacklist eine Schadsoftware nicht, wird die Software erlaubt und kann das Computernetzwerk infizieren. Die technische Herausforderung bei Application Whitelisting ist, dass auf der Whitelist (Liste der erlaubten Software) jegliche beruflich benötigte Software vorhanden sein muss. Kennt die Whitelist eine Software nicht, wird die Software verboten. Daher ist beim Einsatz von Application Whitelisting keine Infektion mit bekannter oder unbekannter Schadsoftware möglich.

Der deutsche Hersteller SecuLution GmbH hat auf der it-sa seine Cloud basierte Whitelist vorgestellt, mit der SecuLution Systeme automatisch live erlernen können. So wird die Freigabe von vertrauenswürdiger Standard-Software auf der Whitelist des Anwenders automatisiert aus der Cloud Datenbank des Herstellers übernommen. Anwender müssen nur noch etwaige Individualsoftware einpflegen.

Im Folgenden berichten Anwender des Application Whitelisting von SecuLution über ihre Erfahrungen mit der Lösung. Etwaige Wiederholungen in den Aussagen wurden gekürzt.

SecuLution GmbH
Alter Hellweg 6
59457 Werl
www.seculution.de
mailto:info@seculution.com

Katholisches Klinikum Lünen/Werne

Betten: ca. 600
IT-Systeme: 600
SecuLution Benutzer seit: 2006

Christian Hübener (operativer IT-Leiter): "Wir hatten vor dem Einsatz von SecuLution als Application Whitelisting Lösung einen Virenscanner. Unsere Sorge war, dass man den Antivirus nicht immer auf den aktuellen Stand hat und dadurch Opfer einer Bedrohung wird. Beispiel: Person A bringt einen Stick mit und darauf ist eine Schadsoftware. Derartige Probleme sind zuverlässig vom Tisch. [...] Wir setzen SecuLution Application Whitelisting daher inzwischen in allen Bereichen der Konzernstruktur ein."

St. Joseph-Stift Dresden

Betten: ca. 600
IT-Systeme: 550
SecuLution Benutzer seit: 2007

Rene Schumann (Systemadministrator): "Wir hatten mit SecuLution noch nie einen erfolgreichen Angriff mit Schadsoftware. Der technische Ansatz, nur die Ausführung von als gut bekannter Software möglich zu machen, gibt uns ein gutes und beruhigendes Gefühl, das vorher nicht da war. [...] Die Administrationsoberfläche von SecuLution ist unser sicherheitstechnischer zentraler Dreh- und Angelpunkt."

Marienkrankenhaus Schwerte GmbH

Betten: ca. 500
IT-Systeme: 450
SecuLution Benutzer seit: 2016

Marco van de Straat (stellvertretender IT-Leiter): "Ein Qualitätsmerkmal einer Software ist meiner Meinung nach, wenn man als Admin im Alltag möglichst wenig damit zu tun hat. Seit dem Update auf SecuLution 2.0, besonders durch die automatische Abfrage der TLDB [Anm: Cloud-basierte zentrale Whitelist als Serviceleistung von SecuLution], ist der Umgang auch viel einfacher geworden. [...] SecuLution hat auf jeden Fall einen großen Mehrwert für uns gebracht. Wir haben im Alltag relativ wenig mit der Administration von SecuLution zu tun!"

Rheinland Klinikum Neuss GmbH

Betten: ca. 700
IT-Systeme: 500
SecuLution Benutzer seit: 2016

Christoph Fischer (EDV Administrator): "Vor meiner Zeit [Anm.: 2016] hatten wir ein massives Problem! Unser Virenscanner hatte einen Angriff nicht erkannt. Unsere gesamte IT Struktur war mit Schadsoftware befallen. Es war den Medien zu entnehmen. Wir brauchten eine zuverlässige Lösung, damit derartiges nicht noch einmal passieren kann. [...] SecuLution Application Whitelisting erfüllt unsere Erwartungen voll."

St. Elisabeth - Hospital GmbH Beckum

Betten: ca. 220
IT-Systeme: 270
SecuLution Benutzer seit: 2005

Volker Kliewe (EDV Administrator): "Vor der Entscheidung für SecuLution als Application Whitelisting Lösung hatten wir trotz unseres aktuellen Virenscanners einen Befall mit Schadsoftware. Seit wir SecuLution Application Whitelisting einsetzen, haben wir überhaupt keine Probleme damit mehr. [...] Das permanente Kontrollieren der Arbeitsplätze, ob alle Updates der Virenscanner erfolgreich installiert waren, hat viel Zeit gefressen. [...] Mit SecuLution haben wir nur einen geringen Aufwand, weil die Umsetzung von Aktionen in Echtzeit passiert und die Reaktion des Programms absolut vorhersehbar ist."

Medizingeräte im Visier von Hackern:
Security Check on Medical Devices von TÜV SÜD für mehr Sicherheit im Gesundheitswesen

Die Digitalisierung ändert den Krankenhausalltag spürbar. In digitalen Patientenakten werden hochsensible persönliche Daten zum Krankheitsverlauf erfasst, wie beispielsweise Laborwerte, Untersuchungsergebnisse, Röntgenbilder oder Medikationen. Untersuchungen werden mittels vernetzter Medizingeräte durchgeführt, und Ärzte haben via Tablet jederzeit Einblick in den Gesundheitsstand ihrer Patienten. Die Digitalisierung macht Krankenhäuser zwar leistungsfähiger und effizienter, aber gleichzeitig auch angreifbarer. Denn jedes vernetzte Gerät kann in einem weit verzweigten Kliniknetzwerk zu einem potenziellen Einfallstor für Hacker werden – sofern es nicht richtig abgesichert ist.

Verdeutlicht wird die Dringlichkeit der IT-Sicherheit von vernetzten Medizingeräten durch die Zunahme von Cyber-Angriffen in Form von Denial-of-Service-Attacken oder Botnet- Angriffen. Unter einem „Denial of Service Angriff" versteht man die absichtliche Überlastung eines Datennetzes, welche zu einer Nicht-Verfügbarkeit des Services führt. Das kann gravierende Folgen haben, wenn beispielsweise lebenserhaltende Systeme in Krankenhäusern betroffen sind. „Botnetze" wiederum sind Netzwerke, die aus ferngesteuerten Computern, IT-Ressourcen und Bots bestehen. Die Computer werden mit Malware infiziert, die es ermöglicht, sie fernzusteuern. Ungesicherte IT oder angeschlossene Medizingeräte eignen sich als ideale Eintrittspforte für Hacker, die sich so über das Netzwerk Zugriff auf weitere Geräte verschaffen. Um solche Szenarien zu verhindern, muss die Cybersicherheit von Medizingeräten heute oberste Priorität haben und als integraler Produktbestandteil betrachtet werden.

Security by Design minimiert das Risiko

Umfassende Cybersicherheit muss weiter gedacht werden, als die bisher üblichen punktuellen Sicherheitsupdates dies leisten können. Sie ist keine Momentaufnahme, sondern ein kontinuierlicher Prozess, der den kompletten Lebenszyklus von Produkten und Systemen betrifft. Auch für Medizingeräte gilt in Zukunft immer mehr: Im Idealfall ist die Cybersicherheit schon von Anfang an eingebaut, man spricht hier von Security by Design. Dabei kommen Dokumenten- und Prozessaudits ebenso zum Einsatz wie regelmäßige Systemprüfungen durch Schwachstellen-Scans und Penetration-Tests.

Hier setzen die Security Check on Medical Device Services von TÜV SÜD an: Umfangreiche Tests bewerten automatisch und manuell den Sicherheitsstatus von vernetzten Medizingeräten. Dabei wird der Sicherheitsstatus der Geräte anhand von Industrienormen wie UL 2900-2-1, IEC/TR 60601-4-5 und generellen Security by Design Prinzipien bewertet. Kritische Punkte, die eine Sicherheitslücke darstellen können, werden dem Hersteller angezeigt. Der Prüfprozess bewertet die kritischsten Bereiche, die die Cybersicherheit von netzwerkfähigen Geräten heute beeinflussen. Analysiert werden u.a. die Geräte-Firmware, produktintegrierte Web-Oberflächen, die Gerätekommunikation, jegliche Schwachstellen, die Sichtbarkeit der verwendeten Hardware- und Softwarekomponenten sowie der offenen Schnittstellen.

Dynamische Bedrohungslage: Angriffen zuvorkommen

Die Bedrohungslandschaft entwickelt sich ständig weiter, und skrupellose Angriffe sind nur noch eine Frage der Zeit. Darum ist es zwingend erforderlich, das Angriffsrisiko auf vernetzte Medizingeräte zu minimieren. Basierend auf den Prioritäten von Kliniken und Arztpraxen werden die Ergebnisse des Medical Testing Services auf die jeweiligen Industriestandards abgebildet. Diese können dann verwendet werden, um die Anforderungen und Bedürfnisse der Betreiber besser zu erfüllen. Letztlich geht es darum, dass sich beide Seiten – sowohl Hersteller als auch Betreiber von vernetzten Medizingeräten – ihrer Verantwortung in Sachen Cybersicherheit bewusst werden und noch enger zusammenarbeiten. Nur so lässt sich ein möglichst hohes Sicherheitsniveau erreichen, um Patienten effektiv zu schützen.

Patientenaufklärungsbögen und eigene Dokumente digital bearbeiten, unterschreiben und sicher archivieren

Eigene Dokumente komplett digital!

E-DocumentPro

Patienten mobil aufklären und informieren!

E-ConsentPro mobile

www.thieme-compliance.de

Thieme Compliance

CLOVERLEAF®

Der Kommunikationsserver

Intelligente Verbindungen.
Auf höchstem Niveau.

Health-Comm GmbH
Software für das Gesundheitswesen

Health-Comm GmbH
Dachauer Str. 11 I 80335 München
Tel.: 089 - 5 99 88 76 - 0
E-Mail: Info@Health-Comm.de
www.Health-Comm.de